Estratégia Concursos

Aula 00

Informática p/ CBM-TO Aluno-Soldado (cargo 2) - Pós-Edital

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

11 de Fevereiro de 2021

Sumário

Redes de Computadores 5
1 - Conceitos Básicos 5
2 – Tipos de Conexão/Enlace 5
3 – Direções de Transmissão 6
4 – Modos de Transmissão 7
5 – Classificação de Redes 7
5.1 – Quanto à Dimensão, Tamanho ou Área Geográfica 7
5.2 – Quanto à Arquitetura de Rede ou Forma de Interação 8
5.3 – Quanto à Topologia (Layout) 12
6 – Meios de Transmissão 18
6.1 – Cabo Coaxial 18
6.2 – Cabo de Par Trançado 19
6.3 – Cabo de Fibra Óptica 20
7 – Equipamentos de Redes 21
7.1 – Network Interface Card (NIC ou Placa de Rede) 21
7.2 – Hub (Concentrador) 21
7.3 – Bridge (Ponte) 23
7.4 – Switch (Comutador) 23
7.5 – Router (Roteador) 25
7.6 – Modem 28
8 – Padrões de Redes 30
8.1 – Padrão Ethernet (IEEE 802.3) 30

8.2 – Padrão Token Ring (IEEE 802.5) 36

8.3 – Padrão Wireless (IEEE 802.11) 36

8.4 – Padrão Bluetooth (IEEE 802.15) 39

8.5 – Padrão WiMAX (IEEE 802.16) 40

Internet 42

1 - Conceitos Básicos 42

2 – Web (WWW) 48

3 – Deep Web e Dark Web 49

4 – Internet das Coisas (IoT) 52

5 – Tecnologias de Acesso 56

5.1 – Dial-Up 57

5.2 – ADSL 58

5.3 – HFC 59

5.4 – Fibra Óptica 59

5.5 – PLC 59

5.6 – Radiodifusão 59

5.7 – Satélite 60

5.8 – Telefonia Móvel 60

Questões Comentadas - CESPE 62

Lista de Questões – CESPE 73

Gabarito – CESPE 77

APRESENTAÇÃO DO PROFESSOR

PROF. DIEGO CARVALHO

FORMADO EM CIÊNCIA DA COMPUTAÇÃO PELA UNIVERSIDADE DE BRASÍLIA (UNB), PÓS-GRADUADO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA E, ATUALMENTE, AUDITOR FEDERAL DE FINANÇAS E CONTROLE DA SECRETARIA DO TESOURO NACIONAL.

ESTRATÉGIA CONCURSOS

Já ministrei mais de 400 cursos de Tecnologia da Informação no Estratégia Concursos. Nosso objetivo é entregar um material completo e focado no edital, de forma que você não precise procurar mais nenhum outro material de estudos para fazer uma excelente prova.

ENTRE EM CONTATO:



INSTAGRAM.COM/PROFESSORDIEGOCARVALHO



FACEBOOK.COM/PROFESSORDIEGOCARVALHO

APRESENTAÇÃO DA AULA

Pessoal, o tema da nossa aula é: **Redes de Computadores e Internet**. A primeira parte não é muito comum em prova (e também não é muito fácil). *Por que?* Porque trata de assuntos bastante técnicos! *Diego, por que isso é cobrado na minha prova?* Cara, isso é um pré-requisito para entender melhor Internet, uma vez que ela é um tipo de Rede de Computadores. Já a parte de Internet em si está no cotidiano de vocês, logo é bem mais tranquilo...

