



Aula 00

*TSE - Concurso Unificado - Informática -
2023 (Pré-Edital)*

Autor:

**Diego Carvalho, Renato da Costa,
Equipe Informática e TI**

Índice

1) Noções Iniciais sobre Redes de Computadores - Parte 1	3
2) Redes de Computadores - Parte 1 - Tipos de Conexão-Enlace	6
3) Redes de Computadores - Parte 1 - Direções de Transmissão	8
4) Redes de Computadores - Parte 1 - Modos de Transmissão	10
5) Redes de Computadores - Parte 1 - Classificação de Redes	11
6) Redes de Computadores - Parte 1 - Meios de Transmissão	29
7) Redes de Computadores - Parte 1 - Equipamentos de Redes	33
8) Redes de Computadores - Parte 1 - Padrões de Redes	46
9) Noções Iniciais de Redes de Computadores - Parte 1 - Internet	61
10) Redes de Computadores - Parte 1 - Gerações da Web	69
11) Redes de Computadores - Parte 1 - Deep Web e Dark Web	72
12) Redes de Computadores - Parte 1 - Internet das Coisas	79
13) Redes de Computadores - Parte 1 - Tecnologias de Acesso	83
14) Resumo - Redes de Computadores - Parte 1	90
15) Mapas Mentais - Redes de Computadores - Parte 1	97
16) Questões Comentadas - Redes de Computadores - Parte 1 - FCC	104
17) Lista de Questões - Redes de Computadores - Parte 1 - FCC	123

REDES DE COMPUTADORES

Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



Quando a internet cai e eu saio do quarto depois de três dias



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 pessoais¹ 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 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 cheio de furinhos chamado 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 muitos 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?

(Assembleia Legislativa de Goiás – 2016) 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) Interligacão de Redes de Computadores

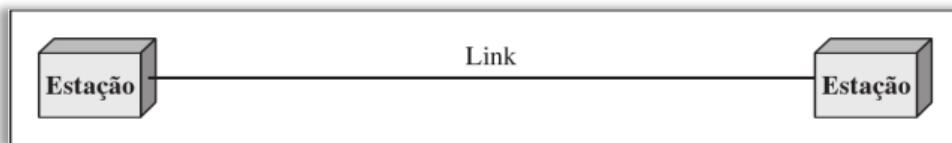
Comentários: quando a banca diz “*um conjunto de unidades processadoras*”, ela só está usando um nome técnico para “*um conjunto de computadores*”. Portanto, um conjunto de computadores interconectados que permite o compartilhamento de recursos tais como impressoras, discos, entre outros, só pode ser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

Tipos de Conexão/Enlace

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

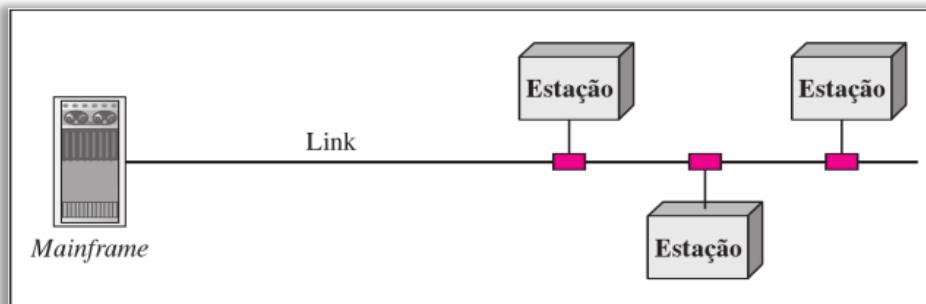
Redes são dois ou mais dispositivos conectados através de links. *O que é um link? Também chamado de enlace, trata-se de um caminho de comunicação que transfere dados de um dispositivo para outro.* Para fins de visualização, é mais simples imaginar qualquer link como uma reta entre dois pontos. Para 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 accesse a internet, eu comarto vários cabos subterrâneos espalhados pelo nosso planeta com todas as pessoas que têm acesso à internet.



Nesse contexto, pode-se afirmar que, quando eu accesso 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, dois ou mais dispositivos compartilham um único link. E um ambiente multiponto, a capacidade do canal de comunicação é compartilhada, seja de forma

espacial ou 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 dois ou mais dispositivos.

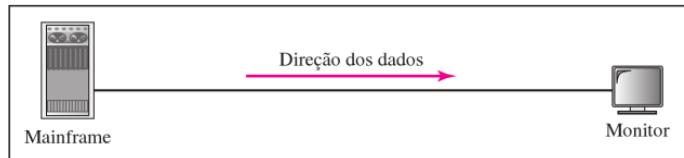
(MPU – 2010) Em rede multiponto, há diversos computadores interligados em um mesmo circuito, no entanto o circuito só pode ser utilizado por um computador de cada vez.

Comentários: perfeito... 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 (Correto).

Direções de Transmissão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Simplex

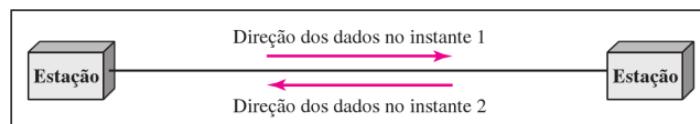


O ENLACE É UTILIZADO APENAS EM UM DOS DOIS POSSÍVEIS SENTIDOS DE TRANSMISSÃO
EXEMPLO: TV, RÁDIO AM/FM, TECLADO, ETC.

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



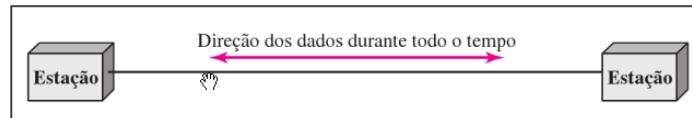
O ENLACE É UTILIZADO NOS DOIS POSSÍVEIS SENTIDOS DE TRANSMISSÃO, PORÉM APENAS UM POR VEZ
EXEMPLO: WALK&TALK E NEXTEL

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.



(CRESS/SC – 2019) Quanto à direção do fluxo de dados, na comunicação entre dois dispositivos no modo Half-Duplex, cada estação pode transmitir e receber, mas nunca ao mesmo tempo.

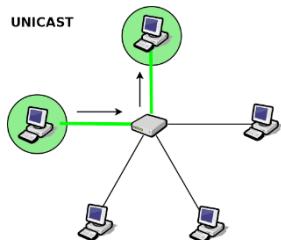
Comentários: na comunicação half-duplex, cada estação transmite e recebe, mas não simultaneamente (Correto).

Modos de Transmissão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

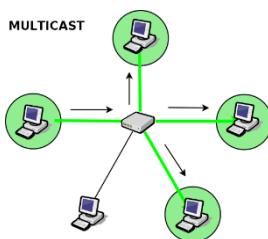
A transmissão de dados em uma rede de computadores pode ser realizada em três sentidos diferentes: *Unicast*, *Multicast* e *Broadcast*. Vamos vê-los em detalhes:

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



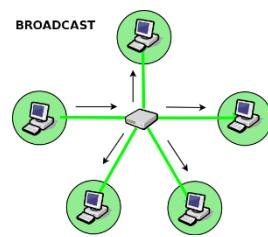
Nessa comunicação, **uma mensagem só pode ser enviada para um destino**. Observem que a primeira estação de trabalho está enviando uma mensagem endereçada especificamente para a terceira estação de trabalho. Analogamente, quando você envia uma mensagem no Whatsapp para uma pessoa específica, você está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

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.**

Classificação de Redes

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. *Fechado?*

PAN (Personal Area Network)

INCIDÊNCIA EM PROVA: BAIXA



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 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, do tamanho máximo de um quarto.

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!



DISTÂNCIA

ALGUNS CENTÍMETROS A POUCOS METROS

LAN (Local Area Network)

INCIDÊNCIA EM PROVA: ALTÍSSIMA



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. *Entendido, camaradas?*

Em geral, esse tipo de rede possui baixa ocorrência de erros por redes pequenas e contidas em um local específico – e, não, espalhadas por vários locais. *E o que tem a ver essa foto, professor?* Galera, a imagem acima é do meu querido local de trabalho. Para quem não conhece, esse é o prédio do Tesouro Nacional e eu orgulhosamente vos apresento o fantástico céu de Brasília. *Tem coisa mais bonita? Venham aqui me visitar e me convidem para o churrasco de posse :)*



DISTÂNCIA

DE ALGUMAS CENTENAS DE METROS A ALGUNS QUILÔMETROS.

MAN (Metropolitan Area Network)

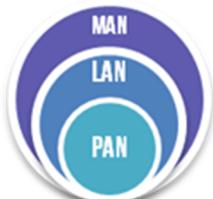
INCIDÊNCIA EM PROVA: ALTÍSSIMA



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 acima, 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.

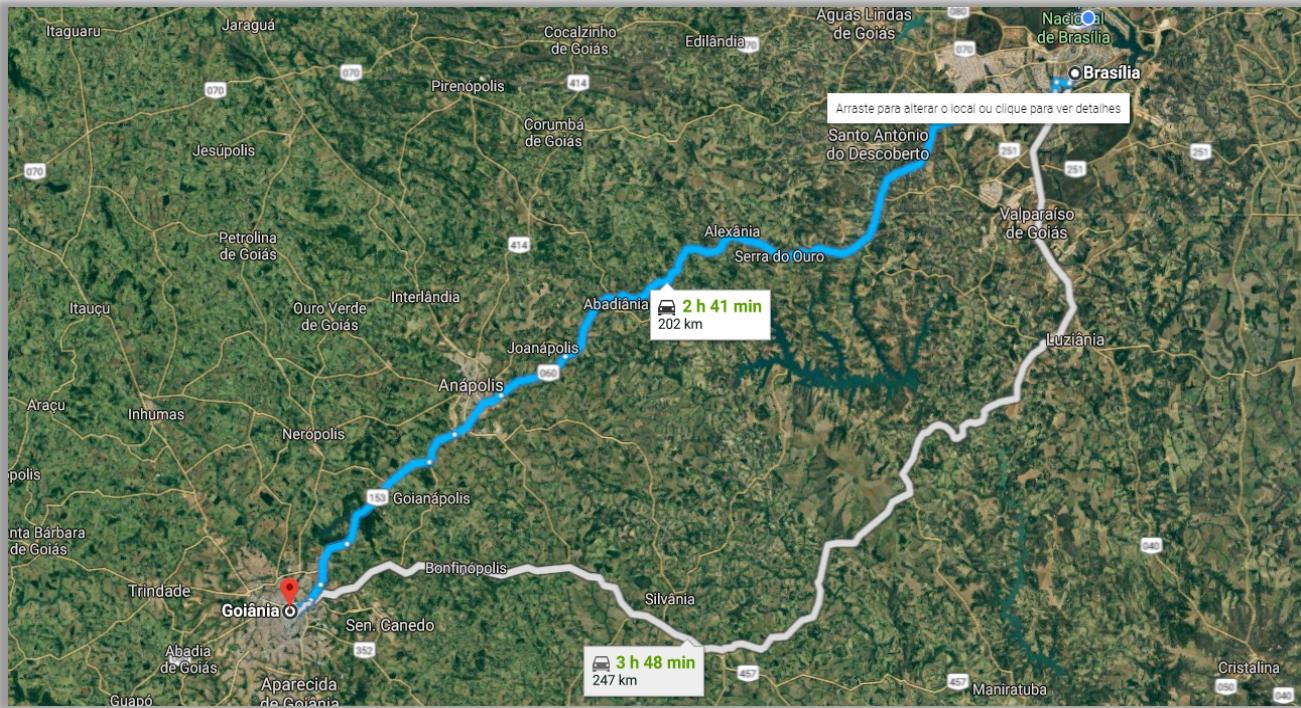


DISTÂNCIA

ALGUMAS DEZENAS DE QUILÔMETROS

WAN (Wide Area Network)

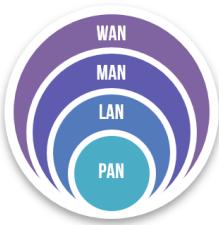
INCIDÊNCIA EM PROVA: ALTÍSSIMA



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.**



DISTÂNCIA

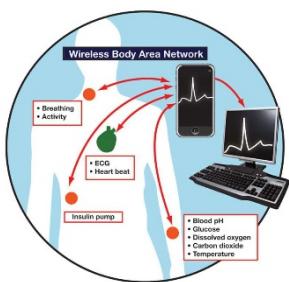
CENTENAS A MILHARES DE QUILÔMETROS

Em suma, a classificação quanto à dimensão pode ser resumida a 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, desenganem 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 :)



(TELEBRÁS – 2015) As redes locais (LANs) são aquelas instaladas em grandes cidades de regiões metropolitanas, para a interconexão de um grupo grande de usuários.

Comentários: grandes cidades de regiões metropolitanas? Não, essa é a MAN (Metropolitan Area Network)! A LAN (Local Area Network) conecta casas, escritórios, pavimentos ou prédios (Errado).

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, melhor na 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?*

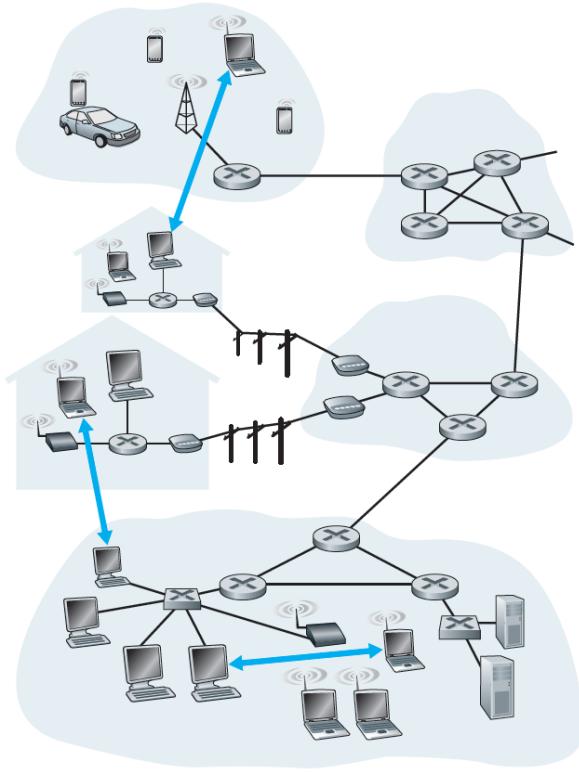
Ora, raramente alguém precisa de uma impressora só para si, portanto o compartilhamento de recursos otimizava bastante os custos e processos de uma organização. No entanto, outros recursos podiam ser compartilhados, como softwares, backups, e-mails e – principalmente – dados. **Uma forma eficiente de 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 aonde? No servidor! E tanto os clientes quanto os servidores estão conectados entre si por uma rede. Como na vida real, cliente é o 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 papéis 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 problema¹.

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,**

¹ 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).



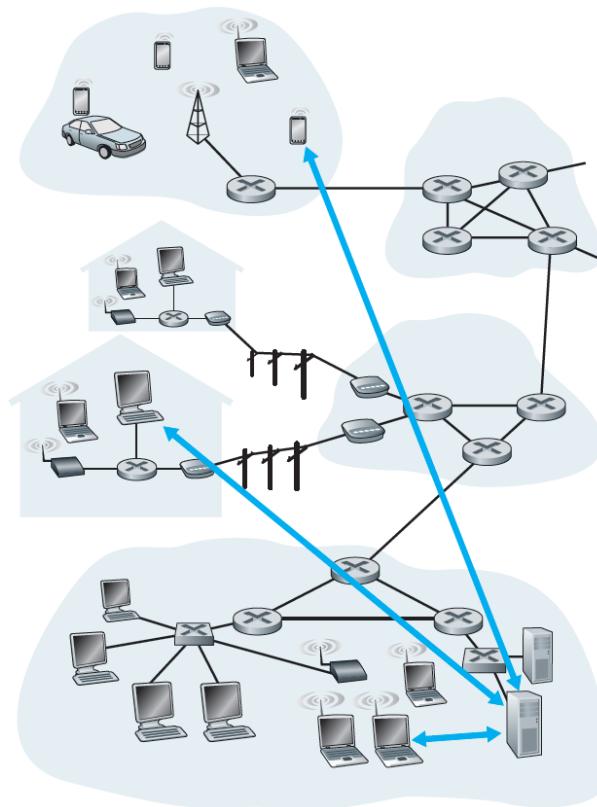
O termo ponto-a-ponto costuma confundir porque pode ser utilizado em dois contextos com significados diferentes. No contexto de **Tipos de Conexão**, ele pode ser utilizado como contraponto ao enlace ponto-multiponto, ou seja, trata-se de um link dedicado entre dois dispositivos, em contraste com o enlace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

5.2.2 – 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 anterior 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.**

(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) Bluetoofh
- b) FTP
- c) POP3
- d) P2P
- e) B2B

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

(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).

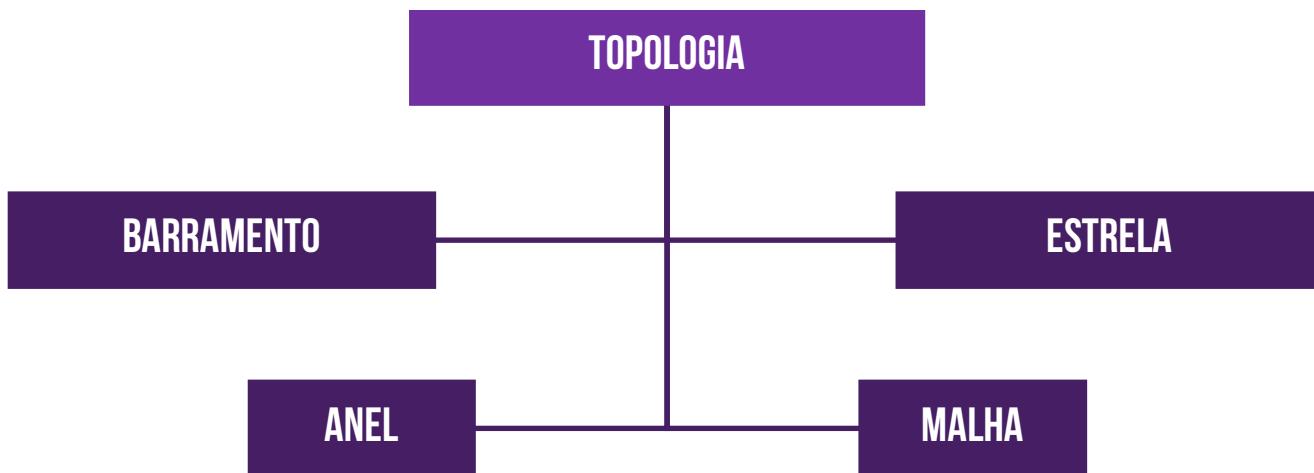
(DPE/PR – 2012) Arquitetura de serviço de rede onde todos os participantes são ao mesmo tempo servidores e clientes entre si. Está-se falando de:

- 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).

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 básicas² 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.



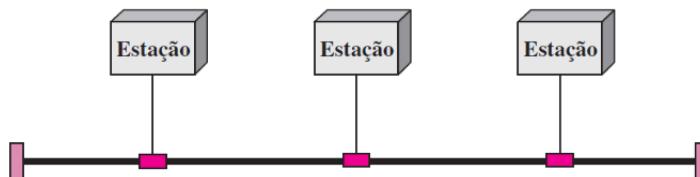
Se uma questão de prova não deixar explícito em sua redação qual é o tipo de topologia, pode-se assumir que ela se refere à **Topologia Física e – não – à Topologia Lógica!**

² Existem outras topologias, como a topologia em árvore, daisy chain, entre outros, 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-multiponto³. 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.

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. Professor, não entendi muito bem! Galera, imaginem que nós temos um varal com diversas roupas

³ Assim como a topologia em anel (que veremos adiante), está em desuso há muitos anos, mas continua sendo cobrada em concursos públicos.

penduradas. Caso haja um rompimento do varal, todas as roupas caem; no entanto, se uma única roupa cair, nada acontece com o restante – é semelhante na Topologia em Barramento!

Vantagens: facilidade de instalação e economia de cabeamento. Em outras palavras, como se trata de 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.

(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).

(CGE/CE – 2019) Em uma rede de comunicação, quando um dispositivo transmite um sinal, toda a rede fica ocupada; se outro dispositivo tentar enviar um sinal ao mesmo tempo, ocorrerá uma colisão e a transmissão deverá ser reiniciada. Nessa situação, a topologia dessa rede de comunicação é do tipo:

- a) barramento
- b) anel
- c) estrela
- d) árvore
- e) ponto a ponto

Comentários: quando um dispositivo transmite um sinal, a rede fica ocupada porque o sinal é enviado em broadcast; se outro dispositivo tentar enviar, ocorre uma colisão – essas são características da topologia barramento (Letra A).

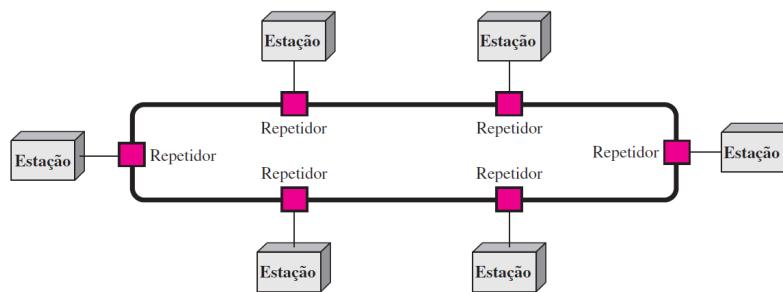
(CRA/PA – 2019) Na topologia em barramento, apenas os computadores das extremidades (pontas) é que podem enviar dados para quaisquer computadores, pois, nesse tipo de topologia, eles são os gerenciadores da rede.

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 deseja 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 que?* 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).

(TRE/GO – 2015) A topologia de uma rede refere-se ao leiaute físico e lógico e ao meio de conexão dos dispositivos na rede, ou seja, como estes estão conectados. Na topologia em anel, há um computador central chamado *token*, que é responsável por gerenciar a comunicação entre os nós.

Comentários: em uma topologia em anel, não há um computador central. O *token* é um recurso que possui a função de permitir que uma estação de trabalho transmita dados por um canal sem o risco de colisões (Errado).

(FUNCAB – 2014) É uma característica das redes com topologia lógica em anel:

- a) os sinais durante a comunicação se propagam em todas as direções.
- b) os dados são transmitidos de forma unidirecional até chegar ao seu destino.
- c) os nós são interligados a um nó central.
- d) os sinais se propagam de forma hierárquica em ambos os sentidos.
- e) o sinal originado por um nó não é regenerado o que causa uma atenuação do sinal.

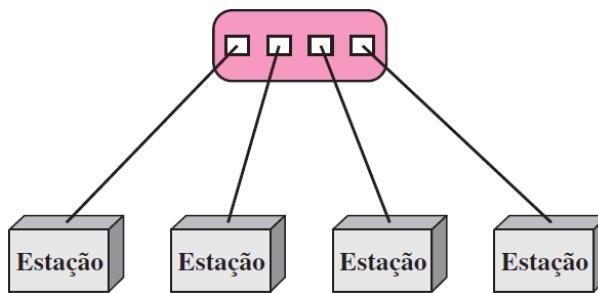
Comentários: (a) Errado, eles se propagam em apenas uma direção; (b) Correto; (c) Errado, não há nó central; (d) Errado, não há hierarquia e a propagação ocorre em apenas uma direção; (e) Errado, o sinal é regenerado e, por isso, não causa atenuação do sinal (Letra B).

Estrela (Star)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Nessa topologia, as estações são ligadas através de uma conexão ponto-a-ponto dedicada a um nó central controlador⁴, 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.

(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).

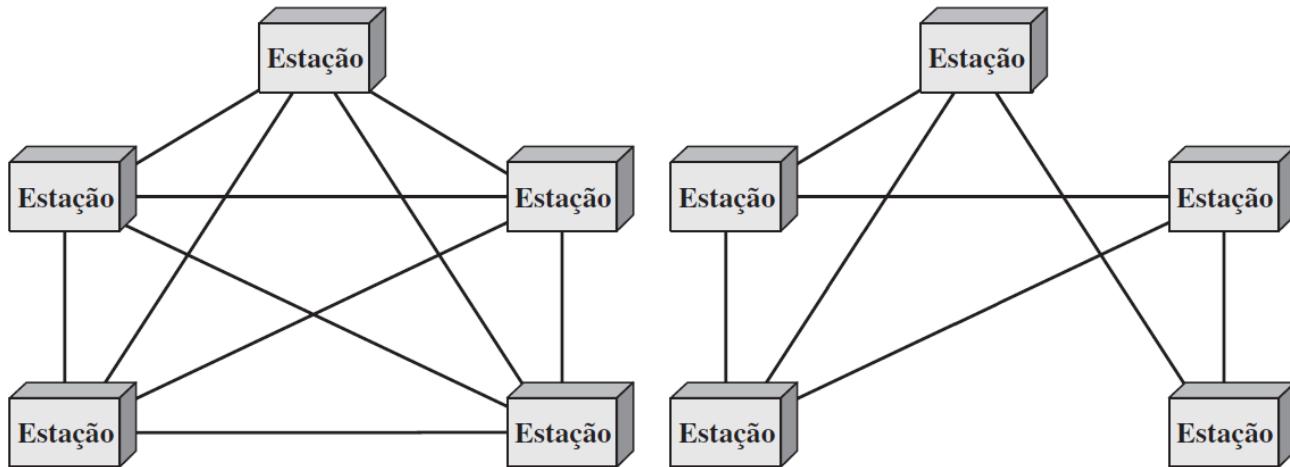
⁴ Nô central é um dispositivo que concentra conexões – em geral, ele liga os cabos dos computadores de uma rede (Ex: Hub ou Switch).

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 existe 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 nós⁵.



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 se 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

⁵ 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 necessários $n.(n-1)/2$ 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. É importante salientar também que existem as redes em malha sem fio, que são comumente utilizadas para interligar – por exemplo – dispositivos sem fio em uma rede local por meio de radiofrequência. Tem sido cada vez mais comum a venda de kits de roteadores wireless capazes de criar uma rede em malha em uma casa.

TOPOLOGIA FÍSICA	DIREÇÃO DE TRANSMISSÃO	TIPO DE ENLACE
BARRAMENTO	Half-Duplex	Multiponto
ANEL	Simplex	Ponto-a-Ponto
ESTRELA	Half-Duplex (se usar Hub) Full-Duplex (se usar Switch)	Ponto-a-Ponto
MALHA	Depende	Ponto-a-Ponto

(CEGÁS – 2017) Uma topologia de rede tem o objetivo de descrever como é estruturada uma rede de computadores, tanto fisicamente como logicamente. A topologia onde cada estação de trabalho está ligada a todas as demais diretamente, possibilitando que todos os computadores da rede, possam trocar informações diretamente com todos os demais, é denominada de:

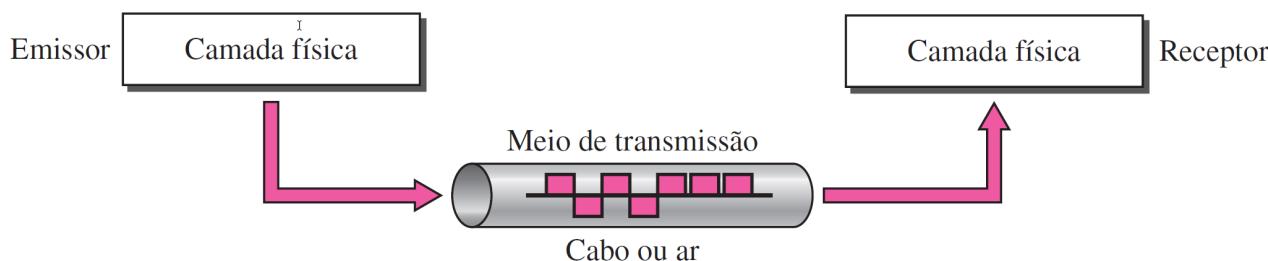
- a) Malha
- b) Árvore
- c) Estrela
- d) Anel

Comentários: a única opção que apresenta uma topologia em que cada estação se comunica diretamente com todas as outras é a topologia em malha – nesse caso, é especificamente uma malha completa (Letra A).

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 trançado, 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.



(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).

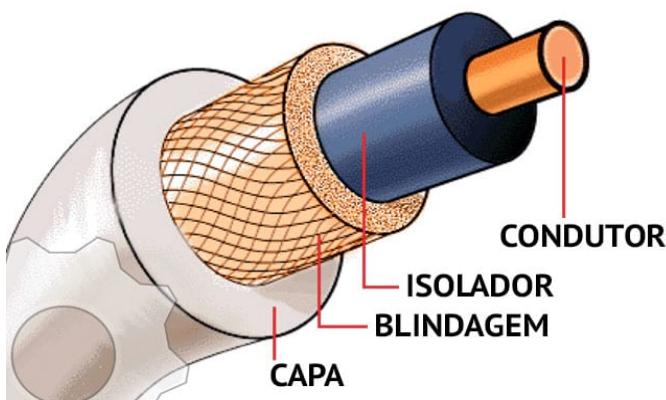
(Prefeitura de Pinhais/PR – 2017) Os meios de transmissão em uma rede podem ser classificados como meios guiados e não guiados. Selecione a alternativa que exemplifica um meio de transmissão não guiado.

- 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).

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, relativamente flexível e muito resistente à interferência eletromagnéticas graças a sua malha de proteção. Esse cabo cobre distâncias maiores que o cabo de par trançado e utiliza um conector chamado BNC.

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.



Professor, eu acabei de olhar aqui e não entra nenhum cabo coaxial no meu computador! Parabéns, você foi olhar! O cabo coaxial do seu Pacote de TV/Internet vem da rua, entra na sua casa e é conectado ao modem e do modem saem dois cabos: um cabo de par trançado, que vai para o seu computador; e um cabo coaxial, que vai para o Decodificador de TV. Bacana? **Outro ponto interessante é que ele é capaz de cobrir longas distâncias, apesar de possuir uma taxa de transmissão menor que a de um cabo de par trançado.** Compreendido? Então, vamos seguir...

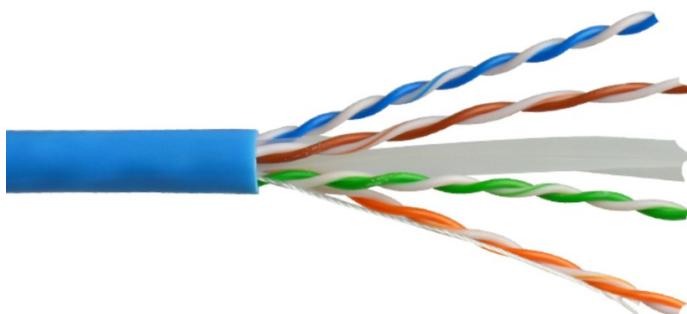
(FUB – 2015) O cabo coaxial, meio físico de comunicação, é resistente à água e a outras substâncias corrosivas, apresenta largura de banda muito maior que um par trançado, realiza conexões entre pontos a quilômetros de distância e é imune a ruídos elétricos.

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 – à 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



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!**).

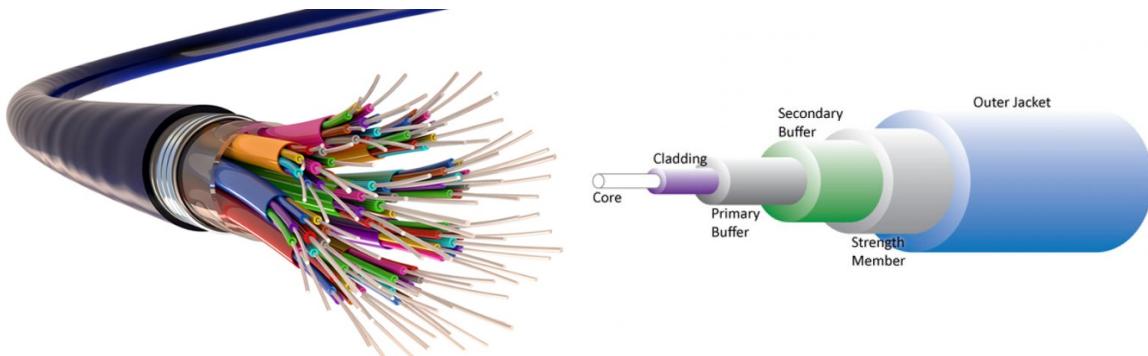
Quando é blindado, ele é chamado de Cabo STP (*Shielded Twisted Pair*) e quando não é blindado, ele é chamado de Cabo UTP (*Unshielded Twisted Pair*). **Galera, esse é aquele cabinho azul que fica atrás do seu computador ligado provavelmente a um roteador. Sabe aquele cabo do telefone fixo da sua casa?**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

CATEGORIA	TAXA MÁXIMA DE TRANSMISSÃO	LARGURA DE BANDA	DISTÂNCIA MÁXIMA
CAT3	Até 10 MBPS	16 MHz	100 Metros
CAT4	Até 16 MBPS	20 MHz	100 Metros
CAT5	Até 100 MBPS	100 MHz	100 Metros
CAT5E	Até 1000 MBPS (1G)	100 MHz	100 Metros
CAT6	Até 10000 MBPS (10G)	250 MHz	100 Metros
CAT6A	Até 10000 MBPS (10G)	500 MHz	100 Metros
CAT7	Até 10000 MBPS (10G)	600 MHz	100 Metros
CAT7A	Até 10000 MBPS (10G)	1000 MHz	100 Metros
CAT8	Até 40000 MBPS (40G)	2000 MHz	100 Metros

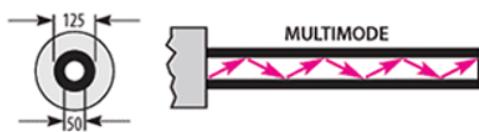
Os cabos de par trançado possuem quatro pares de fios, sendo alguns utilizados para transmissão e outros para recepção, permitindo uma comunicação *full duplex*. Para facilitar a identificação, os pares são coloridos e a ordem dos fios dentro do conector é padronizada. Eles podem ser utilizados na transmissão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

Cabo de Fibra Óptica

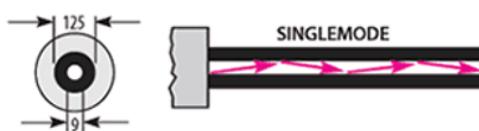
INCIDÊNCIA EM PROVA: MÉDIA



Consiste em uma Casca e um Núcleo (em geral, 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, ele é incapaz de fazer curvas acentuadas, além de ter um custo de instalação e manutenção muito alto em relação ao par trançado. *Entendido?* Há dois tipos de fibra: **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).**

(EMBASA – 2014) 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 nos focar agora nos dispositivos intermediários. Venham comigo...

Network Interface Card (NIC ou Placa de Rede)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



Galera, essa é a famosa Placa de Rede¹! Se vocês olharem na parte de trás do gabinete de um computador, vocês a verão (provavelmente com o cabo azul de par trançado conectado a ela). Esse é o recurso de hardware geralmente instalado no computador para permitir uma comunicação bidirecional – transmissão e recebimento de dados – com os demais elementos da rede. Agora vejam que coisa interessante...

Você tem um CPF, que é um número único que te identifica. *Por que?* Porque não existe outra pessoa no mundo com esse mesmo número. **Da mesma forma, as Placas de Rede possuem um identificador único chamado Endereço MAC (Media Access Control) – é como se fosse o número de série do dispositivo.** Esse endereço físico é representado por 48 bits, representados em hexadecimal e separados por dois-pontos (Ex: 00:1C:B3:09:85:15).

(UFBA – 2012) Uma placa de rede Wi-Fi é um dispositivo de entrada e saída.

Comentários: a questão está perfeita – dados entram e saem da placa de rede wi-fi (Correto).

¹ As placas de rede podem também ser chamadas de Placas NIC. Além disso, a imagem à esquerda mostra uma placa de rede cabeada e a imagem à direita mostra uma placa de rede wireless.

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:



(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).

(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).

(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.

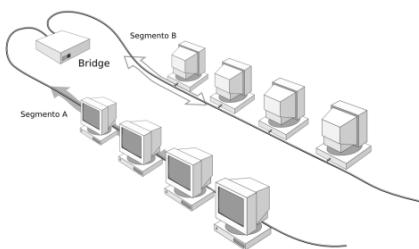
Comentários: o dispositivo em desuso incapaz de direcionar/encaminhar dados porque só transmite em broadcast é o Hub (Letra C).

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 à quem os dados devem ser encaminhados.

Elá 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 específicos e, não, para todos os computadores da rede – como ocorria com o hub! Lembrem-se que o hub envia dados para todos 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 aumenta da largura de banda e a separação dos domínios de colisão.

(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 **autonegotiação**, 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?*

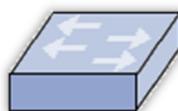
O recurso de autonegotiação do switch permite que seja negociado tanto a taxa de transmissão de dados quanto a direção de transmissão, isto é, se um trabalha com uma taxa de transmissão maior e o outro com uma taxa de transmissão menor, eles negociam o envio de dados a uma taxa de transmissão menor de 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 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 autonegotiação e autoaprendizagem, sendo capaz de funcionar em *full duplex*². A representação de um Switch é abaixo:



(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: dentre as opções equipamento usado na topologia em estrela é o switch (Letra B).

(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).

² 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.

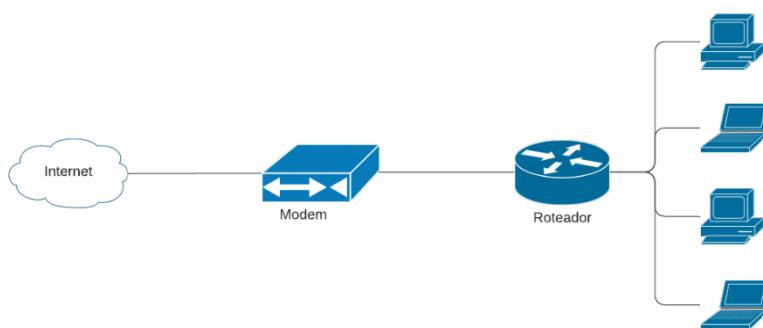
Router (Roteador)

INCIDÊNCIA EM PROVA: ALTA

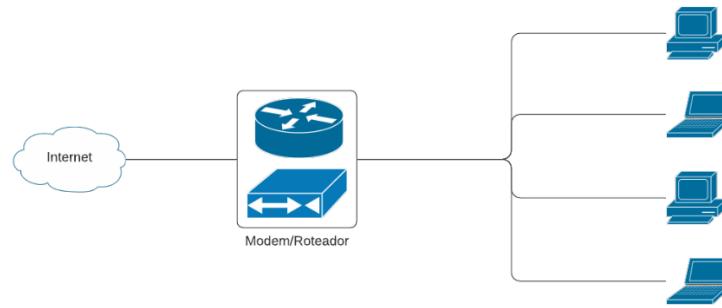


Os roteadores são equipamentos que permitem interligar redes diferentes e escolher a melhor rota para que uma informação chegue ao destino. Esse dispositivo encaminha ou direciona pacotes de dados entre redes de computadores, geralmente funcionando como uma ponte entre redes diferentes. Hoje em dia, 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.

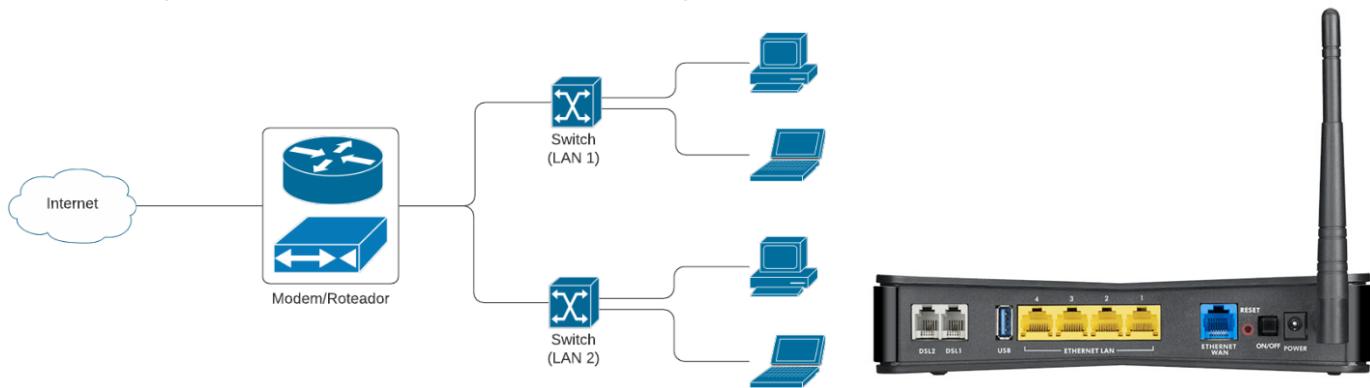


Atualmente, nós estamos na era dos combos, isto é, um único provedor fornece Internet, Telefone e TV a Cabo (Ex: NET/Claro, GVT/Vivo, etc). Nesse caso, um único aparelho condensa as funções de modem e roteador – você provavelmente tem esse aparelho na sua casa! Em geral, um cabo coaxial branco entra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

(Prefeitura de João Pessoa/PB – 2016) Um equipamento de rede que permite que computadores de uma rede possam se conectar a Internet é o:

- a) HCD.
- 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).

(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).

Modem

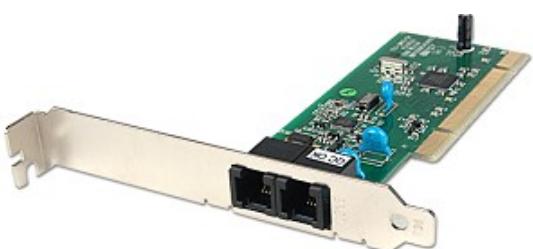
INCIDÊNCIA EM PROVA: MÉDIA



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 (**Modulador/Demodulador**). 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 transmitida 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 Modems ADSL.**

Empresas de telefonia fixa ofereciam acesso em banda larga³ 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?*

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...

³ Banda é a quantidade de bits que podem trafegar por uma conexão em uma determinada unidade de tempo, isto é, velocidade (Ex: 100Mbps).

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).

(Correios – 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: o modem pode auxiliar na comunicação entre computadores através da rede telefônica – nenhum dos outros itens faz qualquer sentido (Letra E).

(DEPEN – 2013) 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.** Na tabela a seguir, é possível ver diversos padrões diferentes de redes de computadores:

PADRÃO	NOME
IEEE 802.3	Ethernet (LAN) ¹
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)

(UFMA – 2016) Considerando os padrões Ethernet em uso utilizados pela maioria das tecnologias de rede local, permitindo que a integração de produtos de diferentes fabricantes funcionem em conjunto. Qual das alternativas diz respeito ao padrão 802.11?

- a) Redes Token King
- b) redes Wi-Fi
- c) redes Cabeada
- d) redes bluetooth
- e) Redes WIMAX

Comentários: o Padrão 802.11 se refere a Redes Wi-Fi (Letra B).

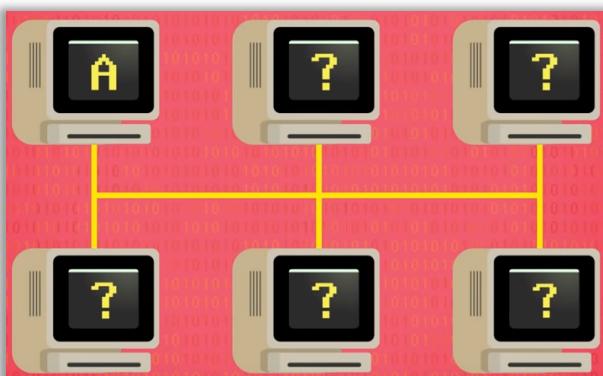
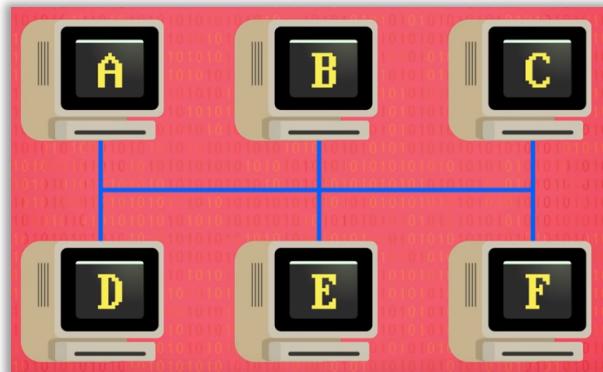
¹ Sendo rigorosamente técnico, há uma diferença entre IEEE 802.3 e Ethernet relacionado a um campo de endereço de origem e destino, mas eu só vi essa diferença ser cobrada em prova uma vez até hoje. Além disso, para lembrar da numeração do Padrão Ethernet, lembre-se de: **ETHERNET → 3TH3RN3T**; e para 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?