PROFESSOR DIEGO CARVALHO - WWW.INSTAGRAM.COM/PROFESSORDIEGOCARVALHO

Galera, todos os tópicos da aula possuem Faixas de Incidência, que indicam se o assunto cai muito ou pouco em prova. *Diego, se cai pouco para que colocar em aula?* Cair pouco não significa que não cairá justamente na sua prova! A ideia aqui é: se você está com pouco tempo e precisa ver somente aquilo que cai mais, você pode filtrar pelas incidências média, alta e altíssima; se você tem tempo sobrando e quer ver tudo, vejam também as incidências baixas e baixíssimas. *Fechado?*

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

INCIDÊNCIA EM PROVA: BAIXA

INCIDÊNCIA EM PROVA: MÉDIA

INCIDÊNCIA EM PROVA: ALTA

INCIDÊNCIA EM PROVA: ALTÍSSIMA





REDES DE COMPUTADORES

1 - Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Uma rede de computadores é um conjunto de terminais, equipamentos, meios de transmissão e comutação que interligados possibilitam a prestação de serviços. **Em outras palavras, é um conjunto de dispositivos (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.

Por que utilizar redes de computadores? Um dos principais motivos é o compartilhamento de 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.

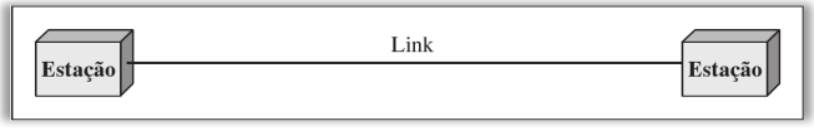
Como nós podemos resumir tudo isso? **Bem, uma rede de computadores basicamente tem como objetivo o compartilhamento de recursos, deixando equipamentos, programas e principalmente dados ao alcance de múltiplos usuários**, sem falar na possibilidade de servir como meio de comunicação entre pessoas através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

2 – Tipos de Conexão/Enlace

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

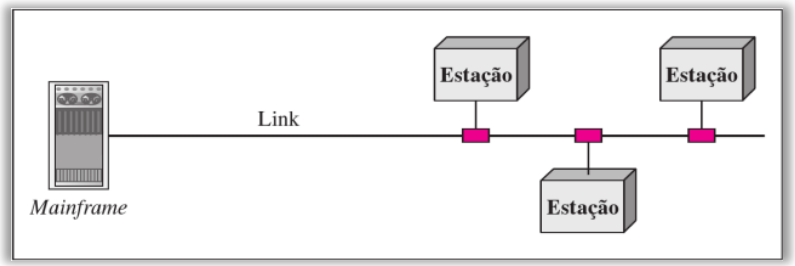
Redes são dois ou mais dispositivos conectados através de links. *O que é um link?* **Também chamado de enlace, trata-se de um caminho de comunicação que transfere dados de um dispositivo para outro.** Para fins de visualização, é mais simples imaginar qualquer link como uma reta entre dois pontos. Para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

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



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

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

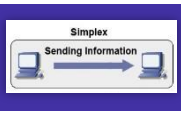
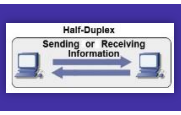


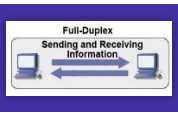
Já uma conexão ponto-multiponto é uma conexão na qual mais de dois dispositivos compartilham um único link. E um ambiente multiponto, a capacidade do canal de comunicação é compartilhada, seja de forma espacial ou seja de forma temporal. Se diversos dispositivos puderem usar o link simultaneamente, ele é chamado de conexão compartilhada espacialmente. Se os usuários tiverem de se revezar entre si, trata-se de uma conexão compartilhada no tempo.