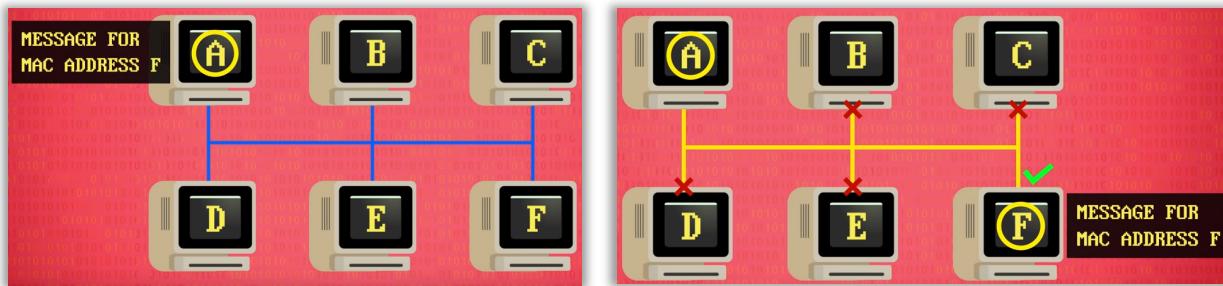


Na imagem acima, temos o *backbone* em azul porque nenhum sinal está sendo transmitido; e na imagem abaixo, temos o *backbone* em amarelo onde o sinal está sendo transmitido. **Notem que o *backbone* está todo amarelo porque – como a transmissão ocorre em broadcast – todas as máquinas o recebem.** Por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

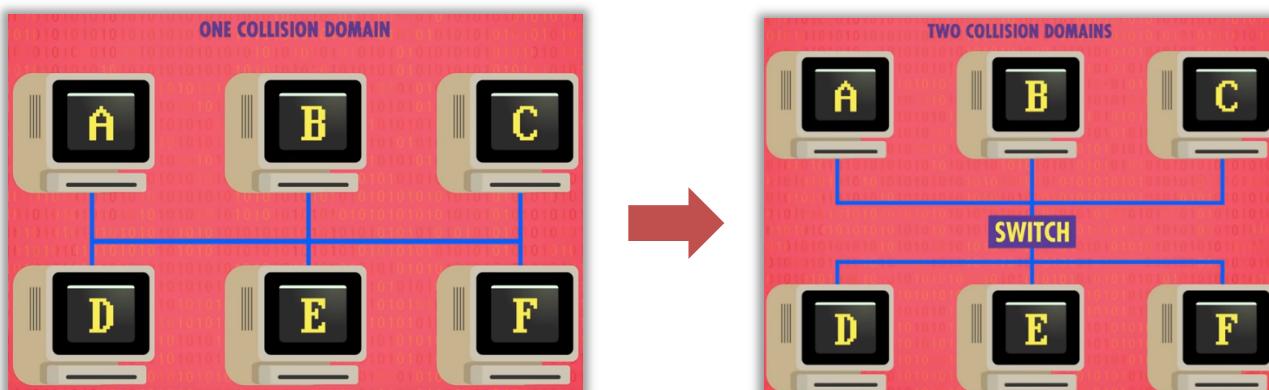
Esse período poderia ser, por exemplo, um segundo! *Professor, se todos os computadores esperarem um segundo, isso não vai resultar no mesmo problema anterior?* Você está esperto, meu caro! Isso é verdade, se todos esperarem um segundo para retransmitir, eles vão colidir novamente após um segundo. **Para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

Lembrem-se 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 se tivermos muitos computadores não resolverá o problema!*

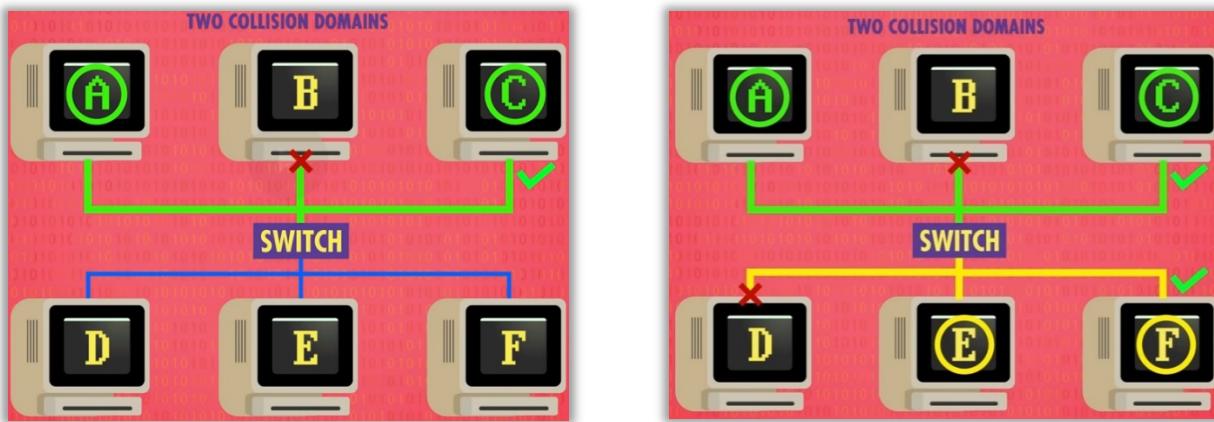
Para resolver esse problema, nós temos mais um truque! Sabemos que se um computador detecta uma colisão, ele esperará um segundo mais um tempo aleatório. Se mesmo assim houver outra colisão, pode ser que a rede esteja congestionada, logo ele não esperará mais um segundo, esperará dois segundos. Se mesmo assim houver colisão, esperará quatro segundos. **Se continuar havendo colisões, esperará oito segundos, e assim por diante até conseguir transmitir.**

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

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

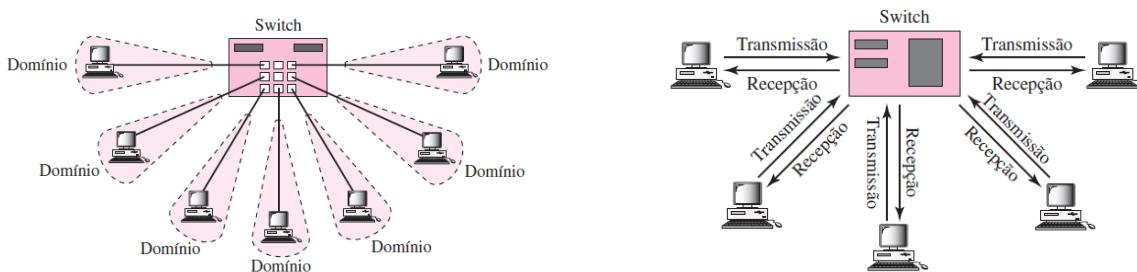


No exemplo anterior, nós tínhamos seis computadores conectados em um único meio de transmissão compartilhado, logo nós tínhamos um único domínio de colisão. Para reduzir a probabilidade de colisões, nós podemos segmentar a rede em dois domínios de colisão. *Como, Diego?* Nós podemos utilizar uma topologia em estrela com uso de um switch². **Ele segmentará nossa rede em duas partes e ficará posicionado entre elas.**



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



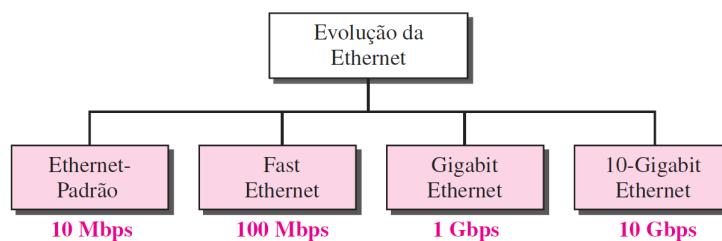
E digo mais: é possível criar um domínio de colisão para cada uma das portas de um switch (conforme apresenta à esquerda). Dessa forma, é possível eliminar toda e qualquer colisão! **Além disso, lembremos que o switch trabalha em full-duplex, ou seja, é capaz de enviar e receber**

² Utilizar a topologia em estrela com um hub não adiantaria nada porque esse dispositivo tem topologia lógica em barramento.

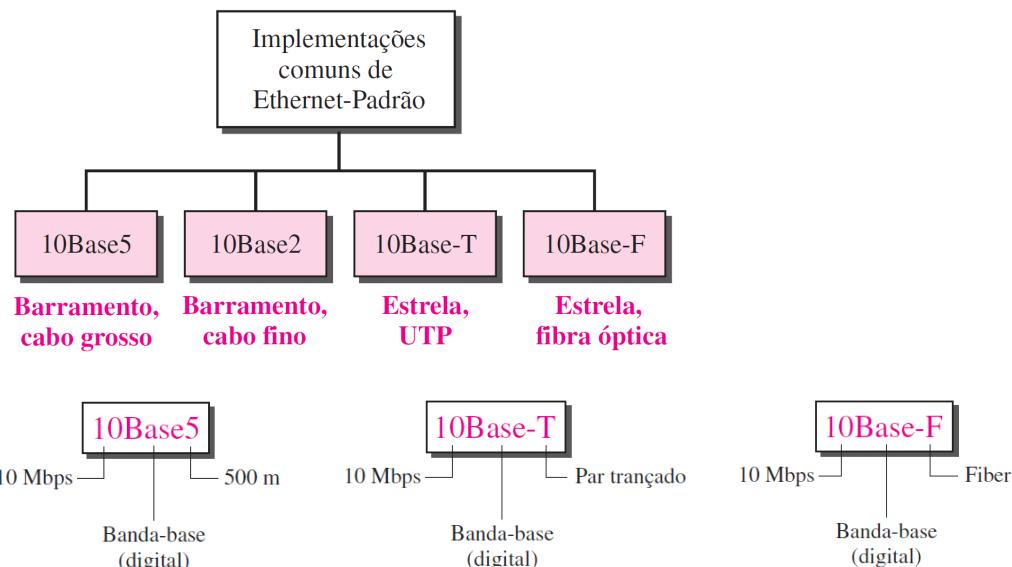
dados simultaneamente, logo não há nenhuma chance de haver colisões! A probabilidade foi reduzida à zero e o nosso problema foi resolvido! :)

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

Para superar essa limitação, podemos utilizar a topologia em estrela com um switch. Por que? 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 à 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



Como 1 bilhão = 1000 milhões, então 1G = 1000M. Dessa forma, fica mais fácil lembrar que a Gigabit Ethernet tem a velocidade de 1000Mbps e que a 10G Ethernet tem a velocidade de 10.000Mbps (lembrando também que MEGA (M) = Milhão e GIGA (G) = Bilhão).

(SEFAZ/RJ – 2008) Uma rede de microcomputadores opera com base no padrão Ethernet IEEE-802.3 e utiliza o protocolo CSMA/CD. No momento em que uma colisão é detectada, as máquinas que estão transmitindo executam o seguinte procedimento:

- a) aceleram o ritmo de transmissão.
- b) param imediatamente de transmitir.
- c) passam a transmitir em modo half-duplex.
- d) retransmitem os frames que provocaram a colisão.
- e) enviam pacotes de sincronismo para as demais máquinas.

Comentários: a regra é parar imediatamente de transmitir e aguardar uma fração de tempo aleatória para reiniciar a transmissão (Letra B).

(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 a Fast Ethernet (Letra B).

Padrão Token Ring (IEEE 802.5)

INCIDÊNCIA EM PROVA: MÉDIA

O Padrão Token Ring é outro padrão cabeados 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*. **Pronto, descobrimos por que se chama Token Ring.**

(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).

(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: esse símbolo (que nós chamamos de envelope) que, na realidade, é um arquivo é o token. Logo, estamos falando do Padrão Token Ring (Letra E).

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 fornece mobilidade aos usuários. **O Padrão Wi-Fi se baseia em uma conexão que utiliza infravermelho ou 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...

RISCOS DE REDES WIRELESS

Por se comunicarem por meio de sinais de rádio, não há a necessidade de acesso físico a um ambiente restrito, como ocorre com as redes cabeadas. Por essa razão, dados transmitidos por clientes legítimos podem ser interceptados por qualquer pessoa próxima com um mínimo de equipamento (Ex: um notebook ou tablet).

Por terem instalação bastante simples, muitas pessoas as instalam em casa (ou mesmo em empresas, sem o conhecimento dos administradores de rede), sem qualquer cuidado com configurações mínimas de segurança, e podem vir a ser abusadas por atacantes, por meio de uso não autorizado ou de "sequestro".

Em uma rede wireless pública (como as disponibilizadas – por exemplo – em aeroportos, hotéis, conferências, etc) os dados que não estiverem criptografados podem ser indevidamente coletados e lidos por atacantes.

Uma rede wireless aberta pode ser propositadamente disponibilizada por atacantes para atrair usuários, a fim de interceptar o tráfego (e coletar dados pessoais) ou desviar a navegação para sites falsos.



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

Para resolver alguns destes riscos foram desenvolvidos mecanismos de segurança, como:

- **WEP (Wired Equivalent Privacy):** primeiro mecanismo de segurança a ser lançado – é considerado frágil e, por isto, o uso deve ser evitado;
- **WPA (Wi-Fi Protected Access):** mecanismo desenvolvido para resolver algumas das fragilidades do WEP – é o nível mínimo de segurança que é recomendado atualmente;
- **WPA-2 (Wi-Fi Protected Access 2):** similar ao WPA, mas com criptografia considerada mais forte – é o mecanismo mais recomendado atualmente.

Galera, é importante também notar que redes wireless podem trabalhar em dois modos: **Ad-hoc** ou **Infraestrutura**. Vejamos:

- a) **Ad-Hoc:** comunicação direta entre equipamentos e válida somente naquele momento, conexão temporária, apresentando alcance reduzido (Ex: 5m). Em outras palavras, não é necessário nenhum equipamento central para intermediar a comunicação.
- b) **Infraestrutura:** 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). Em outras palavras, toda comunicação entre equipamentos deve passar pelo Access Point.

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-hoc³.**

EVOLUÇÃO DO PADRÃO WI-FI (802.11) ⁴		
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	2.4 ou 5.0 Ghz	3.5 Gbps a 14 Gbps

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 que, professor? Porque alguns aparelhos domésticos como controle de garagem, micro-ondas e bluetooth⁵ trabalham na frequência de 2.4Ghz – isso poderia causar problemas de interferência. Como alternativa, ele pode trabalhar em outra frequência de onda de rádio!

Por fim, o Padrão 802.11ac é uma novidade e pode vir a ser uma solução para tráfegos de altíssima velocidade, com taxas superiores a 1Gbps.

(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: está tudo impecável. 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).

³ Em geral, Bluetooth tem um caráter mais ad-hoc e Wi-Fi tem um caráter mais de infraestrutura (apesar de não ser obrigatório).

⁴ Para decorar a ordem, lembre-se da palavra **BAGUNÇA** (lembrando que CA é AC).

⁵ 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

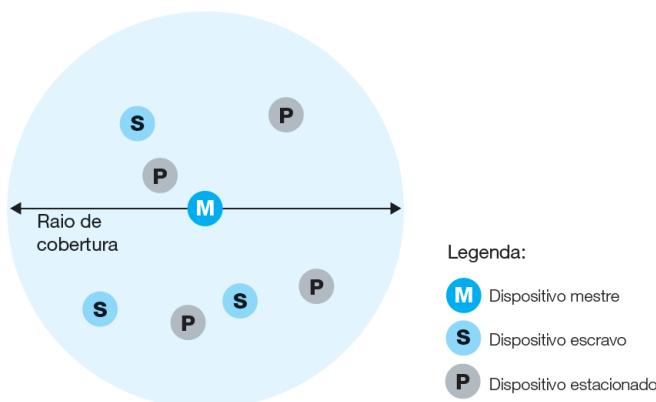


O Padrão Bluetooth tem o objetivo de integrar equipamentos periféricos. **Utilizado em Rede WPAN (Wireless Personal Area Network) – eles padronizam uma rede de baixo custo, curto alcance, baixas taxas de transmissão e sem fio.** Eles operam na faixa de 2.4 Ghz de forma ad-hoc por meio de sua unidade 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.

Uma piconet possui uma topologia em estrela e uma configuração ou arquitetura do tipo Mestre-Escravo⁶. No centro dessa estrela, um dispositivo mestre (também chamado de *master* ou primário) coordena a comunicação com até outros sete dispositivos escravos (também chamados de *slave* ou secundários). Um dispositivo *bluetooth* pode desempenhar qualquer um dos papéis, mas em uma piconet só pode haver um dispositivo mestre.

Além dos dispositivos escravos, a piconet também pode conter até 255 dispositivos estacionados. **Como assim, Diego?** Um dispositivo estacionado não pode se comunicar até que o dispositivo mestre altera 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.**

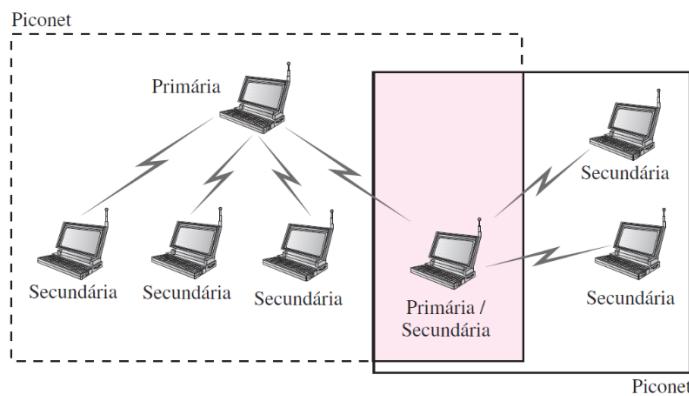
Como apenas oito estações podem estar ativas ao mesmo tempo em uma piconet, retirar uma estação do estado estacionado significa que uma estação ativa terá de ir para o estado estacionado. **Em suma, uma piconet é um conjunto de oito dispositivos: 1 mestre, até 7 escravos e até 255 estacionados.** Vejam na imagem seguinte um esquema em um dispositivo mestre tem um raio de cobertura com três dispositivos escravos e quatro dispositivos estacionados.



E se eu disser para vocês que um dispositivo pode ser escravo em uma piconet e mestre em outra piconet? Pois é, quando redes piconets se combinam, forma-se uma scatternet. Vejam no

⁶ 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.

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 até outros sete 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...**

Agora para fechar, 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

(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).

Padrão WiMAX (IEEE 802.16)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

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

Opera em faixas licenciadas do espectro de frequência (2,5GHz, 3,5GHz, 10,5GHz), portanto é necessário que empresas adquiram a concessão junto à ANATEL (Agência Nacional de Telecomunicações) para oferecer esse serviço. A potência percebida na estação-base, que oferecerá o serviço, pode ter uma grande variação, o que influencia a relação sinal/ruído e, por isso, a tecnologia possui três esquemas de modulação (QAM-64, QAM-16 e QPSK).

(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).

(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).

(TJ/PB – 2012) Padrão responsável pela tecnologia WiMAX, é o:

- a) IEEE 802.3.
- b) IEEE 802.11.
- c) IEEE 802.15.
- d) IEEE 802.16.

Comentários: WiMAX = IEEE 802.16 (Letra D).

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 que?* 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.**

(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 amigo¹. **Essa comunicação funcionava por meio da comutação por circuito!**

¹ 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 que, 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.

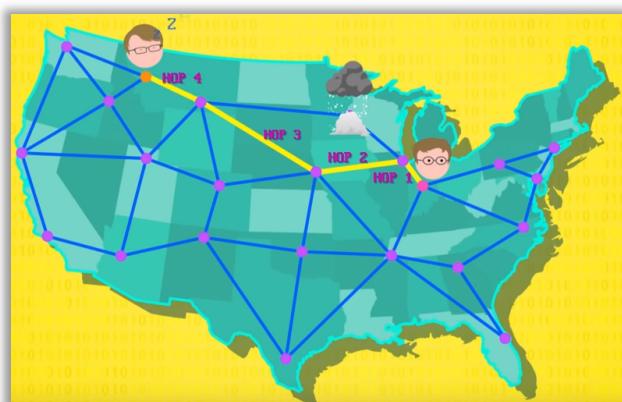
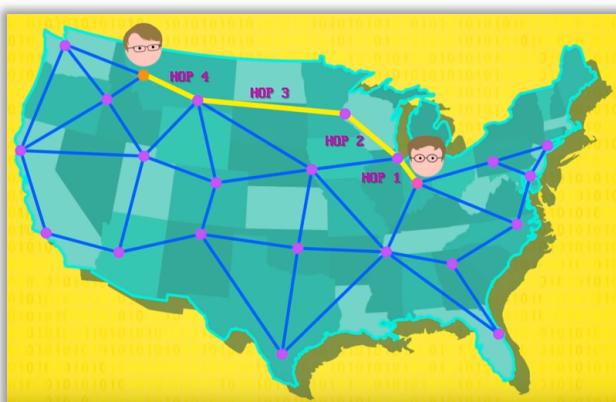
Além disso, a comutação por circuito só permite que eu telefone para uma única pessoa simultaneamente – eu não consigo conversar com dois amigos simultaneamente. *Já imaginaram se a internet funcionasse assim?* Nesse caso, seu computador só poderia se conectar a um único dispositivo ao mesmo tempo. **Seria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

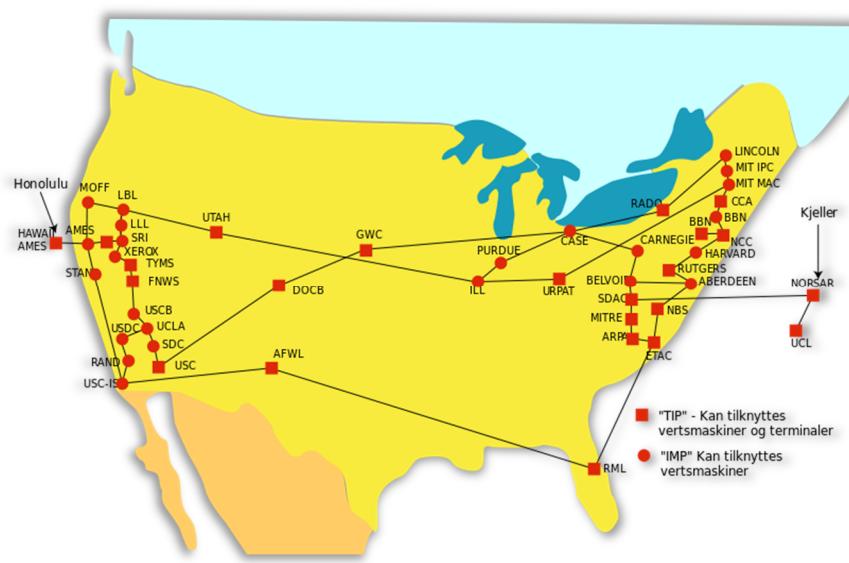


Quando se envia dados pela internet, não é possível prever o caminho percorrido pelo pacote até chegar ao seu destino final. Cada pacote enviado pode seguir por uma rota diferente chegando em ordem diferente da ordem enviada (claro que, após todos os pacotes chegarem, o arquivo é remontado na forma original). 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).

(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).

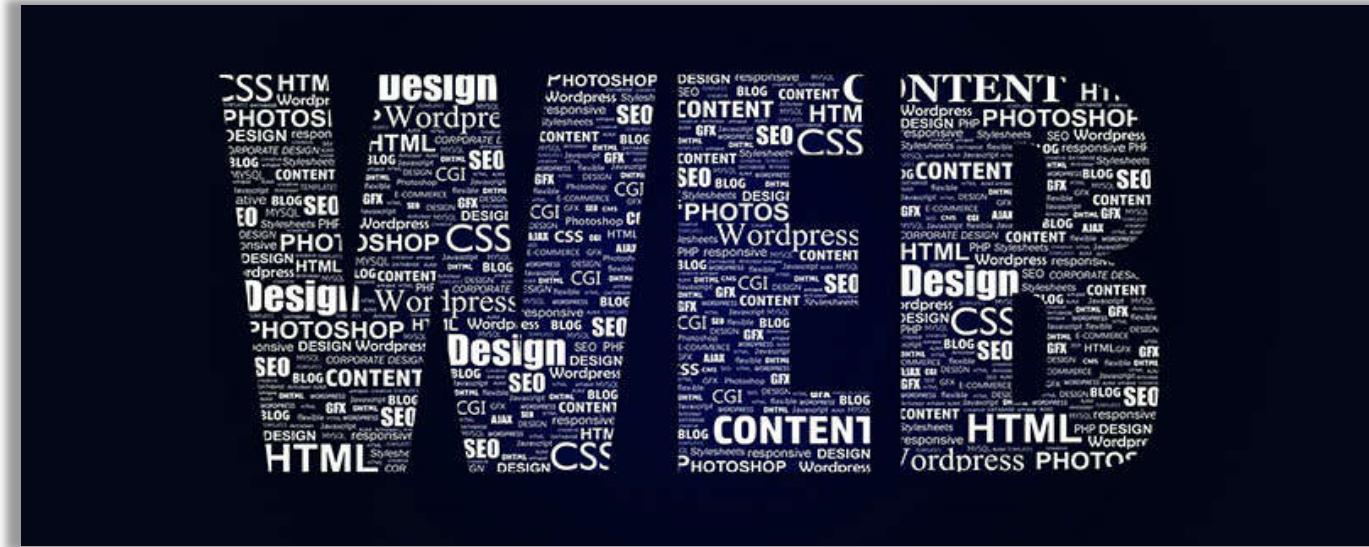
(Ministério da Integração – 2012) Os serviços de Internet mais populares e difundidos são:

- 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).

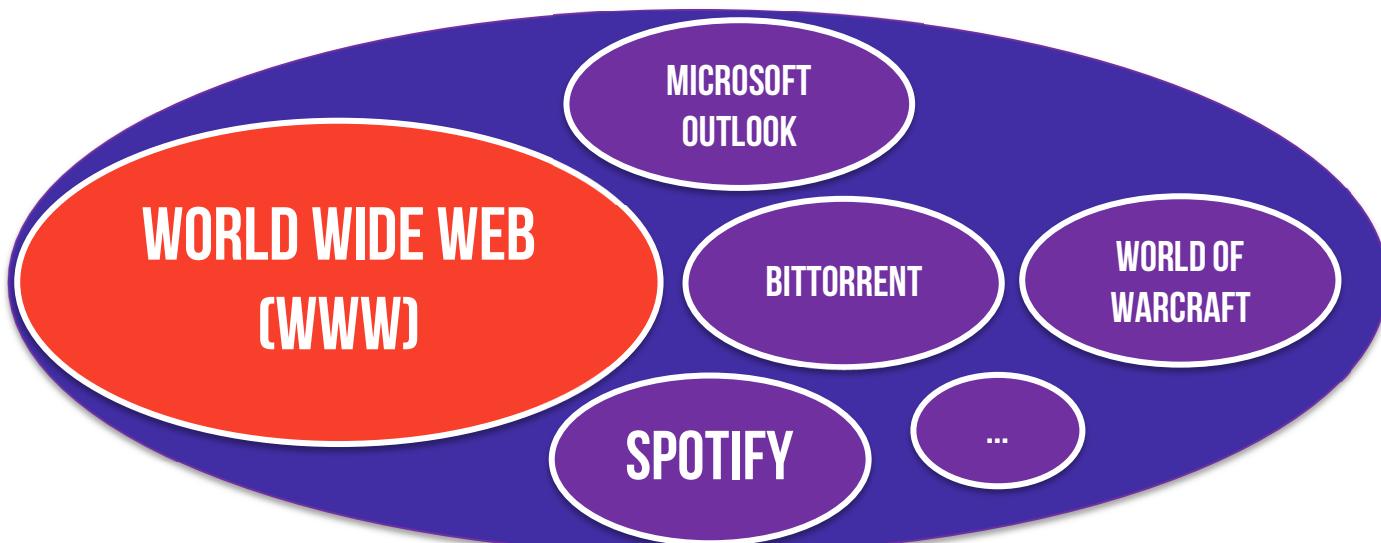
Web (WWW)

INCIDÊNCIA EM PROVA: BAIXA



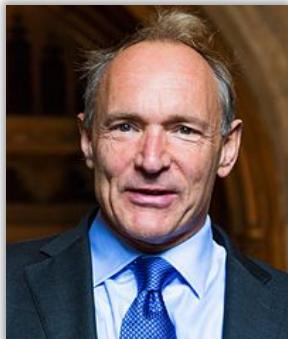
Web é uma contração do termo World Wide Web (WWW). Ah, professor... você tá falando de *internet*, não é? Não! Muito cuidado porque são coisas diferentes! **A internet é uma rede mundial de computadores que funciona como uma estrutura que transmite dados para diferentes aplicações** (Instagram, Skype,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

Professor, ainda não entendi a diferença entre Internet e Web! Galera, a internet é a plataforma que permite a execução de diversas aplicações e a web é simplesmente uma delas. Podemos dizer que se você está acessando por meio de um navegador, trata-se de uma aplicação web. Caso contrário, é somente outra aplicação que roda na internet (Ex: Jogos, BitTorrent, Photoshop, Microsoft Outlook, entre outros).



Vamos falar um pouco agora sobre as gerações da web. Pessoal, as gerações da web 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](http://info.cern.ch/hypertext/www/theproject.html)

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.

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

Web 1.0

A Web 1.0 foi marcada por sites com conteúdos estáticos, produzidos maioritariamente por empresas e instituições, com pouca interatividade entre os internautas. Altavista, Geocities, Yahoo, Cadê, Hotmail eram as grandes estrelas da internet. Era caracterizada pela baixa interação do usuário, permitindo pouca ou nenhuma interação – como por exemplo – deixar comentários ou manipular e criar conteúdos.

As tecnologias e métodos da Web 1.0 ainda são utilizadas para a exibição de conteúdos como leis e manuais. Essa geração foi marcada pela produção centralizada de conteúdos – como os diretórios e portais (Ex: UOL, ZAZ, Terra, AOL). **Nesse contexto, o usuário era responsável pela navegação e localização de conteúdos relevantes por sua própria conta tendo predominantemente uma atuação passiva em um processo onde poucos produzem e muitos consomem.**

Era algo muito parecido com o modelo de broadcasting da indústria midiática como TV, rádio, jornais e revistas – sua grande virtude foi a democratização do acesso à informação.

Web 2.0

Esse termo foi criado em 2003 para designar uma segunda geração de comunidades e serviços baseados na plataforma web. **Não há grandes mudanças tecnológicas, mas – sim – um foco maior na forma como a web é encarada pelos usuários e desenvolvedores.** Os programas e protocolos são os mesmos, porém o foco passa para a integração dos usuários junto às informações dos sites, sendo marcada por páginas que permitem ao próprio usuário inserir conteúdo.

A Web 2.0 também foi a revolução dos blogs e chats, das mídias sociais colaborativas, das redes sociais e do conteúdo produzido pelos próprios internautas. Nesse momento, a internet se popularizou em todo o mundo, e começou a abranger muito mais do que algumas empresas para se tornar obrigatória para qualquer um que queira ter sucesso no mercado. São exemplos: Facebook; Google+; Linkedin; Instagram; Tumblr; Youtube; Blogs; Wikis; entre outros.

Os sites criados para esse momento da internet já não são estáticos e possuem um layout claramente focado no consumidor e também na usabilidade dos buscadores. Nesse momento, a navegação mobile e uso de aplicativos já tem forte presença no dia a dia das pessoas. Outra recomendação é a utilização de uma combinação de tecnologias já existentes (Web Services, AJAX, etc) e de uso simplificado que aumentem a velocidade e a facilidade de uso de aplicações web.

Busca-se ampliar o conteúdo existente na Internet para permitir que usuários comuns publiquem e consumam informação de forma rápida e constante. **A Web 2.0 em contraste à Web 1.0, tem seu conteúdo gerado predominantemente por seus usuários em um processo onde muitos produzem e todos consomem.** Nesse contexto, houve uma demanda por avanços tecnológicos em mecanismos de busca devido ao imenso volume de conteúdo produzido.

Web 3.0

Permite que palavras e figuras sejam organizadas de várias fontes diferentes para tornar a vida de seus usuários mais simples. Seu propósito é permitir que o usuário acesse informações com menos cliques ou reúna interesses de maneira intuitiva. A Web 3.0 é composta de dados onipresentes, conectados e capazes de serem reagrupados sob demanda. **Capaz de oferecer uma inteligência simulada, busca entender o que o usuário deseja através de algoritmos semânticos.**

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, todos as notícias que você já, todo material do Estratégia, Google, Wikipedia, etc... **tudo isso corresponde somente a cerca de 4% da web!**



Galera, 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.

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!*

(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 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 que podem ser utilizados para descobrir quem está acessando e o que está acessando.

The screenshot shows a news article from G1's Technology and Games section. The header includes the G1 logo and navigation links for 'MENU' and 'TECNOLOGIA E GAMES'. The date and time are listed as '19/07/2016 11h28 - Atualizado em 19/07/2016 17h08'. The main title of the article is 'WhatsApp: Justiça do RJ manda bloquear aplicativo em todo o Brasil'. Below the title, a subtitle reads: 'Facebook recusou ceder informações para uma investigação policial. Operadoras de telefonia foram notificadas para suspender acesso ao app.' At the bottom, there is a note: 'Do G1, em São Paulo e no Rio' and social media sharing icons for Facebook, Twitter, Google+, and Pinterest.

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 fazer isso ilegítimos. A China, por exemplo, proíbe seus cidadãos de acessarem o Google, Facebook, Youtube, Twitter, etc.

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 comum¹, 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).

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**². 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.

(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.

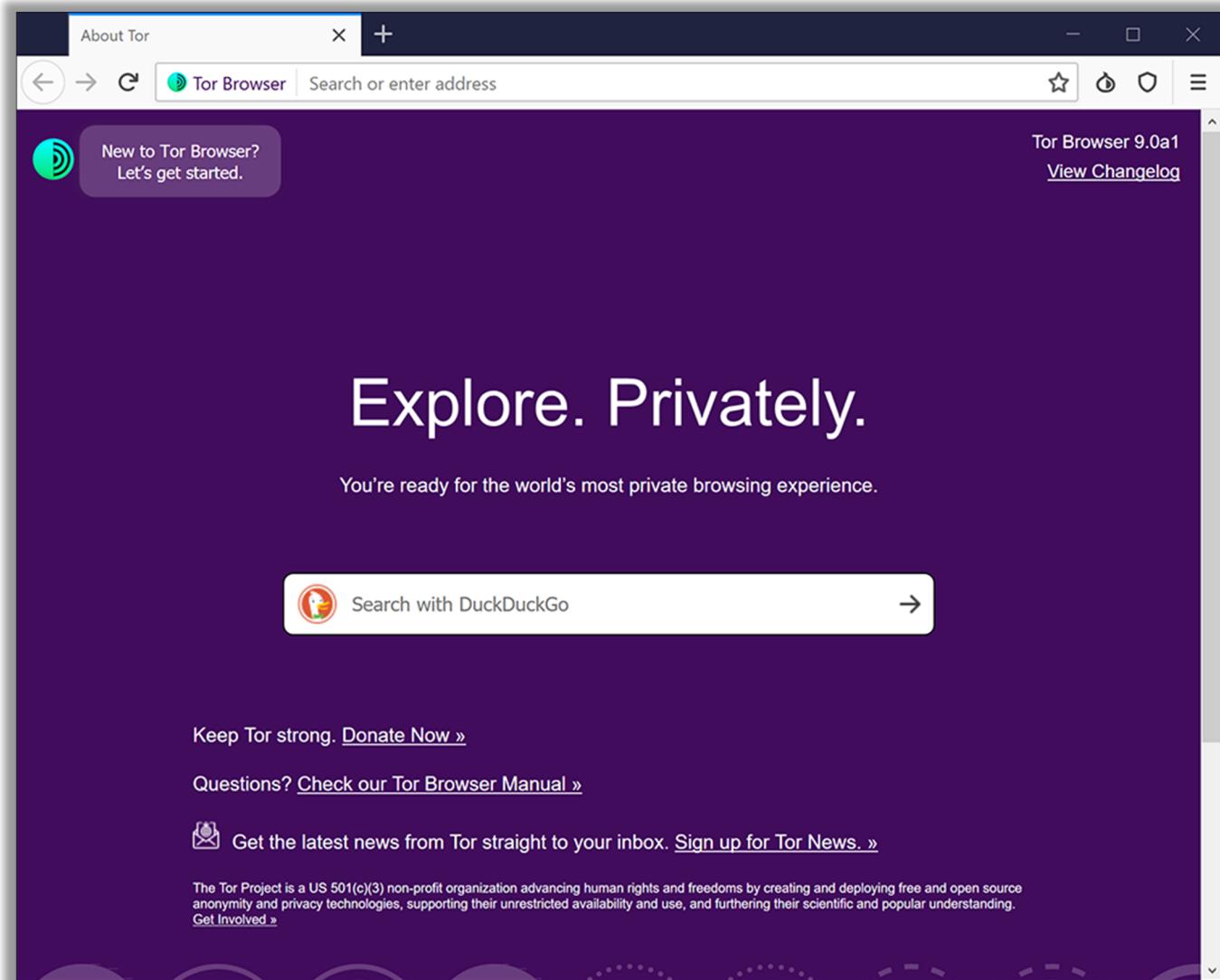
Comentários: vamos analisar por partes - *O aplicativo Tor permite o acesso a sítios na Deep Web?* Sim, ele permite o acesso a sítios da Surface Web, Deep Web e Dark Web. *Sítios da Deep Web não possuem conteúdo disponibilizado em mecanismos de busca?* Perfeito, eles não podem ser indexados por mecanismos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

¹ Exemplo: <http://3g2upl4pq6kufc4m.onion> ou <http://msydqstlz2kzerdg.onion>.

² O nome **Tor** vem de **The Onion Router** (O Roteador Cebola) porque os dados passam por diversas camadas de encriptação como em uma cebola.

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.



(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,

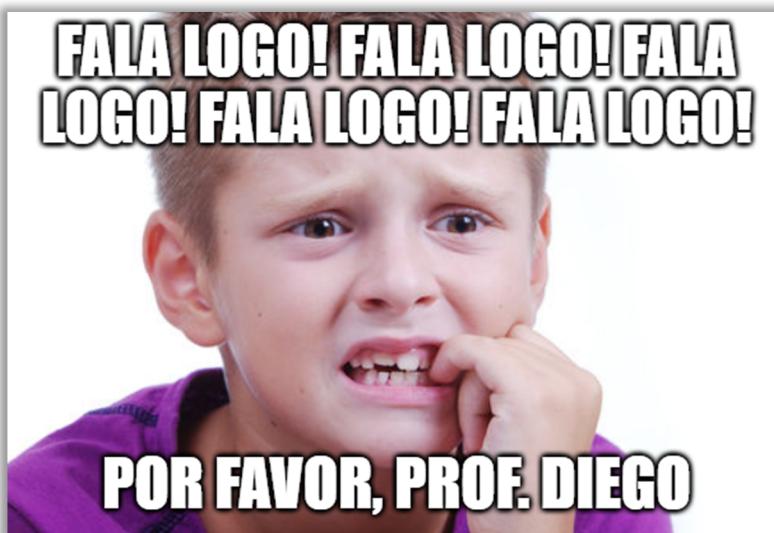
- I. Tor é um browser web que permite navegar na rede TOR.
- II. Para navegar na rede TOR, pode-se utilizar quaisquer browsers web, tais como Firefox e Chrome, configurando propriedades de proxy.
- III. Existe a possibilidade de trafegar dados na rede TOR de forma criptografada.

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.

(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 desregimento, e está repleta de atividades ilegais.

Comentários: perfeito, perfeito, perfeito... lembrem-se que a parte da Deep Web que, longe da vigilância pública, foi tomada por atividades ilegais é a Dark Web (Correto).

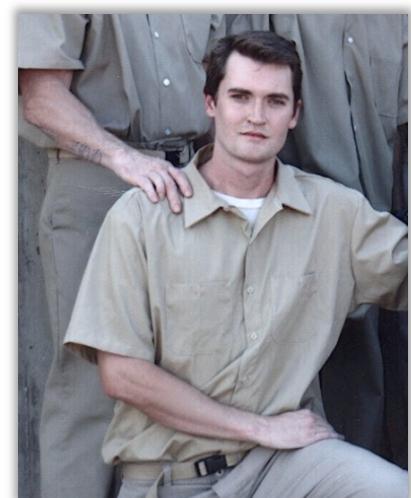
Eu sei que essa aula atiça a curiosidade de várias pessoas, mas eu já adianto que não recomendo que vocês acessem esses sites. Saibam que se trata de um ambiente em que é possível encontrar um bocado de hackers, cibercriminosos e outros profissionais desse tipo. Eu já recebi perguntas de alunos perguntando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

The screenshot shows the Silk Road website interface. At the top, there's a logo of a camel and the text "Silk Road anonymous marketplace". The header also includes "Welcome OzFreelancer!", "messages(0)", "orders(0)", "account(\$0.00)", "settings", and "log out". Below the header, there's a search bar and a shopping cart icon. On the left, a sidebar lists categories under "Shop by category": Drugs (1582), Cannabis (271), Dissociatives (33), Ecstasy (217), Opioids (106), Other (65), Prescription (274), Psychedelics (306), Stimulants (190), Apparel (37), Art (1), Books (300), Computer equipment (9), Digital goods (218), Drug paraphernalia (33), Electronics (13). The main content area displays several product listings with images, names, descriptions, and prices in Bitcoin (BTC):

- 10 Grams high grade MDMA 80+% **B61.17**
- Amphetamines sulfate / Speed freebase... **B28.59**
- 2g Jack Frost (weed) *420 SALE**** **B8.54**
- 5 Grams of pure MDMA crystals **B42.04**
- Dr Amsterdam **B97.77**
- Michael Jackson **B2.52**

On the right side, there's a "News:" section with links to various news items.



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.**

Fóruns na dark web incitam violência e mortes e desafiam polícia

Massacre em Suzano foi comemorado em comunidades virtuais de criminosos

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.

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 :)

(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).

(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 termina com .onion e, não, .on (Errado).

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:

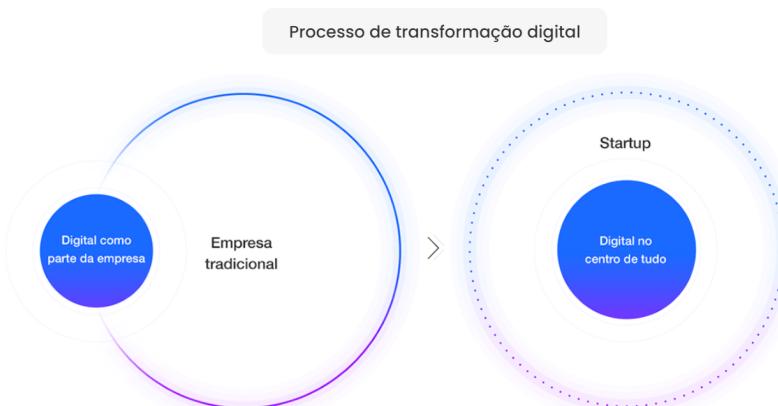
Diga a verdade ... quantos de vocês realmente poderiam passar o dia sem o smartphone?

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 com papel essencial para seu sucesso. Vejam a imagem a seguir:

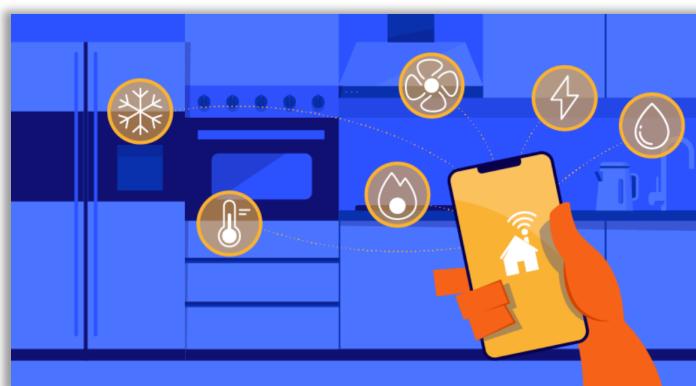
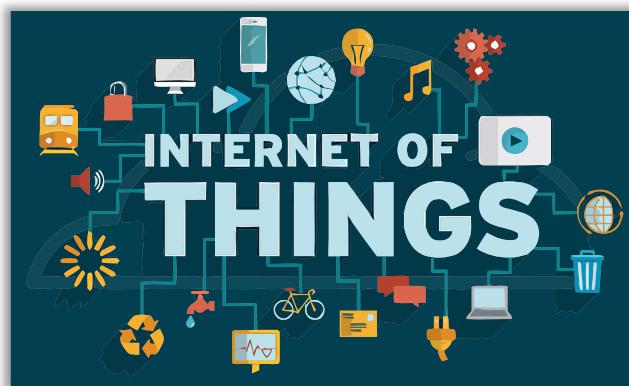


Galera, não há como fugir da transformação digital! *Querem um exemplo óbvio? Eu estou desde o início da pandemia de coronavírus trabalhando remotamente. O vírus basicamente acelerou de forma brutal o processo de transformação digital de órgãos e empresas – talvez, inclusive, de*

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...**

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, etc.



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.

Professor, quais tecnologias são utilizadas? Existem basicamente três componentes: dispositivos, redes de comunicação e sistemas de controle. Os dispositivos, em regra, são equipados com microchips, sensores ou outros recursos de comunicação e monitoramento de dados. Já as redes de comunicação também são conhecidas: Wi-Fi, Bluetooth, NFC, 4G, 5G, etc. Por fim, temos os sistemas de controle...

Ora, não basta que o dispositivo se conecte à internet ou troque informações com outros objetos – **os dados precisam ser processados pelos sistemas de controle, ou seja, devem ser enviados a um sistema que os trate.** Qual, professor? Aí dependerá da aplicação! 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.

(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: essa questão foi considerada correta, mas evidentemente está errada e o examinador não conhece muito bem a língua portuguesa. A evolução do IPv4 para o IPv6 vai ao encontro das tendências da IoT e, não, de encontro à (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 (WAN), 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. *Fechou?*

(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: um detector de fumaças que pode ser acionado via smartphone seria uma solução de IoT (Correto).