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

3 – Direções de Transmissão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

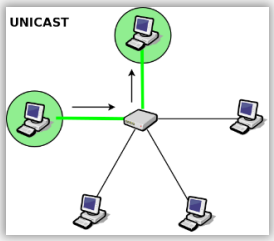
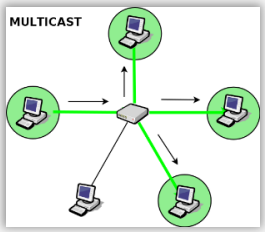
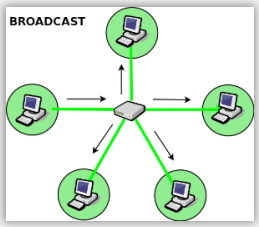
TIPO	REPRESENTAÇÃO	DESCRIÇÃO
SIMPLEX		Uma comunicação é dita simplex quando há um transmissor de mensagem, um receptor de mensagem e esses papéis nunca se invertem no período de transmissão (Ex: TV, Rádio AM/FM, Teclado, etc).
HALF-DUPLEX		Uma comunicação é dita half-duplex quando temos um transmissor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

FULL-DUPLEX		Uma comunicação é dita full-duplex quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados simultaneamente (Ex: Telefone, VoIP, etc).

4 – 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; 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.

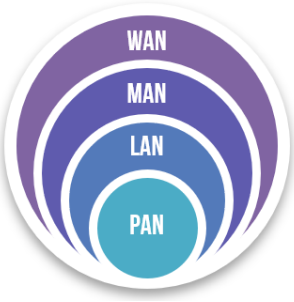
5 – Classificação de Redes

5.1 – Quanto à Dimensão, Tamanho ou Área Geográfica

INCIDÊNCIA EM PROVA: ALTA

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

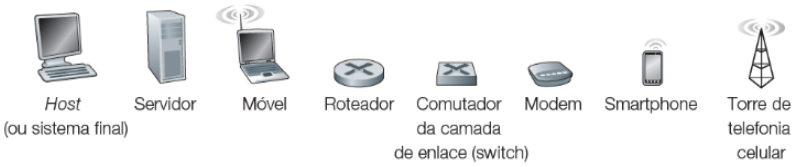
WIDE AREA NETWORK	WAN	Rede de computadores entre cidades, países ou até continentes.	De algumas dezenas a milhares de quilômetros.



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

5.2 – 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?*

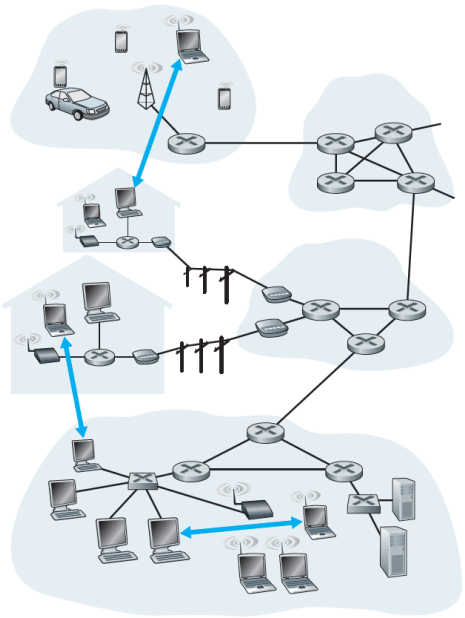
Informalmente, clientes costumam ser computadores de mesa, notebooks, smartphones e assim por diante; ao passo que servidores costumam ser máquinas mais poderosas, que armazenam e distribuem páginas web, vídeo em tempo real, transmissão de e-mails e assim por diante. Hoje, a maioria dos servidores dos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

5.2.1 – Rede Ponto-a-Ponto

INCIDÊNCIA EM PROVA: BAIXA

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

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



Nesse tipo de rede, todas as máquinas oferecem e consomem recursos umas das outras, atuando ora como clientes, ora como servidoras. No entanto, nem tudo são flores! Dependendo do contexto, o gerenciamento pode ser bastante complexo. Quando essa arquitetura é utilizada em redes domésticas com poucos computadores e cuja finalidade é compartilhar impressoras, trocar arquivos e compartilhar internet – não há problema[1].

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, 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.**



[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.