Tecnologias de Acesso

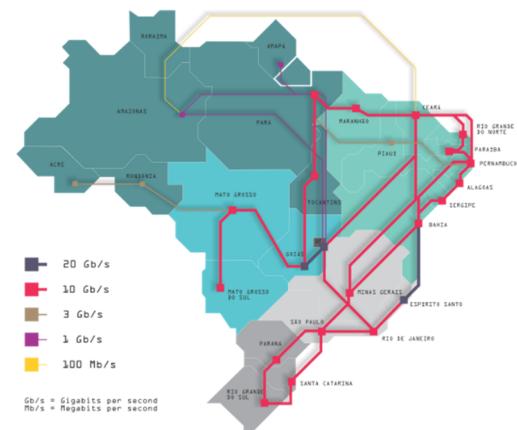
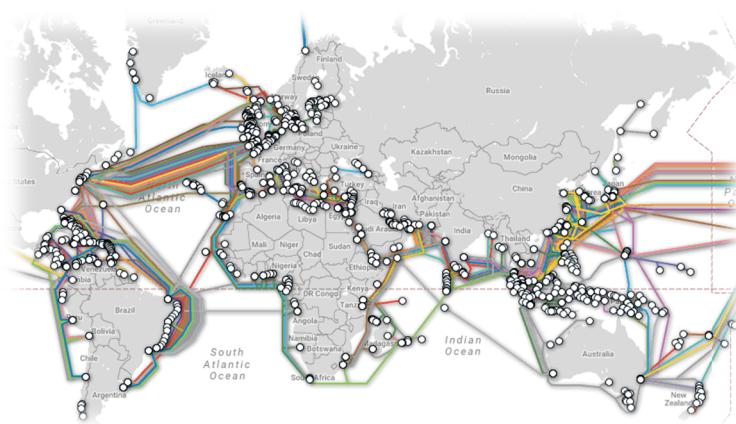
Galera, até o início da década de noventa, só quem sabia o que era internet eram pesquisadores ligados a universidades, ao governo ou à indústria. No entanto, quando um físico chamado Tim Berners-Lee criou a Web (WWW), houve uma mudança nessa realidade e a internet ganhou milhões de novos usuários sem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

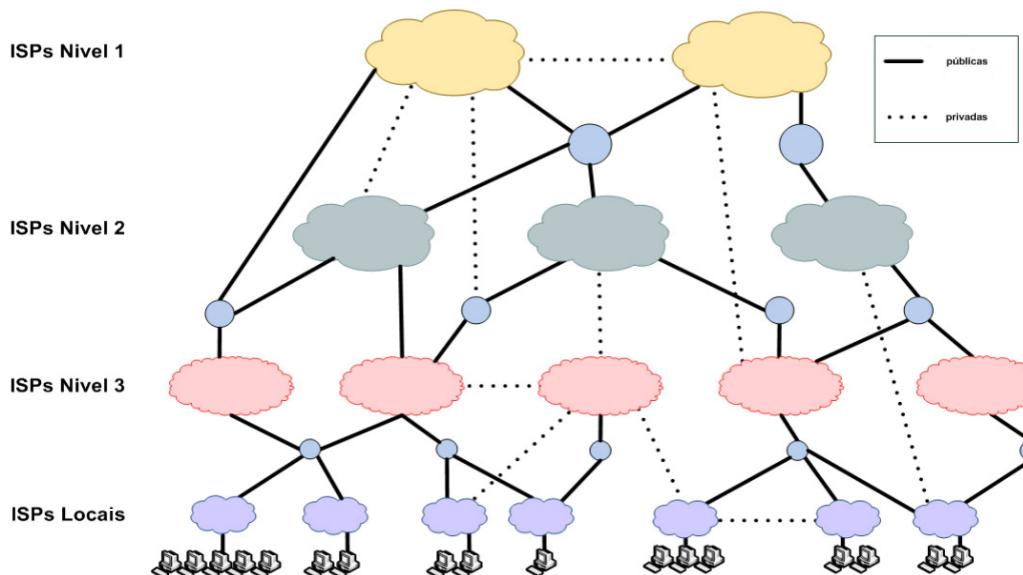
Vamos detalhar isso melhor! A internet pode ser fornecida por meio de satélites, ondas de rádio ou uma rede de milhares de cabos de fibra óptica terrestres ou submarinos, que conectam diversos países, respondendo por 80% de toda a comunicação. **Essa infraestrutura de redes – que forma a espinha dorsal da internet – é chamada de Backbone. Ela possui alto 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 hierarquia entre provedores de acesso: ISP Nível 1 tem cobertura internacional, conectando países ou continentes; ISP Nível 2 tem cobertura nacional, conectando um ou mais ISP Nível 1 e oferecendo serviços a vários ISP Nível 3; e ISP Nível 3 tem cobertura regional – conectando pessoas, casas, escritórios ou conectando provedores locais (aquele que só existe na sua cidade especificamente).



(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: redes de acesso situadas na borda da internet realmente são conectadas ao restante da rede segundo uma hierarquia de níveis de ISP (*Internet Service Provider*). Além disso, conforme vimos na figura acima, os ISP Nível 1 estão realmente no topo dessa hierarquia (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:

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!

(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.

200 Mega

WI-FI Grátis

R\$ 99,99/mês

Assine já

Serviços Digitais
+2

Download até 200 Mbps
Upload até 100 Mbps

Assistência
Vivo Home Assist

200 Mega

Ideal para 7 a 10 dispositivos

Você e sua família podem ver vídeos e filmes em 4K, jogar online e fazer downloads. Tudo ao mesmo tempo.

De R\$119,90
R\$ 99,90/MÊS

No Débito em Conta e Conta Digital.

CONSULTAR DISPONIBILIDADE

Informações da oferta:

- ✓ Fixo Ilimitado
- ✓ Modem WiFi UP
- ✓ Instalação grátis
- ✓ 60 Mega de upload

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 anterior 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 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.***

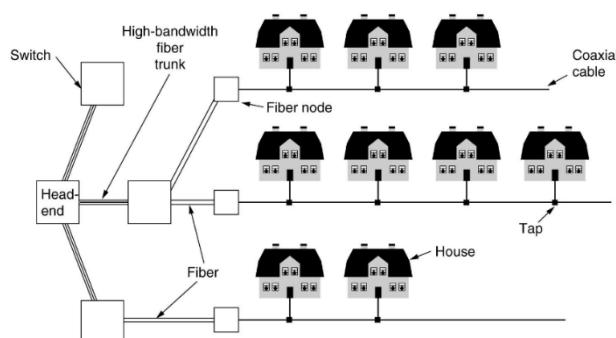
(UFVJM/MG – 2017) Assinale a alternativa que apresenta a sigla que representa uma tecnologia com finalidade de permitir o uso de linha telefônica para transmissão digital de dados em alta velocidade.

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.



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.

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. *Conta aí, você já tem na sua região?*

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.

(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 impedimento; 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.**

(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

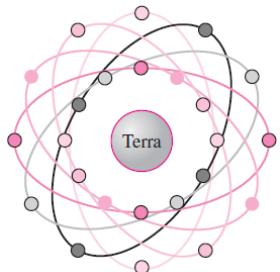
- d) Cabo coaxial
- e) Rede elétrica

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.**

(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 até chegar aos brasileiros.** Vejamos as principais gerações de telefonia celular:

GERAÇÃO	DESCRIÇÃO
1ª 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).
2ª GERAÇÃO (2G)	Para oferecer comunicação de voz de maior qualidade em sistemas móveis (sujeito a menos ruídos) foi criada a segunda geração da rede de telefonia celular. Enquanto a primeira geração foi projetada para comunicação de voz analógica, a segunda foi projetada em grande parte visando voz digitalizada. Essa geração é baseada na tecnologia GSM e – além fornecer serviços de telefonia – permite enviar dados como mensagens de texto (SMS).
2,5ª GERAÇÃO (2,5G)	Baseado na tecnologia GPRS, foi o primeiro sistema de acesso à Internet através de rede celular realmente útil. Apresentava taxas de transmissão similares às de um acesso discado (banda estreita), mas devido à enorme latência na transmissão e ao grande volume de pacotes perdidos e retransmitidos, acabou tendo um resultado bastante inferior. Quando eu vou para o sítio do meu sogro no interior, o 4G do celular é substituído pelo GPRS e a conexão fica extremamente lenta.
3ª GERAÇÃO (3G)	Chegamos na banda larga da telefonia móvel. A terceira geração de telefonia celular se refere a uma combinação de tecnologias que fornece uma série de serviços. Teoricamente, pode fornecer comunicação de voz assim como de dados digitais, isto é, a comunicação por voz via dados com qualidade similar àquela da rede de telefonia fixa. Baseado na tecnologia UMTS, permite teoricamente assistir filmes, ouvir músicas, navegar na Internet, jogar games, fazer uma videoconferência e muito mais.
4ª GERAÇÃO (4G)	Baseado na tecnologia digital LTE (Long Term Evolution), foi disponibilizada no Brasil a partir de 2013, tendo sido implementada com o objetivo de melhorar o padrão UMTS. A principal diferença entre essa geração e a anterior está relacionada a velocidade de transmissão. A tecnologia 3G permite uma conexão com velocidade máxima de 21 Mbps enquanto a tecnologia 4G permite uma conexão com velocidade máxima de 300 Mbps.
5ª GERAÇÃO (5G)	Baseado na tecnologia OFDM, trata-se da próxima geração 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. Enquanto o 4G permite uma conexão com velocidade máxima de 300 Mbps, o 5G pode chegar até 10 Gbps (30 vezes mais rápido).

RESUMO

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.

TIPO DE CONEXÃO	DESCRÍÇÃO
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.

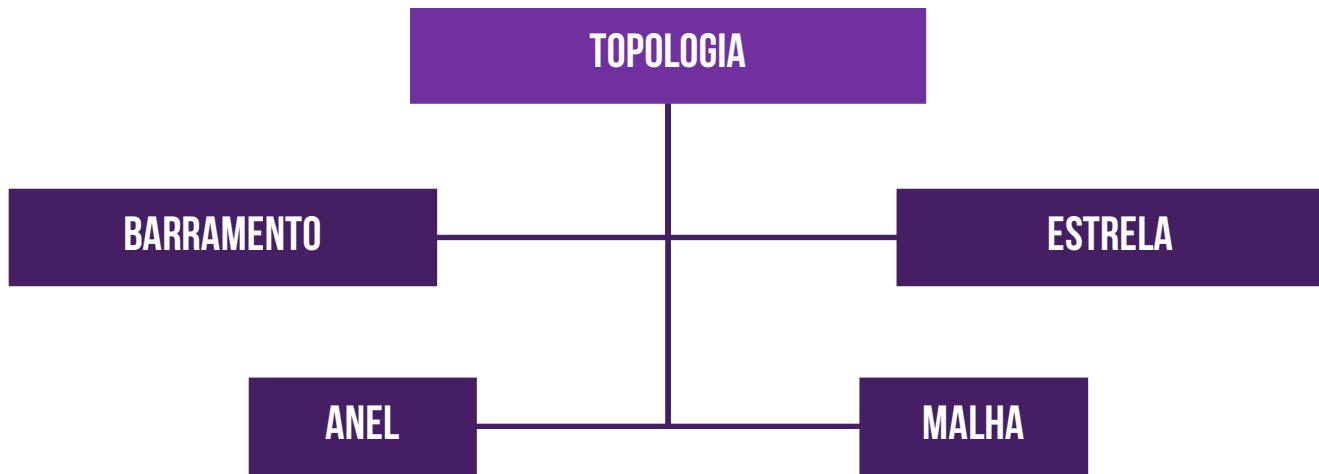
TIPO	REPRESENTAÇÃO	DESCRÍÇÃO
SIMPLEX		Uma comunicação é dita simplex quando há um transmissor de mensagem, um receptor de mensagem e esses papéis nunca se invertem no período de transmissão.
HALF-DUPLEX		Uma comunicação é dita half-duplex quando temos um transmissor e um receptor, sendo que ambos podem 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.

TIPO	REPRESENTAÇÃO	DESCRÍÇÃO
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.

TIPO	SIGLA	DESCRÍÇÃO	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.

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 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.

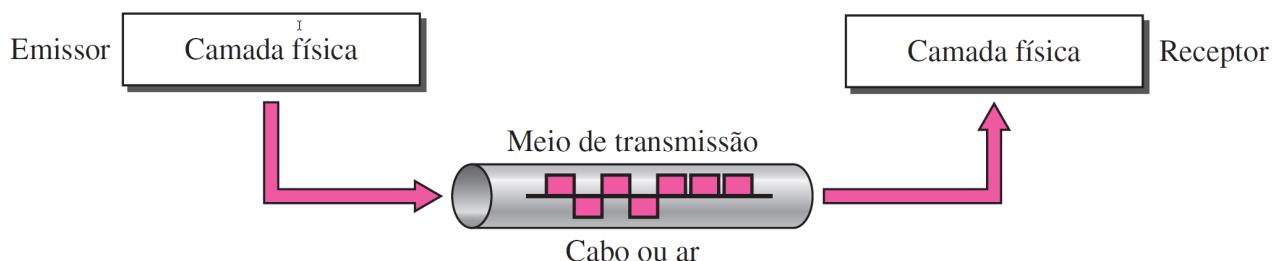


TIPO DE TOPOLOGIA	Descrição
FÍSICA	Exibe o layout (disposição) dos links e nós de rede.
LÓGICA	Exibe o fluxo ou percurso dos dados na rede.

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.

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 trançado, 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.

PLACA DE REDE	HUB (CONCENTRADOR)	BRIDGE (PONTE)
		
Equipamento de rede de comunicação bidirecional (entrada e saída de dados) conectado à placa-mãe do computador. Toda placa de rede possui um número identificador chamado Endereço MAC (48 Bits).	Dispositivo de rede capaz de aumentar o alcance de uma rede local por meio da regeneração de sinais. É capaz de trabalhar apenas com broadcast, isto é, ao receber um pacote de dados, distribui para todas as máquinas da rede.	Equipamento capaz de separar uma rede em segmentos menores, 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 enviar 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.

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)

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

PADRÃO TOKEN RING (IEEE 802.5)

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

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.

EVOLUÇÃO DO PADRÃO WIRELESS (802.11)		
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 +

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 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.

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.

PRINCIPAIS 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 e-mails 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 e TELNET.
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.

WORLD WIDE WEB (WWW)

A Web é uma aplicação que é executada na Internet – trata-se de uma série de páginas web que podem ser acessadas por meio de um navegador web.

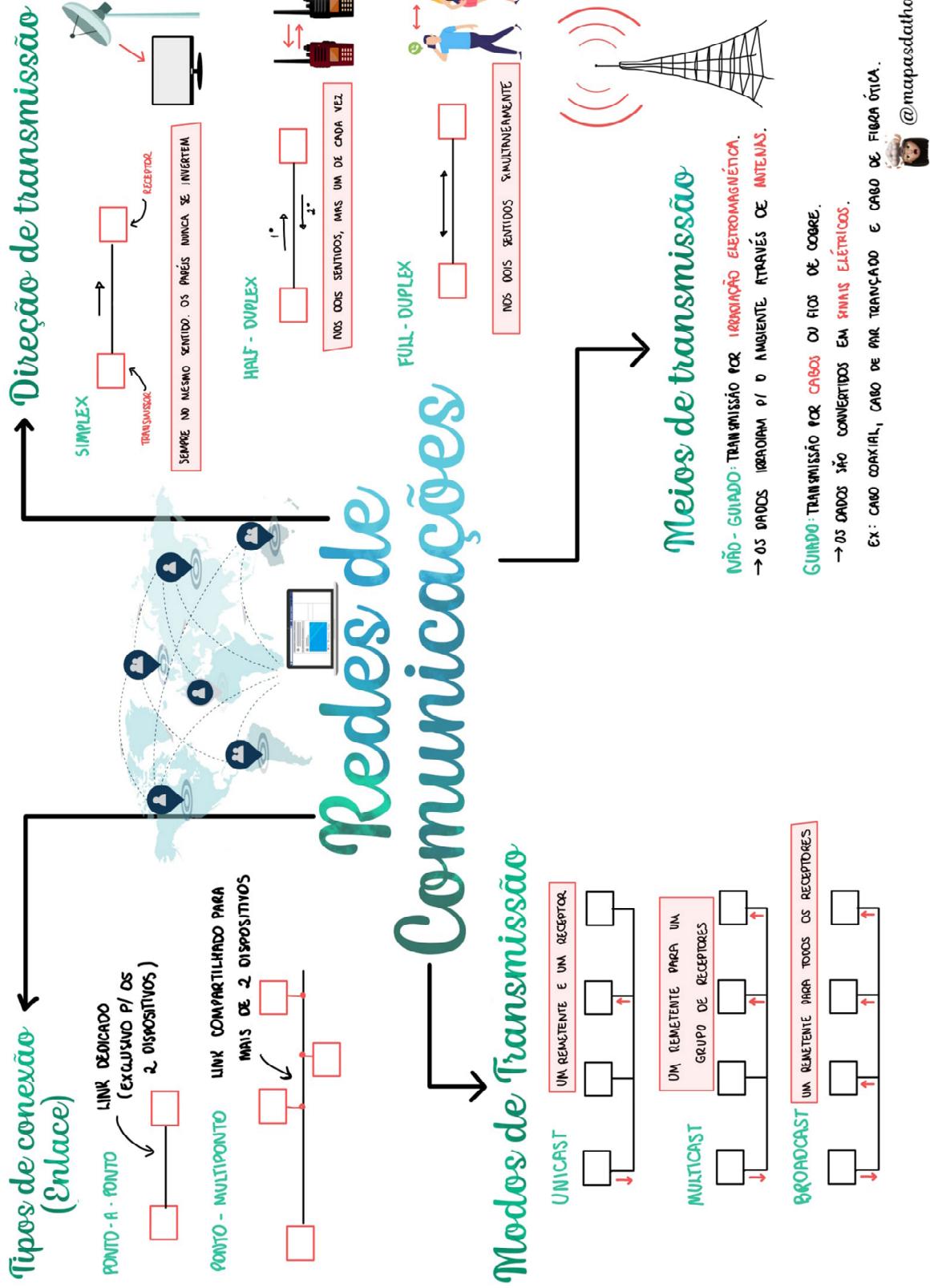
INTERNET DAS COISAS

Trata-se do conceito que se refere à interconexão digital de objetos físicos cotidianos entre si e com usuários por meio de sensores ou softwares capazes de transmitir dados pela internet.

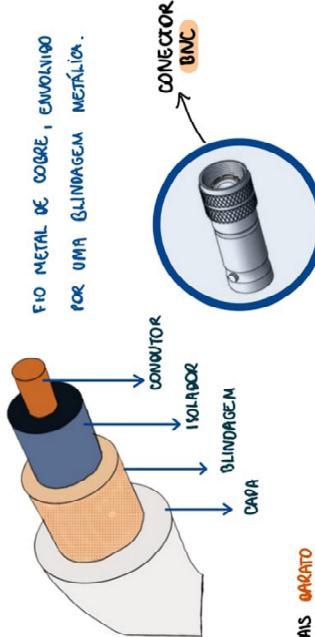
TECNOLOGIAS DE ACESSO	DESCRIÇÃO
DIAL-UP	Trata-se de uma conexão discada através de um modem e uma linha de telefonia fixa. Era a maneira mais popular de acesso da década de 90, hoje encontra-se em desuso. Apresenta um alto custo de implementação, é bastante instável e possui baixas taxas de transmissão. <i>Era banda larga?</i> 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!

ADSL	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.
HFC	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. <i>Por que é um hibridismo, Diego?</i> 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.
FIBRA ÓPTICA	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.
PLC	Trata-se da tecnologia que permite o acesso à internet banda larga via rede elétrica. PLC é a sigla para Power Line Communication. 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.
RADIODIFUSÃO	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.
SATÉLITE	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.
TELEFONIA MÓVEL	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.

MAPA MENTAL



Cabo coaxial



- MAIS QARATO
- RELATIVAMENTE FLEXÍVEL.
- MUITO RESISTENTE (NÃO IMUNE) À INTERFERÊNCIA ELETROMAGNETICA
- CORRE QSTÂNCIAS MENORES
- TAXA DE TRANSMISSÃO MENOR QUE O DOIS DE PAR TRANSCADO
- LARGURA DE BANDA MAIOR
- 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 MINIMIZAR A INTERFERÊNCIA ELETROMAG.
- É O CABO + BARATO
- GARANTE FLEXIBEL
- TRANSMITE SINAL ANALÓGICO E DIGITAL
- 2 PARES P / TRANSMISSÃO E 2 P / RECEPÇÃO (FULL - DUPLEX)
- BLINDADO: STP (SHIELDED TWISTED PAIR)
- NÃO BLINDADO: UTP (UNSHIELDED TWISTED PAIR)
- CONEXÃO MAIS COMPLEXA E MAIS CARA
- USADA MAS WANS

Cabo de fibra ótica

① ÚNICO EM UMA CASA É UM NÚCLEO (DE VIDRO) PARA TRANSMISSÃO DE LUZ.

- CAPACIDADE DE TRANSMISSÃO VIRTUALMENTE INDEFINIDA.
- IMUNE A INTERFERÊNCIAS ELETROMAGNÉTICAS
- LONGAS 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 MOBOS / 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

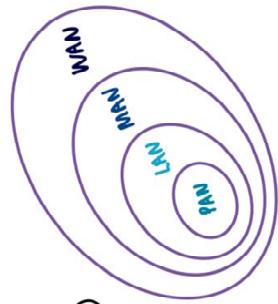
FIBRA MONOMODO



- LEVA O FEIXE DE LUZ POR UM ÚNICO MOO / 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

@mapasdatthai

por Dimensão



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

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

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

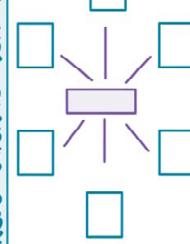
WAN: REDE ENTRE CIDADES, PAÍSES OU CONTINENTES



por Arquitetura/Forma de Interação

Tipos de Rede

REDE CLIENTE - SERVIDOR



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

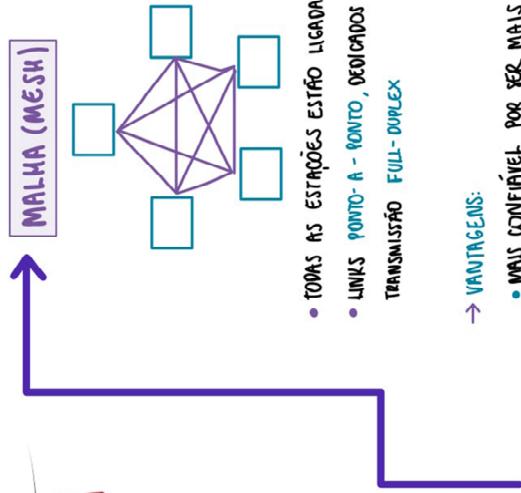
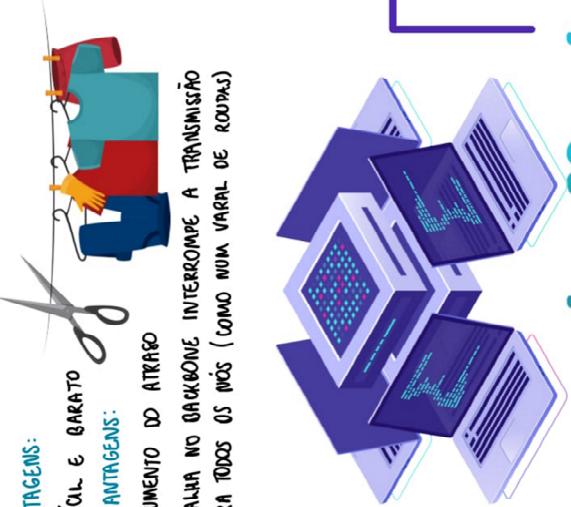
REDE PONTO-A-PONTO



- PEER-TO-PEER (P2P) OU PAR-A-PAR
- TODAS AS ESTAÇÕES PODEM COMUNICAR DADOS E PERIFÉRIOS UNIDAS COM AS OUTRAS

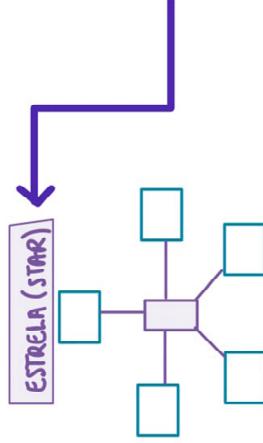
OBS: NÃO HÁ HIERARQUIA, NEM GERENCIAMENTO DE USUÁRIO.
TODAS PODEM SER CLIENTES.
TODAS PODEM SER SERVIDORES.