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:

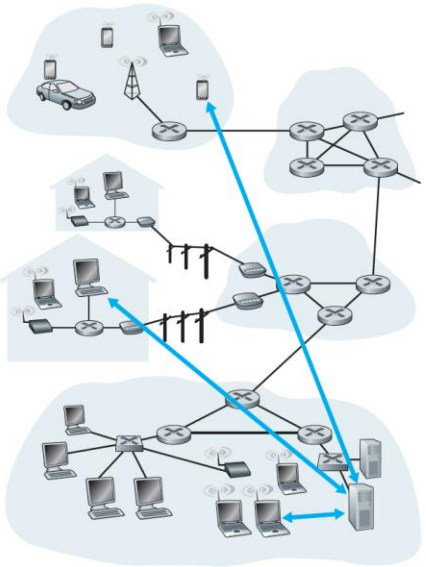
Se existe um link dedicado entre dois dispositivos, trata-se de um tipo de **conexão ponto-a-ponto**. Por outro lado, se um mesmo dispositivo pode exercer função de cliente ou servidor em diferentes momentos, trata-se de um tipo de **arquitetura ponto-a-ponto**. O nome utilizado é exatamente o mesmo, 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 que existem diversos dispositivos clientes se comunicando diretamente com um único servidor – um cliente jamais se comunica diretamente com outro cliente.

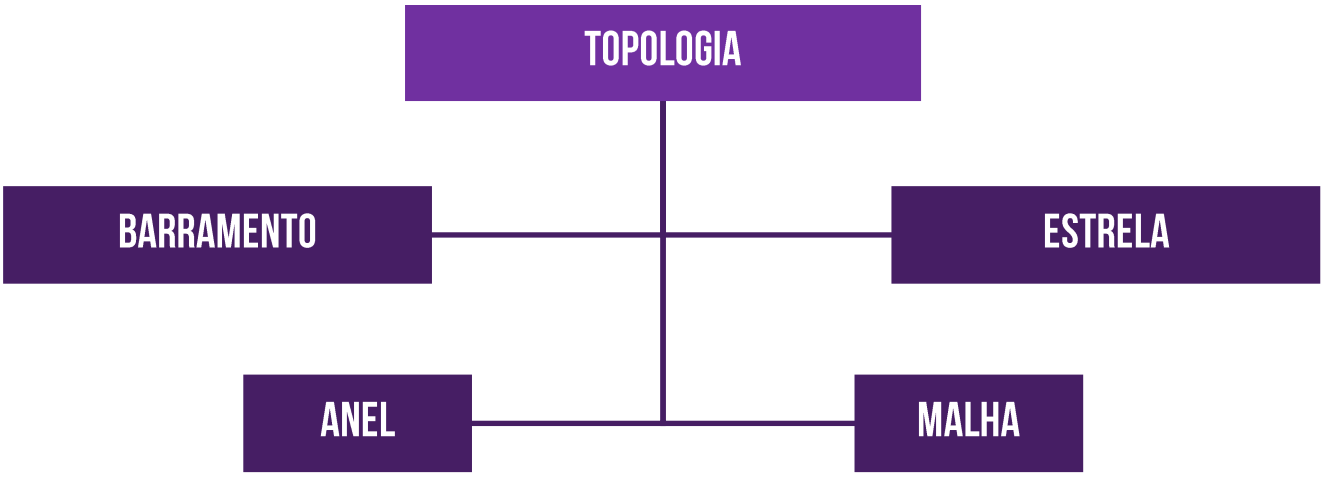


Ao contrário do que ocorre nas redes par-a-par, os computadores que funcionam como clientes – em regra – não fornecem recursos e serviços aos outros computadores da rede. *Que servidores são esses, Diego?* Galera, existem vários tipos de servidores, como por exemplo: servidor de impressão, servidor de 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.**

5.3 – Quanto à Topologia (*Layout*)

Quando falamos em topologia, estamos tratando da forma como os dispositivos estão organizadores. Dois ou mais dispositivos se conectam a um link; dois ou mais links formam uma topologia. A topologia é a representação geométrica da relação de todos os links e os dispositivos de uma conexão entre si. Existem quatro topologias básicas[2] 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

[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.

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

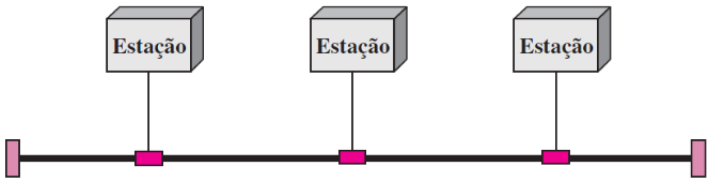


Se uma questão de prova não deixar explícito em sua redação qual é o tipo de topologia, pode-se assumir que ela se refere à **Topologia Física e – não – à Topologia Lógica!**

5.3.1 – Barramento (Bus)

INCIDÊNCIA EM PROVA: ALTA

Nessa topologia, todas as estações ficam conectadas ao mesmo meio de transmissão em uma conexão ponto-multiponto[3]**.** *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

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

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...

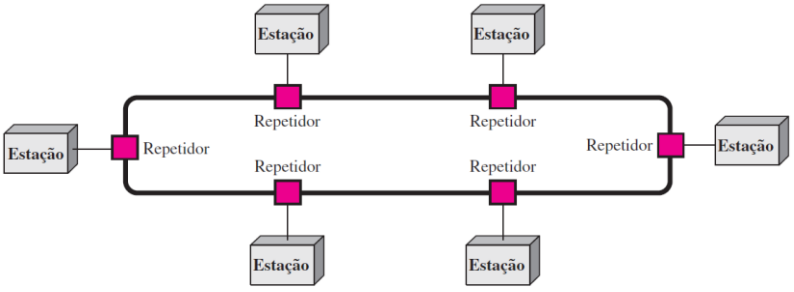
Além disso, uma falha ou ruptura no cabo de backbone implica a interrupção da transmissão, até mesmo entre os dispositivos que se encontram do mesmo lado em que ocorreu o problema. *Professor, não entendi muito bem!* **Galera, imaginem que nós temos um varal com diversas roupas penduradas**. Caso haja 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!

Entre as vantagens, temos a 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. **Entre as desvantagens, temos o aumento do atraso e o isolamento de falhas.** Como o link é compartilhado, quanto maior o número de máquinas, maior o atraso (delay) na comunicação e menor o desempenho da rede.

5.3.2 – Anel (Ring)

INCIDÊNCIA EM PROVA: MÉDIA

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



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

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

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

Pessoal, existe uma modalidade do atletismo chamada Corrida de Revezamento. Quatro atletas percorrem uma pista circular segurando um bastão: o primeiro corre e passa o bastão para o segundo; o segundo corre e passa o bastão para o terceiro; o terceiro corre e passa o bastão para o quarto; e o quarto corre até o final do circuito. Em outras palavras, um atleta somente pode correr caso ele esteja com o bastão em suas mãos. **Aqui funciona de maneira semelhante...**

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

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

Nessa topologia, um anel é relativamente fácil de ser instalado e reconfigurado, com isolamento de falhas simplificado. *Por 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.

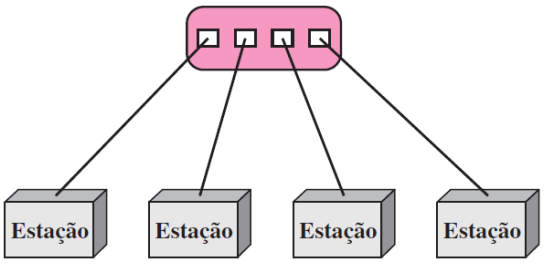
Por outro lado, há também desvantagens: se algum enlace for rompido, a rede inteira para de funcionar. Além disso, como o tráfego de dados é simplex, se alguma estação se tornar inoperante por alguma razão, a rede também para de funcionar. Existem também uma limitação quanto ao comprimento máximo do 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.