@mapasdathai



Tipos de Rede

por Topologia/Layout



- SE O DISPOSITIVO CENTRAL FALHAR, TODA A REDE SERÁ AFETADA
- ISOLAMENTO DE FAIXAS AMPLIFICADO
- LIMITAÇAO DO TAMANHO → QUANTO MAIOR, PIOR O DESEMpenHO
- TRAFEGO UNIDIRECIONAL
- LIMITAÇÃO DO TAMANHO → QUANTO MAIOR, PIOR O DESEMpenHO
- UMA INTERRUPÇÃO NO ANEL PODE DESLIGAR TODA A REDE



@mapasdathai



NIC (PLACA DE REDE)



- RECURSO DE HARDWARE MÍNIMO PARA TER UMA COMUNICAÇÃO BIRECIONAL.
- POSSUI UM IDENTIFICADOR CHAMADO DE ENDERECO MAC (MEDIUM ACCESS CONTROL)
 - ↳ 48 BITS
 - ↳ HEXADECIMAL
 - ↳ REPARTIDOS POR DOIS PONTOS
 - Ex: 00: 1C: 83: 08: F5: 15

SWITCH (COMUTADOR)



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

BRIDGE (PONTE)

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



HUB (CONCENTRADOR)

- CONCENTRA O TRÁFEGO DE REDE QUE PROVÉM DE VÁRIOS DISPOSITIVOS
- RODA MULTICAST (POFORQUEIRO)
- TOPOLOGIA FÍSICA: ESTRELLA
- TOPOLOGIA LÓGICA: BARRAMENTO
- HALF - DUPLEX

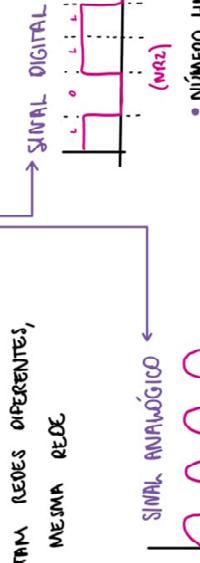
Equipamentos de Redes

MODEM (MODULADOR/DEMODULADOR)

- É O INTERMÉDIO QUE PERMITE A TRANSMISSÃO DE DADOS DIGITAIS POR UM MEIO QUE NÃO 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

ACCESS POINT (PONTO DE ACESSO)

- OFERECE ACESSO SEM FIO A UMA REDE CABEADA
- ESTENDE A CONVERSAÇÃO DE UMA REDE VEM EIU
- REPELETOR DE UMA REDE WIRELESS
- NÃO DISPENSA O USO DE UM ROTEADOR



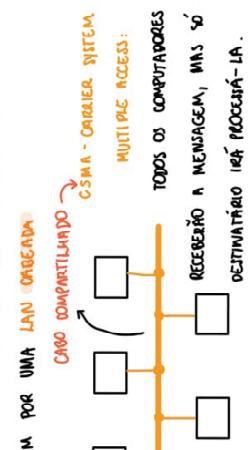
- NÚMERO LIMITADO DE VALORES
- 0 ou 1 (BITS)
- CONTATADORES SÓ ENTENDEM BITS
- MAIS NÍVEIS DE INTENSIDADE

@mapasdathai



Wireless

EVOLUÇÃO DOS PADRÕES ETHERNET	
ETHERNET	10 BASE-T / 10Mbps / 100m
ETHERNET	10 BASE-5 / 10Mbps / 500m
ETHERNET	10 BASE-T / 10 Mbps
FAST ETHERNET	100 BASE-T / 100 Mbps
GIGABIT ETHERNET	1000 BASE-T / 1000 Mbps
ETHERNET	10 G BASE-T / 10,000 Mbps



DOMÍNIO DE COLLISÃO: QUANDO A REDE É MUITO GRANDE.

DOMÍNIO DE COLLISÃO:

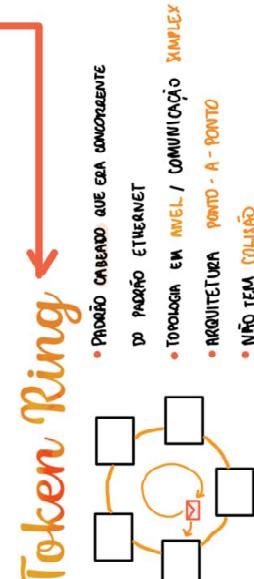
É UMA SEGMENTAÇÃO DA REDE. DIMINUI A QUANTIDADE DE DISPOSITIVOS NOS MEIOS DE TRANSMISSÃO COMPARTILHADOS PARA DIMINUIR A PROBABILIDADE DE COLISÕES.

Padrões de Redes

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	Wi-Max (WMAN)
IEEE 802.20	Móvel-f (WMAN)

Bluetooth

- OBJETIVO: INTEGRAR EQUIPAMENTOS PERIFÉRICOS NA WMAN
- REDE DE BAIXO CUSTO
- CURTO ALCANCE
- GRANDES TAXAS DE TRANSMISSÃO
- FREQUÊNCIA DE 2.4 GHz
- CONEXÃO MÉTICULADA
- ARCQUITETURA MASTER / SLAVE



- SUA CONEXÃO UTILIZA ONDAS DE RÁDIO
- EVOLUÇÃO DO PADRÃO WIRELESS
- PADRÃO FREQUÊNCIA TAXA DE TRANSMISSÃO
- IEEE 802.11B 2.4GHz 11Mbps
- IEEE 802.11A 5.0GHz 54Mbps
- IEEE 802.11G 2.4GHz 54Mbps
- IEEE 802.11N 2.4 ou 5.0GHz 150, 300 até 600 Mbps
- IEEE 802.11AC 5.0GHz 300Mbps, 1Gbps ou +

Observações:

- 802.11B + 802.11A NÃO SÃO EVOLUÇÕES UNA DO OUTRO, ELES SÓNGRAM SIMULTANEAMENTE
- O 802.11G ENTROU NO MERCADO PRIMEIRO
- O 802.11N É DUAL-BAND (PERMITE DUAS BANDAS DE FREQUÊNCIA)



- BASEADA NO PADRÃO WIRELESS 802.11
- CONEXÃO POR PONTOS DE ACESO (AP/ROUTER)
- P/TER ACESO, O USUÁRIO DEVE POSSE A TECNOLOGIA WI-FI INTEGRADA
- PADRÃO SEM FIO DE ALTA VELOCIDADE PARA REDES METROPOLITANAS (WMAN)
- CADAIDO P/ OPERAR INTEROPERABILIDADE ENTRE OS EQUIPAMENTOS
- RÁIO DE ATÉ 40 KM
- OPERA NO ESPECTRO DE FREQUÊNCIA 2.4 GHz, 3.5 GHz E 10.5 GHz
- NECESSÁRIO CONCEDER DA ANATEL
- POSSUI 3 ESPECTRAS DE MODULAÇÃO: QAM - 64, QAM - 16 E QPSK

@mapasdasdai

Ethernet

PERMITE QUE 2 OU MAIS COMPUTADORES SE

CONECTEM POR UMA LAN CABEADA

CÉGICO COMPARTILHADO →

CSMA - CARRIER SYSTEM.

MULTIPLEX ACESSO:

TODOS OS COMPUTADORES

RECEBERÃO A MENSAGEM, MAS SÓ O

DESTINATÁRIO IRÁ PROCESSAR-IA.

DESVANTAGEM:

TRAFEGO AUTO PODE GERAR COLISÃO = MENORAS MINTENCIÃGAIS

DOMÍNIO DE COLLISÃO: SOLUÇÃO: ESPERAR EM VELÊNIO DURANTE UMA PERÍODO DE TEMPO ALEATORIO ANTES DE TENTAR NOVAMENTE

DOMÍNIO DE COLLISÃO:

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

Token Ring

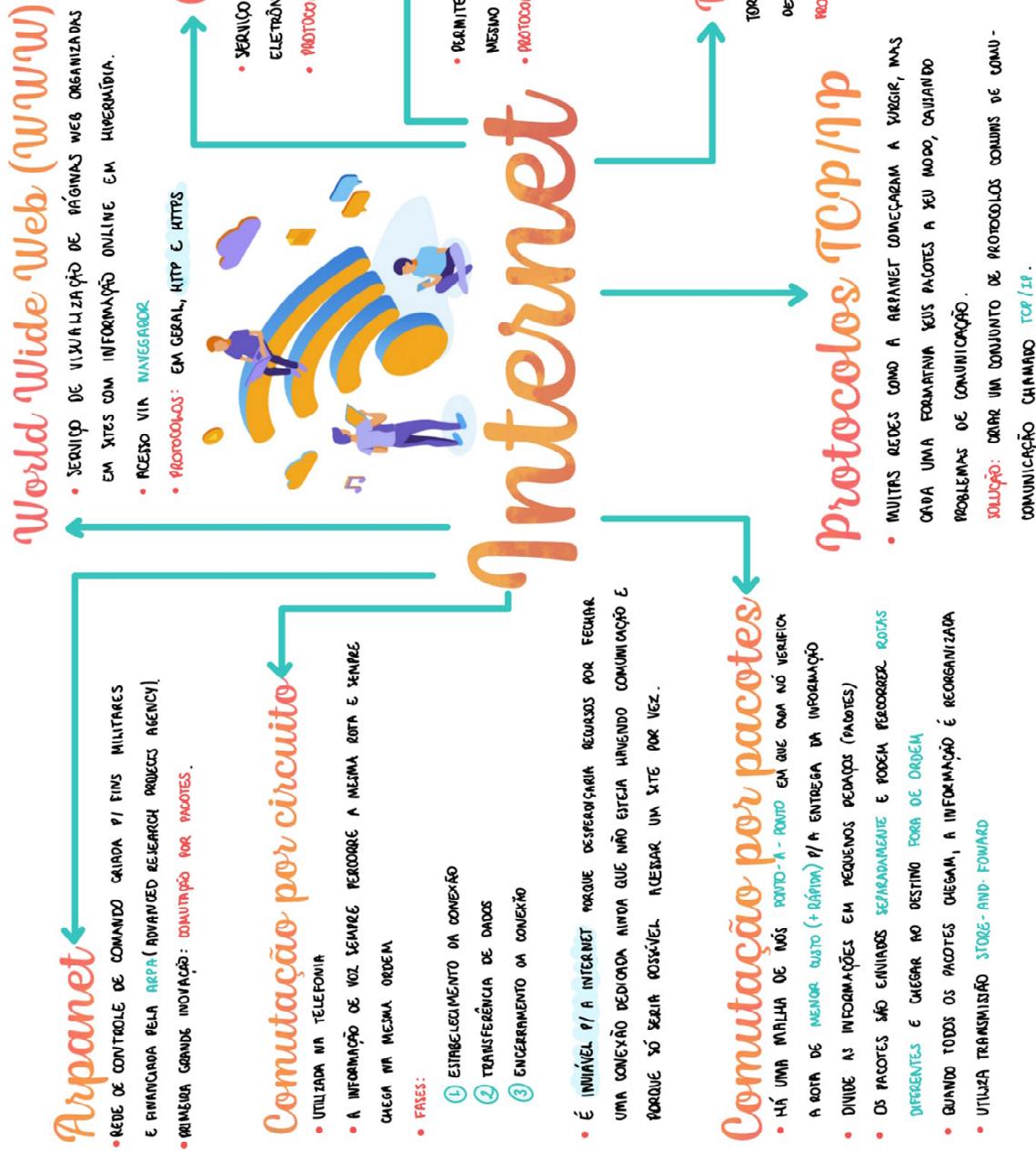
- Padrão criado que era dominante do padrão ETHERNET
- TOPOLOGIA EM ANEL / COMUNICAÇÃO SIMPLEX
- ARQUITETURA PONTO-A-PONTO
- NÃO TEM COLLISÃO

Wimax

OBJETIVO: SEM FIO DE ALTA VELOCIDADE PARA REDES METROPOLITANAS (WMAN)

- CADAIDO P/ OPERAR INTEROPERABILIDADE ENTRE OS EQUIPAMENTOS
- RÁIO DE ATÉ 40 KM
- OPERNA NO ESPECTRO DE FREQUÊNCIA 2.4 GHz, 3.5 GHz E 10.5 GHz
- NECESSÁRIO CONCEDER DA ANATEL
- POSSUI 3 ESPECTRAS DE MODULAÇÃO: QAM - 64, QAM - 16 E QPSK

@mapasdasdai



QUESTÕES COMENTADAS – FCC

1. (FCC / Prefeitura de São José do Rio Preto/SP – 2019) Ao entrar em contato com a Central de Serviços da organização onde trabalha para relatar dificuldades em conectar o computador à internet, o atendente solicitou ao Agente Administrativo a realização de um procedimento que envolvia a identificação de um componente da rede conhecido como RJ45, que é:
- a) o conector na extremidade do cabo de rede.
 - b) o botão usado para reiniciar o roteador.
 - c) o aparelho que transmite o sinal de internet via wireless.
 - d) a antena do roteador de internet.
 - e) o cabo de rede que liga o roteador ao computador.

Comentários:

RJ-45 é o nome dado ao conector da extremidade de um cabo de rede de par trançado.

Gabarito: Letra A

2. (FCC / SABESP – 2019) Acredita-se que, a partir de 2020, pelo menos 50 bilhões de coisas estarão conectadas à internet. Desde carros autônomos com capacidade de se comunicar com os sinais de trânsito, até sistemas de automação industrial, passando por drones e pessoas. Portanto, é necessário que a rede tenha capacidade de suportar um número massivo de dispositivos conectados ao mesmo tempo, notadamente os sem fio. O mundo espera por esta nova tecnologia de redes móveis. No Brasil, há um certo otimismo com relação à sua chegada, porém a faixa de frequência que deverá ser usada em todo mundo para essa tecnologia, 3.5GHz já é usada por operadoras de TV por antena parabólica, podendo haver interferências de sinais caso as duas atuem juntas. Entretanto, a Anatel acredita que será feita uma limpeza da faixa antes da sua instalação definitiva.

(Disponível em: <http://www.each.usp.br/petsi/jornal/?p=2402>)

Um Estagiário, ao ler essa notícia, conclui corretamente que o artigo se refere à tecnologia

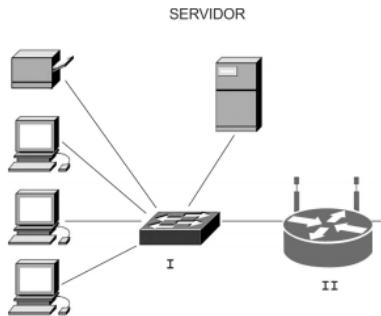
- a) IoT – Internet of Things.
- b) LTE – Long Tech Evolution.
- c) WG – Wireless Generation.
- d) HSDPA – High-Speed Double Packet Access.
- e) 5G.

Comentários:

A aguardada tecnologia que permitirá conectar um número massivo de dispositivos ao mesmo tempo será o 5G (5^a Geração da Telefonia Celular).

Gabarito: Letra E

3. (FCC / Prefeitura de São José do Rio Preto – 2019) Considere a figura abaixo, que mostra uma rede local de computadores. Os equipamentos de rede indicados por I e II são, respectivamente:



- a) modem e hub
- b) hub e switch
- c) bridge e hub
- d) roteador e bridge
- e) switch e roteador

Comentários:

A figura possui três computadores de mesa, uma impressora e um servidor conectados a um switch (I), que está conectado a um roteador wireless (II) – é possível distinguir pelas antenas. Essa é uma configuração muito comum em redes locais.

Gabarito: Letra E

4. (FCC / SABESP – 2019) Considere as recomendações para um dispositivo utilizado em redes móveis.

Existem várias questões importantes que devem ser consideradas na escolha e configuração deste dispositivo. É muito importante determinar quais recursos de criptografia e autenticação são suportados. Outro fator importante é saber se o dispositivo possibilita upgrades de firmware, permitindo incorporar novos padrões e eventuais correções lançadas pelo fabricante. Muitos modelos vêm com configurações de fábrica que são de conhecimento público, incluindo senhas default. É extremamente importante que todas as configurações originais sejam mudadas antes de colocar este dispositivo de rede móvel em produção, incluindo: senhas de administração, SSID, chaves WEP etc.

(Adaptado de: Práticas de Segurança para Administradores de Redes Internet – NIC BR Security Office)

Um Estagiário, ao ler essas recomendações, conclui que se trata do dispositivo denominado:

- a) hub.
- b) bluetooth.
- c) switcher.
- d) access point.
- e) SNMP.

Comentários:

(a) Errado. Hub não possui recursos de criptografia, autenticação e configurações de rede móvel; (b) Errado. Bluetooth é um padrão de redes e, não, um dispositivo; (c) Errado. Switch não possui recursos de criptografia, autenticação e configurações de rede móvel – Switcher não existe; (d) Correto. Contempla todas as características apresentadas no enunciado; (e) Errado. SNMP é um protocolo de gerenciamento de redes de computadores.

Gabarito: Letra D

5. (FCC / DETRAN-SP – 2019) Um Agente de Trânsito precisa adquirir um equipamento para conectar vários computadores em uma Local Area Network – LAN, de forma que os dados vindos do computador de origem somente sejam repassados por esse equipamento ao computador de destino e não a todos os computadores da rede. O equipamento que realiza essa função é um:

- a) modem.
- b) firewall.
- c) hub.
- d) switch.
- e) backbone.

Comentários:

(a) Errado, modem é um dispositivo que modula um sinal digital em um sinal analógico a ser transmitida por meio de uma linha telefônica e que demodula o sinal analógico e o converte para o sinal digital original; (b) Errado, firewall é uma ferramenta de segurança que permite gerenciar o tráfego entre redes de computadores; (c) Errado, hub trabalha em broadcast, logo dados vindos do computador de origem são repassados a todos os computadores da rede; (d) Correto, switch realmente conecta vários computadores em uma rede local, de forma que os dados não sejam enviados necessariamente em broadcast; (e) Errado, backbone é a espinha dorsal que suporta a rede mundial de computadores – internet.

Gabarito: Letra D

6. (FCC / SEGEP-MA / Técnico de Fiscalização Agropecuária - 2018) A tecnologia de rede de computadores:

- a) WiMax foi desenvolvida para funcionar em redes locais, tendo curto alcance, justamente o oposto do Wi-Fi, que foi desenvolvido para funcionar em redes metropolitanas. As duas tecnologias atuam de forma complementar.
- b) Wi-Fi permite o acesso à internet da casa ou da empresa de um usuário através de ondas do tipo bluetooth. O usuário poderá acessar a internet a até 1 km do aparelho receptor.
- c) 3G é uma das possibilidades de conexão de computadores usando banda larga sem fio. O sistema permite que voz, dados e imagens sejam transmitidos e acessados em alta velocidade, via satélite.
- d) Wi-Fi não precisa de cabeamento, pois o sinal de internet chega, por infravermelho, até o roteador através da infraestrutura sem fio da rede telefônica ou da TV a cabo.
- e) WiMax é uma evolução da Wi-Fi, sendo uma tecnologia que permite acesso sem fio à internet.

Comentários:

(a) Errado, a questão inverteu os conceitos; (b) Errado, são ondas eletromagnéticas de rádio e de curto alcance; (c) Errado, ela realmente oferece conexão banda larga, mas não via satélite, é via antena; (d) Errado, o sinal chega no roteador por meio de cabos e um Access Point ou um Roteador Wireless o difundem via wi-fi; (e) Correto. Questão perfeita!

Gabarito: Letra E

7. (FCC / SEGEP-MA – 2018) Há uma correta associação entre o problema e a sua solução usando o tipo correto de rede de computadores em:

- a) Uma empresa possui dois escritórios em uma mesma cidade e deseja que os computadores permaneçam interligados. Para isso deve-se utilizar uma LAN – Local Area Network que conecta diversas máquinas dentro de dezenas de quilômetros.
- b) Uma empresa possui um enorme volume de dados e precisa interligar o servidor principal aos outros computadores. Para permitir esta conexão deve-se utilizar uma SAN – Servidor Area Network que conecta diversas máquinas a um servidor central.
- c) Há diversos dispositivos em uma residência que precisam se comunicar dentro de uma distância bastante limitada. Para isso deve ser utilizada uma rede PAN – Private Area Network, que utiliza tecnologias como Wi-Fi e bluetooth.

- d) Deseja-se conectar redes de escritórios de uma mesma empresa ou de vários campi de universidades. A melhor solução é utilizar uma WLAN – Wireless Local Area Network, a versão wireless (sem fio) de uma LAN que alcança centenas de quilômetros.
- e) Uma empresa presta serviços online 24 horas para países localizados em diferentes continentes. Deve-se utilizar uma WAN – Wide Area Network, que vai além da MAN – Metropolitan Area Network, conseguindo alcançar uma área maior, como um país ou mesmo um continente.

Comentários:

(a) Errado, deve-se utilizar uma MAN; (b) Errado, SAN (*Storage Area Network*) é uma rede para armazenamento de dados; (c) Errado, PAN é *Personal Area Network* e, não, *Private Area Network*. Ademais, PAN usa apenas bluetooth; (d) Errado, a WLAN alcança centenas de metros – o ideal para o caso seria uma MAN; (e) Correto. A WAN (*Wide Area Network*) resolveria o problema.

Gabarito: Letra E

8. (FCC / METRÔ-SP / Oficial Logística de Almoxarifado - 2018) Em uma empresa há um modem, que também é roteador, que recebe o sinal de Internet e o distribui por cabo e via wireless para computadores e dispositivos móveis dos funcionários. Como esse roteador não possui portas suficientes para ligar por cabos outros 5 computadores, um técnico sugeriu utilizar um equipamento que, ligado ao roteador, poderá oferecer portas suficientes para ligar outros computadores do escritório, permitindo, inclusive, acesso à Internet. O equipamento sugerido foi um:

- a) switch.
- b) hub usb.
- c) dmz.
- d) proxy.
- e) vnc bridge.

Comentários:

Um roteador geralmente possui apenas quatro portas, logo ele seria capaz de conectar apenas quatro computadores. Como a rede possui cinco computadores, é necessário inserir um switch, que possui diversas portas. Dessa forma, teríamos a seguinte configuração:

5 COMPUTADORES ----- SWITCH ----- ROTEADOR/MODEM ----- INTERNET

Gabarito: Letra A

9. (FCC / SEFAZ-SC / Auditor Fiscal da Receita Estadual - 2018) O Auditor Fiscal foi designado para especificar a aquisição de um dispositivo de rede de computadores para realizar a interconexão e a comunicação entre uma rede Ethernet e uma rede Token-Ring. O dispositivo especificado pelo Auditor deve ser:

- a) Hub.
- b) Firewall.
- c) Switch.
- d) Roteador.
- e) Bridge.

Comentários:

Nós sabemos que o equipamento que permite conectar segmentos de redes diferentes que podem ou não utilizar tecnologias/protocolos de enlace distintos (Ex: Ethernet, Token Ring, etc) é a Bridge (Ponte). O Switch – apesar de ser considerado uma bridge multiportas – não permite interconectar tecnologias/protocolos de enlace distintos.