5.3.3 – Estrela (*Star*)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Nessa topologia, as estações são ligadas através de uma conexão ponto-a-ponto dedicada a um nó central controlador[4], 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.

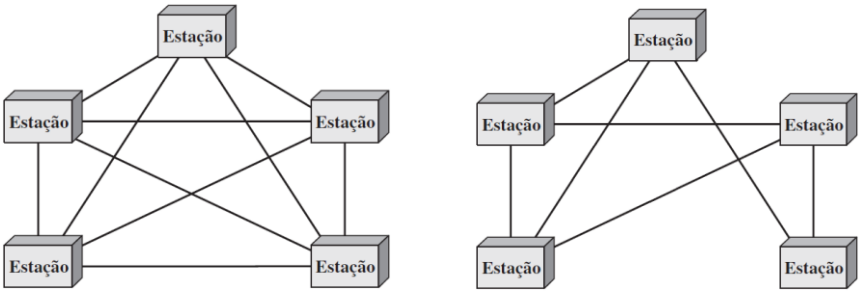
5.3.4 – Malha (Mesh)

INCIDÊNCIA EM PROVA: BAIXA

Nessa topologia, cada estação de trabalho possui uma conexão ponto a ponto direta e dedicada entre as demais estações da rede, de modo que não exista uma hierarquia entre elas. Nas imagens seguintes, temos dois exemplos de Topologia em Malha: à esquerda, temos uma malha completa (também chamada de *Full Mesh*), isto é, cada nó se conecta a todos os outros nós; à direita, temos uma malha parcial, isto é, nem todos os nós se conectam aos outros nós[5].

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

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



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 espaço disponível seja capaz de acomodar (nas paredes, tetos ou pisos). Finalmente, o hardware necessário para conectar cada link (portas, placas e/ou cabos) pode ter um custo proibitivo. **Por tais razões, uma topologia de malha normalmente é implementada de forma limitada.**

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

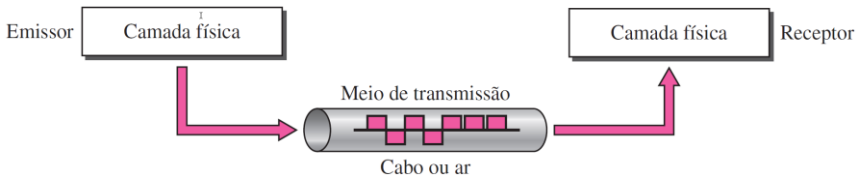
A utilização mais comum desse tipo de rede é para interligar – por exemplo – matrizes e filiais em uma rede metropolitana cabeada. É importante salientar também que existem as redes em malha sem fio, que são comumente utilizadas para interligar – por exemplo – dispositivos sem fio em uma rede local por 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

6 – Meios de Transmissão

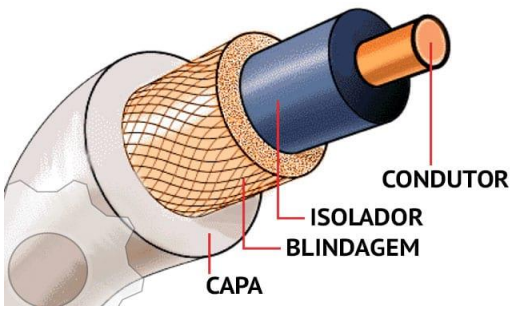
Um meio de transmissão, em termos gerais, pode ser definido como qualquer coisa capaz de transportar informações de uma origem a um destino. Por exemplo: o meio de transmissão para duas pessoas conversando durante um jantar é o ar; para uma mensagem escrita, o meio de transmissão poderia ser um carteiro,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

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



6.1 – 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.

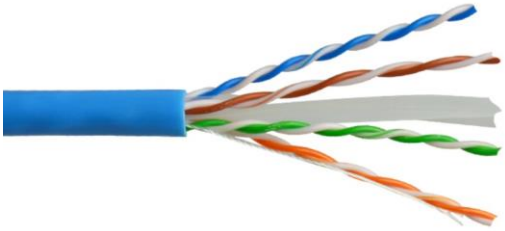
Foi utilizado até meados da década de 90 em redes de computadores, quando começou a ser substituído pelo cabo de par trançado. Ele ainda é utilizado em telecomunicações, basta dar uma olhadinha no decodificador da sua TV por Assinatura. **O cabo que chega na sua casa/prédio e que entra em um modem é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

6.2 – 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:

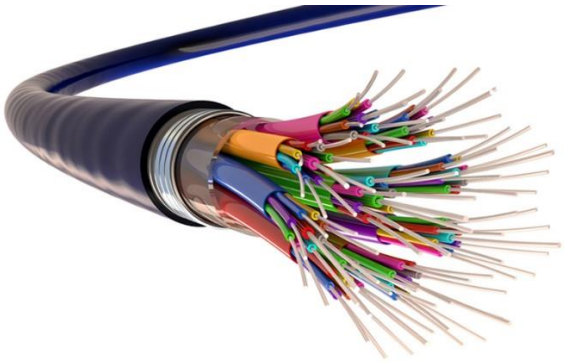
CATEGORIA	TAXA DE TRANSMISSÃO	LARGURA DE BANDA	DISTÂNCIA MÁXIMA
CAT3	Até 10 MBPS	16 MHz	100 Metros
CAT4	Até 16 MBPS	20 MHz	100 Metros
CAT5	Até 100 MBPS	100 MHz	100 Metros

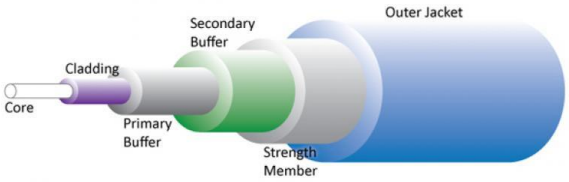
CAT5E	Até 1000 MBPS (1G)	100 MHz	100 Metros
CAT6	Até 10000 MBPS (10G)	250 MHz	100 Metros
CAT6A	Até 10000 MBPS (10G)	500 MHz	100 Metros
CAT7	Até 10000 MBPS (10G)	600 MHz	100 Metros
CAT7A	Até 10000 MBPS (10G)	1000 MHz	100 Metros
CAT8	Até 40000 MBPS (40G)	2000 MHz	100 Metros

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.

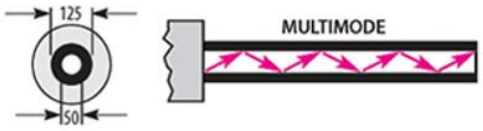
6.3 – Cabo de Fibra Óptica

INCIDÊNCIA EM PROVA: MÉDIA

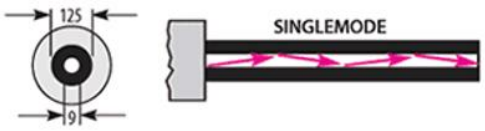




Consiste em uma Casca e um Núcleo (em geral, de vidro) para transmissão de luz. Possui capacidade de transmissão virtualmente infinita, é imune a interferências eletromagnéticas e consegue ligar distâncias maiores sem a necessidade de repetidores. Como desvantagens, ele é incapaz de fazer curvas acentuadas, 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).**

7 – 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...

7.1 – Network Interface Card (NIC ou Placa de Rede)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



Galera, essa é a famosa Placa de Rede! 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).