Gabarito: Letra E

10. (FCC / SEFAZ/SC – 2018) Acerca da Internet das Coisas, assinale a alternativa correta.

- a) Internet das Coisas é uma forma mais econômica de acesso à internet, a qual permite que dispositivos como geladeiras ofereçam internet a celulares e computadores de usuários, dispensando a necessidade de aquisição de roteadores ADSL à parte.
- b) Como exemplo de Internet das Coisas, é correto citar um dispositivo que mede a temperatura ambiente interna de um escritório e envia essa informação pela internet.
- c) Um exemplo de Internet das Coisas é o bitcoin, que é uma moeda virtual e iniciou a era da Internet das Moedas, com bancos virtuais sem agências.
- d) A Internet das Coisas opera separadamente da Internet das Pessoas e, por isso, não é possível enviar os dados coletados por dispositivos conectados à Internet das Coisas para a nuvem.
- e) A Internet das Coisas tem grande aplicação em ambientes domésticos e escritórios, mas pouca em ambientes industriais.

Comentários:

(a) Errado, não há relação com economia de custos, geladeiras não vão oferecer internet – vão acessar à internet, e não dispensam a aquisição de um roteador; (b) Correto; (c) Errado, não há nenhuma relação entre bitcoin e IoT; (d) Errado, opera em conjunto e permite – sim – enviar dados para nuvem; (e) Errado, tem aplicação em ambientes industriais.

11. (FCC / SEFAZ/SC – 2018) Cada vez mais a tecnologia wireless tem se tornado popular e sido mais utilizada em suporte à transmissão de dados. Um dos padrões tem as seguintes características:

- funciona na frequência de 2,4 GHz;
- oferece uma velocidade de 54 Mbps;
- baseia-se na compatibilidade com os dispositivos 802.11b;
- emprega autenticação WEP estática já aceitando outros tipos de autenticação como WPA (Wireless Protect Access) com criptografia dinâmica (método de criptografia TKIP e AES);
- apresenta os mesmos inconvenientes do padrão 802.11b, que são as incompatibilidades com dispositivos de diferentes fabricantes e a alta interferência tanto na transmissão como na recepção de sinais, porque funcionam a 2,4 GHz equivalentes aos telefones móveis;
- apresenta como vantagens o baixo preço dos seus dispositivos, a largura de banda gratuita bem como a disponibilidade gratuita em todo o mundo;
- tem sido bastante utilizado na comunicação com notebooks em redes sem fio em curtas distâncias.

Esse padrão é conhecido como:

- a) IEEE-802.11n.
- b) IEEE-802.11a.
- c) IEEE-802.11g.
- d) IEEE-802.11j.
- e) IEEE-802.11h.

Comentários:

Evolução do Padrão Wi-Fi (802.11)

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 +

Todas essas características nos remetem ao Padrão IEEE 802.11g.

Gabarito: Letra C

12. (FCC / TRT-PE / Analista Administrativo - 2018) Um Analista comprou um roteador wireless e o conectou por cabo em um switch para acessar a estrutura de rede cabeadas. Isso permitiu que todos os dispositivos sem fio conectados nesse roteador tivessem acesso a todos os serviços disponíveis na rede cabeadas, como por exemplo, acesso à internet. Nesse caso, o roteador foi configurado pelo Analista para operar no modo:

- a) ponto-a-ponto.
- b) access point.
- c) bridge.
- d) modem.
- e) backbone.

Comentários:

Se o roteador wireless conectado ao switch permitiu acesso aos recursos compartilhadas de uma rede local compartilhada, ele só pode ter sido configurado como um Access Point.

Gabarito: Letra B

13. (FCC / SEGEP-MA / Fiscal Estadual Agropecuário - 2018) Uma agência recebe o sinal da internet via cabo de fibra ótica em um modem, que está ligado a um dispositivo que funciona como um ponto de encontro, distribuindo o sinal da internet para todos os computadores e permitindo que eles se comuniquem por cabos de rede. Nesta situação, esse dispositivo é:

- a) switch.
- b) web server.
- c) firewall.
- d) hub USB.
- e) dmz server.

Comentários:

Galera, o Switch é o dispositivo capaz de distribuir o sinal de Internet e permitir que eles se comuniquem por meio de cabos.

Gabarito: Letra A

14. (FCC / DPE-RS / Técnico em Segurança - 2017) Considere uma rede de computadores instalada e em funcionamento que é caracterizada pelo seu alcance local, por se tratar de uma rede interna de curto alcance. De acordo com sua extensão geográfica, essa rede é classificada como:

- a) Metropolitan Area Network – MAN.
- b) Local Area Network – LAN.
- c) Wide Area Network – WAN.
- d) Storage Area Network – SAN.
- e) Popular Area Network – PAN.

Comentários:

Alcance local, rede interna e curto alcance... só pode ser uma Rede de Área Local (LAN).

Gabarito: Letra B

15. (FCC / ARTESP / Especialista em Regulação de Transporte - 2017) Considere a seguinte situação hipotética: um usuário recebe o sinal de Internet no seu computador desktop através de um modem de banda larga que também é roteador wireless, ligado diretamente ao computador por um cabo ethernet. Apesar de todos os equipamentos serem atuais e terem sido instalados recentemente, em determinado momento a Internet para de funcionar e aparece um símbolo de falha no ícone da rede da barra de tarefas.

Um conjunto de possíveis problemas relacionados a esta situação e ações para resolvê-los é elencado abaixo.

I. O cabo ethernet de par trançado pode ter se desconectado ou ficado frouxo, em decorrência do usuário movimentar o gabinete ou o modem. É recomendável que o usuário verifique a conexão do cabo, tanto no modem quanto no gabinete do computador.

II. O modem pode não estar funcionando bem em decorrência, por exemplo, de sobrecarga no tráfego de informações. É recomendável que o usuário desligue o modem e ligue-o novamente após alguns segundos, para que ele seja reiniciado e o seu funcionamento normal seja restaurado.

III. O adaptador de rede pode estar desativado, o driver pode estar desatualizado ou a placa de rede pode estar danificada. É recomendável que o usuário atualize o driver do adaptador de rede, ative-o, caso esteja desativado, ou providencie a troca da placa de rede, caso esteja danificada.

IV. O cabo ethernet coaxial pode ter se rompido devido ao seu núcleo de alumínio ser bastante sensível, principalmente nas proximidades dos conectores RJ-35 usados para fazer a ligação ao modem e ao gabinete do computador. É recomendável que o usuário faça uma verificação visual para saber se o cabo está rompido.

São problemas e ações corretas que podem ser tomadas para tentar resolvê-los o que consta APENAS em:

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

Comentários:

(I) Correto. O Cabo de Par-Trançado pode ter sofrido algum problema em decorrência de movimentações. Caso você fique sem internet algum dia, recomendo que verifique esse cabo.

(II) Correto. Se o modem estiver sofrendo com sobrecarga de recomendações, é realmente recomendável desligá-lo, esperar alguns segundos e religá-lo.

(III) Correto. Adaptador de Rede é qualquer dispositivo que permita a conexão a uma rede. A Placa de Rede é um tipo de Adaptador de Rede. Dito isso, ambos podem estar danificados ou desativados, e o driver pode estar desatualizado. É recomendável verificar todas essas opções.

(IV) Errado. O Cabo Ethernet Coaxial pode ter realmente se rompido, mas ele não possui um núcleo de alumínio, é de cobre. Ademais, ele utiliza conectores BNC (Cabos de Par Trançado utilizam conectores RJ-45 ou RJ-11).

Gabarito: Letra A

16.(FCC / ARTESP – 2017) Redes Wi-Fi se tornaram populares pela mobilidade que oferecem e pela facilidade de instalação e de uso em diferentes tipos de ambientes. Embora sejam bastante convenientes, oferecem diversos riscos à segurança das informações. Para resolver alguns destes riscos foram desenvolvidos mecanismos de segurança, como o:

- a) WEP (Wi-Fi Equivalent Privacy), fortemente recomendado por oferecer segurança total para smartphones.
- b) WPN (Wi-Fi Private Network), mecanismo desenvolvido para ambiente de redes móveis privadas.
- c) Bluetooth, mecanismo de proteção para comunicação de dados e voz para dispositivos móveis.
- d) WPA-2 (Wi-Fi Protected Access 2), mecanismo mais recomendado por oferecer criptografia considerada mais forte.

e) HPPTS, mecanismo que utiliza assinatura digital para assegurar a identidade tanto do site de destino como a do usuário da rede sem fio.

Comentários:

(a) Errado. WEP (Wired Equivalent Privacy) foi o primeiro mecanismo de segurança a ser lançado – é considerado frágil e, por isto, o uso deve ser evitado; (b) Errado, esse mecanismo não existe; (c) Errado, Bluetooth é um padrão de rede assim como as Redes Wi-Fi; (d) Correto. WPA-2 (Wi-Fi Protected Access 2) é um mecanismo de segurança que possui mecanismos de criptografia considerada forte – é o mecanismo mais recomendado atualmente; (e) Errado. HTTPS é um protocolo seguro de transferência de hipertexto.

Gabarito: Letra D

17. (FCC / DPE-RR / Técnico em Informática - 2015) A velocidade de transmissão 100 Mbit/s do Fast-Ethernet é alcançada com uma largura de banda de 31,25 MHz. Dessa forma, só é possível atender esta banda requerida com os cabos de par trançado de categoria:

- a) 5 ou superior
- b) 5a ou superior
- c) 6a
- d) 5e ou 6e
- e) 6 ou superior

Comentários:

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 MPBS (10G)	1000 MHz	100 Metros
CAT8	Até 40000 MBPS (40G)	2000 MHz	100 Metros

Só é possível atender a banda requerida por meio de cabos de par trançado de Categoria 5 ou superior. Notem que ele atinge velocidades de até 1000 Mbps e Frequência de até 100 Mhz.

Gabarito: Letra A

18.(FCC / DPE-RR / Técnico em Informática - 2015) Com relação ao meio de propagação do sinal, as fibras ópticas podem ser classificadas em monomodo e multimodo. As fibras multimodo:

- são usadas principalmente em LANs, pois têm um baixo custo e apresentam alto índice de refração quando comparadas com outras fibras.
- apresentam desvantagem no alinhamento dos núcleos nas emendas e conectores em relação às fibras monomodo.
- possuem o diâmetro do seu núcleo menor se comparado com o núcleo de uma fibra monomodo.
- têm taxas de transmissão mais altas, quando comparadas às fibras ópticas monomodo.
- são mais utilizadas em enlaces intercontinentais, nacionais e metropolitanos, devido à sua baixa atenuação para longas distâncias.

Comentários:

(a) Correto, são utilizadas principalmente em LANs, porque são mais baratas e apresentam alto índice de refração – o que causa um pouco mais de perdas e atenuação; (b) Errado, como o núcleo tem um diâmetro maior (como mostrado na figura da teoria), as emendas e os conectores que podem ser utilizados são mais fáceis de alinhar; (c) Errado, possuem diâmetro do seu núcleo maior (como mostrado na figura da teoria); (d) Errado, têm taxas de transmissão menores; (e) Errado, são utilizados em redes locais. Para enlaces intercontinentais, recomenda-se a utilização de fibras monomodo – que possuem baixo índice de refração e atenuação.

Gabarito: Letra A

19.(FCC / DPE-RR – 2015) Considerando a taxa de transferência de dados como o número de bits por segundo que podem ser enviados pelo enlace, a taxa de transferência máxima em redes Wi-Fi (802.11g) e o comprimento máximo indicado do enlace são, respectivamente,

- 100 Mbps e 100m.
- 54 Mbps e 100m.
- 64 Mbps e 150m.
- 11 Mbps e 50m.
- 54 Mbps e 50m.

Comentários:

EVOLUÇÃO DO PADRÃO WI-FI (802.11)		
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 802.11g possui taxa de transferência máxima de 54 Mbps e um alcance máximo de 100m.

Gabarito: Letra B

20. (FCC / TRE-RS / Auditor Público Externo - Engenharia Civil - Conhecimentos Básicos - 2014)

Atualmente, grande parte das instalações físicas de redes de computadores é realizada utilizando a tecnologia Ethernet com cabos de pares trançados. Neste tipo de instalação,

- a) um defeito em um dos computadores conectados não afeta o funcionamento da rede.
- b) utilizam-se menos cabos do que em uma instalação semelhante utilizando cabos coaxiais.
- c) são disponibilizadas maior largura de banda e velocidade do que permitem os cabos de Fibra Óptica podem disponibilizar.
- d) o conector utilizado nas terminações dos cabos é denominado UTP.
- e) a topologia de rede estabelecida é do tipo Barramento.

Comentários:

(a) Correto, cada nó possui uma conexão ponto-a-ponto com o nó central. Logo, um defeito em um dos computadores não afetará o funcionamento da rede como um todo; (b) Errado, não existe nenhuma relação entre tipo e quantidade de cabos; (c) Errado, cabos de fibra óptica podem oferecer larguras de banda infinitamente maiores; (d) Errado. UTP é um tipo de cabo de par trançado – o conector se chama RJ-45; (e) Errado, a topologia de rede estabelecida é do tipo Estrela.

Gabarito: Letra A

21. (FCC / TRT - 1ª REGIÃO (RJ) / Analista Judiciário – Área Administrativa / 2013) Sabendo que

uma intranet utiliza a infraestrutura de rede da empresa e fazendo uso das informações contidas no texto, considere que o computador de Paulo pode se comunicar com o computador servidor do Tribunal porque os recursos necessários estão fisicamente localizados em um raio de até 500 metros dentro do prédio do Tribunal, incluindo o computador de Paulo e o servidor. Isso significa que a rede utilizada é do tipo.

- a) WAN
- b) CAN
- c) LAN
- d) MAN
- e) ADSL

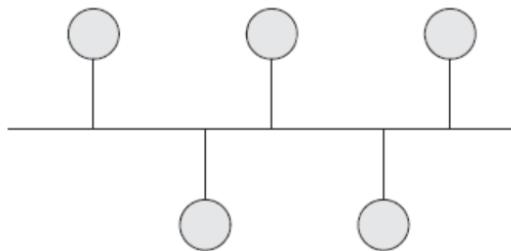
Comentários:

O texto introdutório é muito grande e irrelevante para responder à questão. Se recursos estão fisicamente localizados em um raio de até 500 metros, trata-se de uma Rede Local (LAN).

Gabarito: Letra C

22. (FCC / SPPREV / Analista em Gestão Previdenciária - 2012) A topologia de uma rede de comunicação refere-se à forma com que os enlaces físicos e os nós de comutação estão organizados, determinando os caminhos físicos existentes e utilizáveis entre quaisquer pares de estações conectadas a essa rede.

Figura 1



A denominação correta da Figura 1 é:

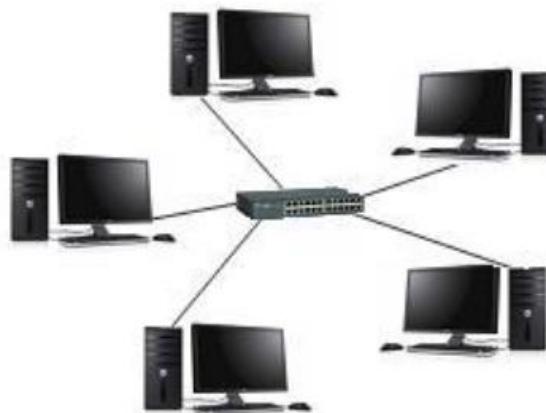
- a) Anel.
- b) Hierárquica
- c) Malha
- d) Barramento
- e) Estrela

Comentários:

Pessoal, a figura acima trata da Topologia em Barramento.

Gabarito: Letra D

23. (FCC / INSS / Técnico do Seguro Social - 2012) Pedro trabalha em uma pequena imobiliária cujo escritório possui cinco computadores ligados em uma rede com topologia estrela. Os computadores nessa rede são ligados por cabos de par trançado a um switch (concentrador) que filtra e encaminha pacotes entre os computadores da rede, como mostra a figura abaixo.



Certo dia, Pedro percebeu que não conseguia mais se comunicar com nenhum outro computador da rede. Vários são os motivos que podem ter causado esse problema, EXCETO:

- a) O cabo de rede de um dos demais computadores da rede pode ter se rompido.
- b) A placa de rede do computador de Pedro pode estar danificada.
- c) A porta do switch onde o cabo de rede do computador de Pedro está conectado pode estar danificada.
- d) O cabo de rede que liga o computador de Pedro ao switch pode ter se rompido.
- e) Modificações nas configurações do computador de Pedro podem ter tornado as configurações de rede incorretas.

Comentários:

(a) Errado, caso um cabo de rede de um dos demais computadores da rede se rompa, não afetará o restante da rede; (b) Correto, a placa de rede pode estar danificada; (c) Correto, a porta do Switch pode realmente estar danificada; (d) Correto, o cabo que liga especificamente o computador do Pedro ao Switch pode ter se rompido; (e) Correto, pode ter havido modificações nas configurações do computador de Pedro.

Gabarito: Letra A

24. (FCC / TRE-SP / Técnico Judiciário - Área Administrativa - 2012) Para que o computador de uma residência possa se conectar à Internet, utilizando a rede telefônica fixa, é indispensável o uso de um hardware chamado:

- a) hub.
- b) Modem.
- c) Acess point.
- d) Adaptador 3G.
- e) Switch.

Comentários:

O modem é o dispositivo que se conecta à Internet por meio de uma rede de telefonia fixa.

Gabarito: Letra B

25. (FCC / SEE-MG / Especialista em Educação - Supervisão Pedagógica- 2012) É usado para centralizar um ponto de acesso para Internet em uma rede e/ou criar uma rede de computadores com ou sem cabos para conectá-los. Pode ser utilizado em lugares como aeroportos e escolas com redes sem fio.

O texto refere-se ao dispositivo de redes chamado:

- a) Switch.
- b) Roteador wireless.
- c) WI-FI hub.
- d) Cable modem wireless.

Comentários:

Se o dispositivo é utilizado para centralizar um ponto de acesso para Internet em uma rede, ele pode ser um Roteador Wireless ou um Access Point. No entanto, a questão diz que ele pode criar uma rede de computadores com ou sem cabos para conectá-los, logo não pode ser um Access Point, porque ele só tem a função de centralizar um ponto de acesso ou estender a cobertura de uma rede sem fio.

Gabarito: Letra B

26. (FCC / TRT - 4ª REGIÃO (RS) / Técnico Judiciário - Área Administrativa- 2011) Numa rede LAN (*Local Area Network*), o recurso de hardware mínimo que deverá estar instalado no computador para permitir a comunicação com os demais elementos da rede é:

- a) o teclado.
- b) o hub.
- c) o cartão de memória.
- d) o switch.
- e) a placa de rede.

Comentários:

Trata-se da Placa de Rede, que é o recurso a ser instalado no seu computador para permitir a comunicação com os demais elementos.

Gabarito: Letra E

27. (FCC / INFRAERO / Técnico de Segurança do Trabalho - 2011) Sobre a infraestrutura para uma Intranet, considere:

- I. Wireless é um padrão específico de uma tecnologia de redes sem fio.
- II. Wi-Fi refere-se genericamente à transmissão de dados sem a utilização de meios físicos.
- III. WLAN é uma rede local sem fio para fazer conexão com a Internet ou entre os dispositivos da rede.

Está correto o que se afirma em:

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

Comentários:

(I) Errado. Wi-Fi (e, não, Wireless) é um padrão específico – uma marca comercial registrada; (II) Errado. Wireless (e, não, Wi-Fi) refere-se genericamente à transmissão de dados sem a utilização de meios físicos; (III) Correto. A WLAN (Wireless Local Area Network) é uma rede local sem fio para fazer conexão com a Internet ou entre os dispositivos da rede.

Gabarito: Letra B

28. (FCC / TRE-TO / Analista Judiciário - Área Administrativa - 2011) Os dispositivos que têm como principal função controlar o tráfego na Internet são denominados:

- a) Switches.
- b) Comutadores.
- c) Roteadores.
- d) Firewalls.
- e) Web servers.

Comentários:

A questão trata dos roteadores – eles são os responsáveis por controlar o tráfego na Internet. São aquelas anteninhas que permite que você compartilhe a conexão de internet com dois ou mais aparelhos. Firewalls têm a função de filtrar o tráfego de pacotes, mas não o controlar! Não confundam filtrar com controlar o tráfego: filtrar é o ato de decidir que pacotes podem ou não entrar e sair da rede; controlar é o ato de definir que caminho (rota) deve ser tomada pelos pacotes para chegarem ao seu destino. Quem controla o tráfego são os roteadores que são dispositivos utilizados para interligar redes.

29.(FCC / TRE-AL / Analista Judiciário - Área Judiciária - 2010) Ao compartilhar pastas e impressoras entre computadores, evitando que pessoas não autorizadas possam acessar os arquivos pela Internet, pode-se montar a rede usando um firewall, baseado em hardware, por meio do dispositivo denominado:

- a) Hub
- b) Switch
- c) Roteador
- d) Repetidor
- e) Cross-over

Comentários:

Os roteadores permitem compartilhar dados entre computadores em uma rede. Ressaltando que um firewall é um dispositivo de uma rede que aplica políticas de segurança a um determinado ponto de uma rede.

30.(FCC / TRT-SP – 2008) A configuração de rede mais adequada para conectar computadores de:

- um pavimento
- um estado
- uma nação

é, respectivamente:

- a) LAN, WAN, WAN.
- b) LAN, LAN, WAN.
- c) LAN, LAN, WAN.
- d) WAN, WAN, LAN.
- e) WAN, LAN, LAN.

Comentários:

Para conectar um pavimento ou andar de um prédio, utilizamos uma LAN. Já para conectar um estado, isto é, as cidades que o compõem, nós utilizamos uma WAN. Por fim, para conectar uma nação, isto é, os estados que a compõem, nós utilizamos uma WAN. Professor, e a MAN? Galera, lembrem-se que a MAN é para conectar redes dentro de uma mesma cidade – que não era o caso da questão. Tranquilo? Então, a resposta é LAN, WAN e WAN.

31. (FCC / TRT-SP – 2008) 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:

Redes de curta distância? Poucos metros? Usa Bluetooth? Sem fio? Usado em fones de ouvido, celulares, teclados e mouses? Todas essas são características de uma Rede de Área Pessoal (PAN).

32. (FCC / MPE-RS / Agente Administrativo - 2008) Os dispositivos de rede de computadores que são interconectados física e logicamente para possibilitar o tráfego de informações pelas redes compõem layouts denominados.

- a) Protocolos.
- b) Topologias.
- c) Roteamentos.
- d) Arquiteturas.
- e) Cabeamento.

Comentários:

Os layouts físicos de lógicos de uma rede de computadores são chamados de Topologias.

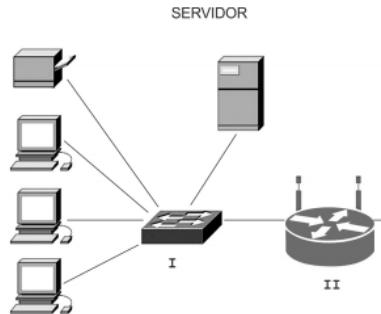
LISTA DE QUESTÕES – FCC

1. **(FCC / Prefeitura de São José do Rio Preto/SP – 2019)** Ao entrar em contato com a Central de Serviços da organização onde trabalha para relatar dificuldades em conectar o computador à internet, o atendente solicitou ao Agente Administrativo a realização de um procedimento que envolvia a identificação de um componente da rede conhecido como RJ45, que é:
 - a) o conector na extremidade do cabo de rede.
 - b) o botão usado para reiniciar o roteador.
 - c) o aparelho que transmite o sinal de internet via wireless.
 - d) a antena do roteador de internet.
 - e) o cabo de rede que liga o roteador ao computador.
2. **(FCC / SABESP – 2019)** Acredita-se que, a partir de 2020, pelo menos 50 bilhões de coisas estarão conectadas à internet. Desde carros autônomos com capacidade de se comunicar com os sinais de trânsito, até sistemas de automação industrial, passando por drones e pessoas. Portanto, é necessário que a rede tenha capacidade de suportar um número massivo de dispositivos conectados ao mesmo tempo, notadamente os sem fio. O mundo espera por esta nova tecnologia de redes móveis. No Brasil, há um certo otimismo com relação à sua chegada, porém a faixa de frequência que deverá ser usada em todo mundo para essa tecnologia, 3.5GHz já é usada por operadoras de TV por antena parabólica, podendo haver interferências de sinais caso as duas atuem juntas. Entretanto, a Anatel acredita que será feita uma limpeza da faixa antes da sua instalação definitiva.

(Disponível em: <http://www.each.usp.br/petsi/jornal/?p=2402>)

Um Estagiário, ao ler essa notícia, conclui corretamente que o artigo se refere à tecnologia

- a) IoT – Internet of Things.
 - b) LTE – Long Tech Evolution.
 - c) WG – Wireless Generation.
 - d) HSDPA – High-Speed Double Packet Access.
 - e) 5G.
3. **(FCC / Prefeitura de São José do Rio Preto – 2019)** Considere a figura abaixo, que mostra uma rede local de computadores. Os equipamentos de rede indicados por I e II são, respectivamente:



- a) modem e hub
- b) hub e switch
- c) bridge e hub
- d) roteador e bridge
- e) switch e roteador

4. (FCC / SABESP – 2019) Considere as recomendações para um dispositivo utilizado em redes móveis.

Existem várias questões importantes que devem ser consideradas na escolha e configuração deste dispositivo. É muito importante determinar quais recursos de criptografia e autenticação são suportados. Outro fator importante é saber se o dispositivo possibilita upgrades de firmware, permitindo incorporar novos padrões e eventuais correções lançadas pelo fabricante. Muitos modelos vêm com configurações de fábrica que são de conhecimento público, incluindo senhas default. É extremamente importante que todas as configurações originais sejam mudadas antes de colocar este dispositivo de rede móvel em produção, incluindo: senhas de administração, SSID, chaves WEP etc.

(Adaptado de: Práticas de Segurança para Administradores de Redes Internet – NIC BR Security Office)

Um Estagiário, ao ler essas recomendações, conclui que se trata do dispositivo denominado:

- a) hub.
- b) bluetooth.
- c) switcher.
- d) access point.
- e) SNMP.

5. (FCC / DETRAN-SP – 2019) Um Agente de Trânsito precisa adquirir um equipamento para conectar vários computadores em uma Local Area Network – LAN, de forma que os dados vindos do computador de origem somente sejam repassados por esse equipamento ao computador de destino e não a todos os computadores da rede. O equipamento que realiza essa função é um:

- a) modem.
- b) firewall.

- c) hub.
- d) switch.
- e) backbone.

6. (FCC / SEGEPE-MA / Técnico de Fiscalização Agropecuária - 2018) A tecnologia de rede de computadores:

- a) WiMax foi desenvolvida para funcionar em redes locais, tendo curto alcance, justamente o oposto do Wi-Fi, que foi desenvolvido para funcionar em redes metropolitanas. As duas tecnologias atuam de forma complementar.
- b) Wi-Fi permite o acesso à internet da casa ou da empresa de um usuário através de ondas do tipo bluetooth. O usuário poderá acessar a internet a até 1 km do aparelho receptor.
- c) 3G é uma das possibilidades de conexão de computadores usando banda larga sem fio. O sistema permite que voz, dados e imagens sejam transmitidos e acessados em alta velocidade, via satélite.
- d) Wi-Fi não precisa de cabeamento, pois o sinal de internet chega, por infravermelho, até o roteador através da infraestrutura sem fio da rede telefônica ou da TV a cabo.
- e) WiMax é uma evolução da Wi-Fi, sendo uma tecnologia que permite acesso sem fio à internet.

7. (FCC / METRÔ-SP / Oficial Logística de Almoxarifado - 2018) Em uma empresa há um modem, que também é roteador, que recebe o sinal de Internet e o distribui por cabo e via wireless para computadores e dispositivos móveis dos funcionários. Como esse roteador não possui portas suficientes para ligar por cabos outros 5 computadores, um técnico sugeriu utilizar um equipamento que, ligado ao roteador, poderá oferecer portas suficientes para ligar outros computadores do escritório, permitindo, inclusive, acesso à Internet. O equipamento sugerido foi um:

- a) switch.
- b) hub usb.
- c) dmz.
- d) proxy.
- e) vnc bridge.

8. (FCC / SEGEPE-MA – 2018) Há uma correta associação entre o problema e a sua solução usando o tipo correto de rede de computadores em:

- a) Uma empresa possui dois escritórios em uma mesma cidade e deseja que os computadores permaneçam interligados. Para isso deve-se utilizar uma LAN – Local Area Network que conecta diversas máquinas dentro de dezenas de quilômetros.

- b) Uma empresa possui um enorme volume de dados e precisa interligar o servidor principal aos outros computadores. Para permitir esta conexão deve-se utilizar uma SAN – Servidor Area Network que conecta diversas máquinas a um servidor central.
- c) Há diversos dispositivos em uma residência que precisam se comunicar dentro de uma distância bastante limitada. Para isso deve ser utilizada uma rede PAN – Private Area Network, que utiliza tecnologias como Wi-Fi e bluetooth.
- d) Deseja-se conectar redes de escritórios de uma mesma empresa ou de vários campi de universidades. A melhor solução é utilizar uma WLAN – Wireless Local Area Network, a versão wireless (sem fio) de uma LAN que alcança centenas de quilômetros.
- e) Uma empresa presta serviços online 24 horas para países localizados em diferentes continentes. Deve-se utilizar uma WAN – Wide Area Network, que vai além da MAN – Metropolitan Area Network, conseguindo alcançar uma área maior, como um país ou mesmo um continente.

9. (FCC / SEFAZ-SC / Auditor Fiscal da Receita Estadual - 2018) O Auditor Fiscal foi designado para especificar a aquisição de um dispositivo de rede de computadores para realizar a interconexão e a comunicação entre uma rede Ethernet e uma rede Token-Ring. O dispositivo especificado pelo Auditor deve ser:

- a) Hub.
- b) Firewall.
- c) Switch.
- d) Roteador.
- e) Bridge.

10. (FCC / SEFAZ/SC – 2018) Acerca da Internet das Coisas, assinale a alternativa correta.

- a) Internet das Coisas é uma forma mais econômica de acesso à internet, a qual permite que dispositivos como geladeiras ofereçam internet a celulares e computadores de usuários, dispensando a necessidade de aquisição de roteadores ADSL à parte.
- b) Como exemplo de Internet das Coisas, é correto citar um dispositivo que mede a temperatura ambiente interna de um escritório e envia essa informação pela internet.
- c) Um exemplo de Internet das Coisas é o bitcoin, que é uma moeda virtual e iniciou a era da Internet das Moedas, com bancos virtuais sem agências.
- d) A Internet das Coisas opera separadamente da Internet das Pessoas e, por isso, não é possível enviar os dados coletados por dispositivos conectados à Internet das Coisas para a nuvem.

e) A Internet das Coisas tem grande aplicação em ambientes domésticos e escritórios, mas pouca em ambientes industriais.

11. (FCC / SEFAZ/SC – 2018) Cada vez mais a tecnologia wireless tem se tornado popular e sido mais utilizada em suporte à transmissão de dados. Um dos padrões tem as seguintes características:

- funciona na frequência de 2,4 GHz;
- oferece uma velocidade de 54 Mbps;
- baseia-se na compatibilidade com os dispositivos 802.11b;
- emprega autenticação WEP estática já aceitando outros tipos de autenticação como WPA (Wireless Protect Access) com criptografia dinâmica (método de criptografia TKIP e AES);
- apresenta os mesmos inconvenientes do padrão 802.11b, que são as incompatibilidades com dispositivos de diferentes fabricantes e a alta interferência tanto na transmissão como na recepção de sinais, porque funcionam a 2,4 GHz equivalentes aos telefones móveis;
- apresenta como vantagens o baixo preço dos seus dispositivos, a largura de banda gratuita bem como a disponibilidade gratuita em todo o mundo;
- tem sido bastante utilizado na comunicação com notebooks em redes sem fio em curtas distâncias.

Esse padrão é conhecido como:

- a) IEEE-802.11n.
- b) IEEE-802.11a.
- c) IEEE-802.11g.
- d) IEEE-802.11j.
- e) IEEE-802.11h.

12. (FCC / TRT-PE / Analista Administrativo - 2018) Um Analista comprou um roteador wireless e o conectou por cabo em um switch para acessar a estrutura de rede cabeadas. Isso permitiu que todos os dispositivos sem fio conectados nesse roteador tivessem acesso a todos os serviços disponíveis na rede cabeadas, como por exemplo, acesso à internet. Nesse caso, o roteador foi configurado pelo Analista para operar no modo:

- a) ponto-a-ponto.
- b) access point.
- c) bridge.
- d) modem.

e) backbone.

13. (FCC / SEGEP-MA / Fiscal Estadual Agropecuário - 2018) Uma agência recebe o sinal da internet via cabo de fibra ótica em um modem, que está ligado a um dispositivo que funciona como um ponto de encontro, distribuindo o sinal da internet para todos os computadores e permitindo que eles se comuniquem por cabos de rede. Nesta situação, esse dispositivo é:

- a) switch.
- b) web server.
- c) firewall.
- d) hub USB.
- e) dmz server.

14. (FCC/DPE-RS / Técnico em Segurança - 2017) Considere uma rede de computadores instalada e em funcionamento que é caracterizada pelo seu alcance local, por se tratar de uma rede interna de curto alcance. De acordo com sua extensão geográfica, essa rede é classificada como:

- a) Metropolitan Area Network – MAN.
- b) Local Area Network – LAN.
- c) Wide Area Network – WAN.
- d) Storage Area Network – SAN.
- e) Popular Area Network – PAN.

15. (FCC / ARTESP / Especialista em Regulação de Transporte - 2017) Considere a seguinte situação hipotética: um usuário recebe o sinal de Internet no seu computador desktop através de um modem de banda larga que também é roteador wireless, ligado diretamente ao computador por um cabo ethernet. Apesar de todos os equipamentos serem atuais e terem sido instalados recentemente, em determinado momento a Internet para de funcionar e aparece um símbolo de falha no ícone da rede da barra de tarefas.

Um conjunto de possíveis problemas relacionados a esta situação e ações para resolvê-los é elencado abaixo.

I. O cabo ethernet de par trançado pode ter se desconectado ou ficado frouxo, em decorrência do usuário movimentar o gabinete ou o modem. É recomendável que o usuário verifique a conexão do cabo, tanto no modem quanto no gabinete do computador.

II. O modem pode não estar funcionando bem em decorrência, por exemplo, de sobrecarga no tráfego de informações. É recomendável que o usuário desligue o modem e ligue-o novamente após alguns segundos, para que ele seja reiniciado e o seu funcionamento normal seja restaurado.

III. O adaptador de rede pode estar desativado, o driver pode estar desatualizado ou a placa de rede pode estar danificada. É recomendável que o usuário atualize o driver do adaptador de

rede, ative-o, caso esteja desativado, ou providencie a troca da placa de rede, caso esteja danificada.

IV. O cabo ethernet coaxial pode ter se rompido devido ao seu núcleo de alumínio ser bastante sensível, principalmente nas proximidades dos conectores RJ-35 usados para fazer a ligação ao modem e ao gabinete do computador. É recomendável que o usuário faça uma verificação visual para saber se o cabo está rompido.

São problemas e ações corretas que podem ser tomadas para tentar resolvê-los o que consta APENAS em:

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

16. (FCC / ARTESP – 2017) Redes Wi-Fi se tornaram populares pela mobilidade que oferecem e pela facilidade de instalação e de uso em diferentes tipos de ambientes. Embora sejam bastante convenientes, oferecem diversos riscos à segurança das informações. Para resolver alguns destes riscos foram desenvolvidos mecanismos de segurança, como o:

- a) WEP (Wi-Fi Equivalent Privacy), fortemente recomendado por oferecer segurança total para smartphones.
- b) WPN (Wi-Fi Private Network), mecanismo desenvolvido para ambiente de redes móveis privadas.
- c) Bluetooth, mecanismo de proteção para comunicação de dados e voz para dispositivos móveis.
- d) WPA-2 (Wi-Fi Protected Access 2), mecanismo mais recomendado por oferecer criptografia considerada mais forte.
- e) HPPTS, mecanismo que utiliza assinatura digital para assegurar a identidade tanto do site de destino como a do usuário da rede sem fio.

17. (FCC / DPE-RR / Técnico em Informática - 2015) A velocidade de transmissão 100 Mbit/s do Fast-Ethernet é alcançada com uma largura de banda de 31,25 MHz. Dessa forma, só é possível atender esta banda requerida com os cabos de par trançado de categoria:

- a) 5 ou superior
- b) 5a ou superior
- c) 6a

- d) 5e ou 6e
- e) 6 ou superior

18. (FCC / DPE-RR / Técnico em Informática - 2015) Com relação ao meio de propagação do sinal, as fibras ópticas podem ser classificadas em monomodo e multimodo. As fibras multimodo:

- a) são usadas principalmente em LANs, pois têm um baixo custo e apresentam alto índice de refração quando comparadas com outras fibras.
- b) apresentam desvantagem no alinhamento dos núcleos nas emendas e conectores em relação às fibras monomodo.
- c) possuem o diâmetro do seu núcleo menor se comparado com o núcleo de uma fibra monomodo.
- d) têm taxas de transmissão mais altas, quando comparadas às fibras ópticas monomodo.
- e) são mais utilizadas em enlaces intercontinentais, nacionais e metropolitanos, devido à sua baixa atenuação para longas distâncias.

19. (FCC / DPE-RR – 2015) Considerando a taxa de transferência de dados como o número de bits por segundo que podem ser enviados pelo enlace, a taxa de transferência máxima em redes Wi-Fi (802.11g) e o comprimento máximo indicado do enlace são, respectivamente,

- a) 100 Mbps e 100m.
- b) 54 Mbps e 100m.
- c) 64 Mbps e 150m.
- d) 11 Mbps e 50m.
- e) 54 Mbps e 50m.

20. (FCC / TRE-RS / Auditor Público Externo - Engenharia Civil - Conhecimentos Básicos - 2014)

Atualmente, grande parte das instalações físicas de redes de computadores é realizada utilizando a tecnologia Ethernet com cabos de pares trançados. Neste tipo de instalação,

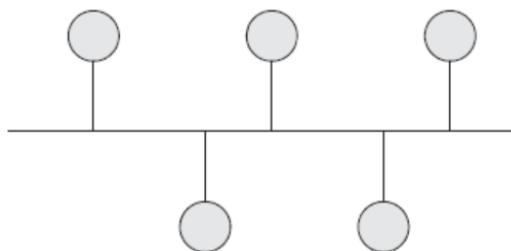
- a) um defeito em um dos computadores conectados não afeta o funcionamento da rede.
- b) utilizam-se menos cabos do que em uma instalação semelhante utilizando cabos coaxiais.
- c) são disponibilizadas maior largura de banda e velocidade do que permitem os cabos de Fibra Óptica podem disponibilizar.
- d) o conector utilizado nas terminações dos cabos é denominado UTP.
- e) a topologia de rede estabelecida é do tipo Barramento.

21. (FCC / TRT - 1ª REGIÃO (RJ) / Analista Judiciário – Área Administrativa / 2013) Sabendo que uma intranet utiliza a infraestrutura de rede da empresa e fazendo uso das informações contidas no texto, considere que o computador de Paulo pode se comunicar com o computador servidor do Tribunal porque os recursos necessários estão fisicamente localizados em um raio de até 500 metros dentro do prédio do Tribunal, incluindo o computador de Paulo e o servidor. Isso significa que a rede utilizada é do tipo.

- a) WAN
- b) CAN
- c) LAN
- d) MAN
- e) ADSL

22. (FCC / SPPREV / Analista em Gestão Previdenciária - 2012) A topologia de uma rede de comunicação refere-se à forma com que os enlaces físicos e os nós de comutação estão organizados, determinando os caminhos físicos existentes e utilizáveis entre quaisquer pares de estações conectadas a essa rede.

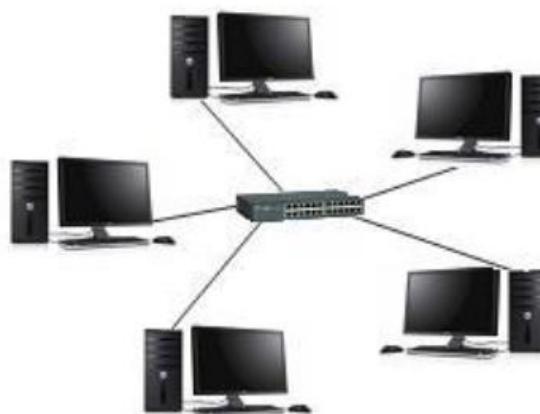
Figura 1



A denominação correta da Figura 1 é:

- a) Anel.
- b) Hierárquica
- c) Malha
- d) Barramento
- e) Estrela

23. (FCC / INSS / Técnico do Seguro Social - 2012) Pedro trabalha em uma pequena imobiliária cujo escritório possui cinco computadores ligados em uma rede com topologia estrela. Os computadores nessa rede são ligados por cabos de par trançado a um switch (concentrador) que filtra e encaminha pacotes entre os computadores da rede, como mostra a figura abaixo.



Certo dia, Pedro percebeu que não conseguia mais se comunicar com nenhum outro computador da rede. Vários são os motivos que podem ter causado esse problema, EXCETO:

- a) O cabo de rede de um dos demais computadores da rede pode ter se rompido.
- b) A placa de rede do computador de Pedro pode estar danificada.
- c) A porta do switch onde o cabo de rede do computador de Pedro está conectado pode estar danificada.
- d) O cabo de rede que liga o computador de Pedro ao switch pode ter se rompido.
- e) Modificações nas configurações do computador de Pedro podem ter tornado as configurações de rede incorretas.

24. (FCC / TRE-SP / Técnico Judiciário - Área Administrativa - 2012) Para que o computador de uma residência possa se conectar à Internet, utilizando a rede telefônica fixa, é indispensável o uso de um hardware chamado:

- a) hub.
- b) Modem.
- c) Acess point.
- d) Adaptador 3G.
- e) Switch.

25. (FCC / SEE-MG / Especialista em Educação - Supervisão Pedagógica- 2012) É usado para centralizar um ponto de acesso para Internet em uma rede e/ou criar uma rede de computadores com ou sem cabos para conectá-los. Pode ser utilizado em lugares como aeroportos e escolas com redes sem fio.

O texto refere-se ao dispositivo de redes chamado:

- a) Switch.
- b) Roteador wireless.
- c) WI-FI hub.
- d) Cable modem wireless.

26. (FCC / TRT - 4ª REGIÃO (RS) / Técnico Judiciário - Área Administrativa- 2011) Numa rede LAN (*Local Area Network*), o recurso de hardware mínimo que deverá estar instalado no computador para permitir a comunicação com os demais elementos da rede é:

- a) o teclado.
- b) o hub.
- c) o cartão de memória.
- d) o switch.
- e) a placa de rede.

27. (FCC / INFRAERO / Técnico de Segurança do Trabalho - 2011) Sobre a infraestrutura para uma Intranet, considere:

- I. Wireless é um padrão específico de uma tecnologia de redes sem fio.
- II. Wi-Fi refere-se genericamente à transmissão de dados sem a utilização de meios físicos.
- III. WLAN é uma rede local sem fio para fazer conexão com a Internet ou entre os dispositivos da rede.

Está correto o que se afirma em:

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

28.(FCC / TRE-TO / Analista Judiciário - Área Administrativa - 2011) Os dispositivos que têm como principal função controlar o tráfego na Internet são denominados:

- a) Switches.
- b) Comutadores.
- c) Roteadores.
- d) Firewalls.
- e) Web servers.

29.(FCC / TRE-AL / Analista Judiciário - Área Judiciária - 2010) Ao compartilhar pastas e impressoras entre computadores, evitando que pessoas não autorizadas possam acessar os arquivos pela Internet, pode-se montar a rede usando um firewall, baseado em hardware, por meio do dispositivo denominado:

- a) Hub
- b) Switch
- c) Roteador
- d) Repetidor
- e) Cross-over

30. (FCC / TRT-SP – 2008) A configuração de rede mais adequada para conectar computadores de:

- um pavimento
- um estado
- uma nação

é, respectivamente:

- a) LAN, WAN, WAN.
- b) LAN, LAN, WAN.
- c) LAN, LAN, WAN.
- d) WAN, WAN, LAN.
- e) WAN, LAN, LAN.

31. (FCC / TRT-SP – 2008) 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).

32. (FCC / MPE-RS / Agente Administrativo - 2008) Os dispositivos de rede de computadores que são interconectados física e logicamente para possibilitar o tráfego de informações pelas redes compõem layouts denominados.

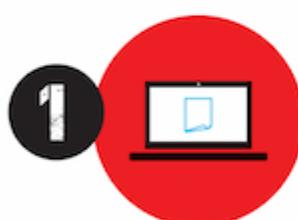
- a) Protocolos.
- b) Topologias.
- c) Roteamentos.
- d) Arquiteturas.
- e) Cabeamento.

GABARITO – FCC

- | | | |
|--------------------|--------------------|--------------------|
| 1. LETRA A | 12. LETRA B | 23. LETRA A |
| 2. LETRA E | 13. LETRA A | 24. LETRA B |
| 3. LETRA E | 14. LETRA B | 25. LETRA B |
| 4. LETRA D | 15. LETRA A | 26. LETRA E |
| 5. LETRA D | 16. LETRA D | 27. LETRA B |
| 6. LETRA E | 17. LETRA A | 28. LETRA C |
| 7. LETRA E | 18. LETRA A | 29. LETRA C |
| 8. LETRA A | 19. LETRA B | 30. LETRA A |
| 9. LETRA E | 20. LETRA A | 31. LETRA C |
| 10. LETRA B | 21. LETRA C | 32. LETRA B |
| 11. LETRA C | 22. LETRA D | |

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).



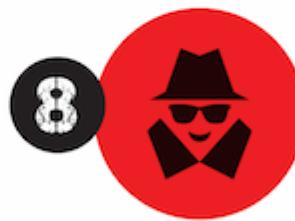
6

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

Concursado(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.