7.2 – 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:



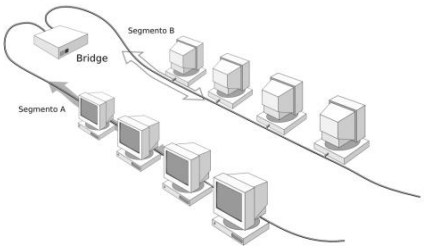
7.3 – Bridge (Ponte)

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.

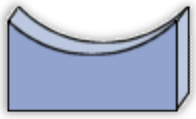
Ela também permite conectar segmentos de redes diferentes que podem ou não utilizar tecnologias/protocolos de enlace distintos (Ex: Ethernet, Token Ring, etc). *O que é um segmento de rede?* É simplesmente subdivisão de uma rede. Vejam abaixo que uma rede foi separada em dois segmentos: Segmento A e 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. Aliás, uma desvantagem das Bridges é que elas geralmente só possuem duas portas, logo só conseguem separar a rede em dois segmentos. **Em contraste com o Switch, que veremos a seguir, que é conhecido como Bridge Multiporta por ter várias portas e suportar várias segmentações**. A representação de uma Bridge é apresentada abaixo:



Em suma: uma bridge é um equipamento de rede que permite conectar redes diferentes que podem utilizar tecnologias/protocolos de enlace distintos em segmentos menores, permitindo filtrar os quadros de forma que somente passe para o outro segmento da bridge dados enviados para algum destinatário presente nele. **Em contraste com o hub, que envia dados em broadcast, a bridge é capaz de enviar dados em *unicast* – para um destinatário específico**.

7.4 – Switch (Comutador)

INCIDÊNCIA EM PROVA: MÉDIA



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

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

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

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

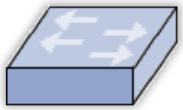
Outro recurso interessante é o autoaprendizado, ou seja, switches são equipamentos que não precisam ser configurados manualmente. *Como assim, Diego?* Quando você conecta um computador ao switch, você não precisa acessar o switch e informá-lo que o computador com endereço X está localizado na porta Y. O switch possui uma tabela dinâmica que automaticamente associa endereços 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 – ele é um roteador mais sofisticado; e um Switch de Camada 2 opera nas camadas física e de enlace. Nós estudaremos melhor as camadas na próxima aula. **Se a questão não especificar, considere se tratar do Switch de Camada 2.**

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



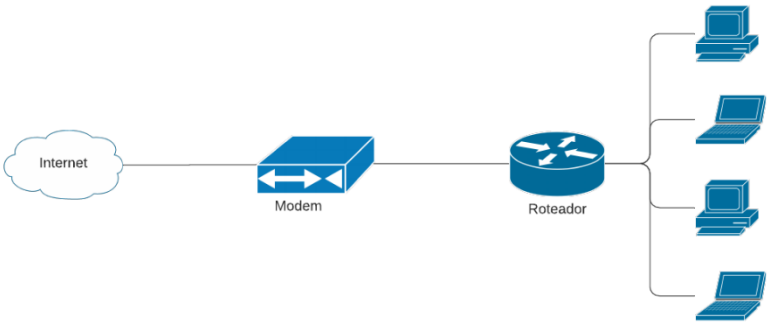
7.5 – Router (Roteador)

INCIDÊNCIA EM PROVA: ALTA



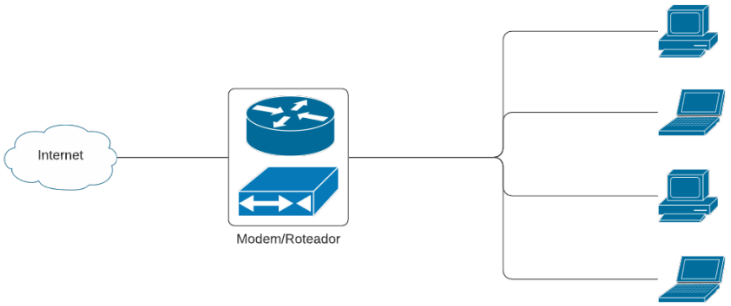
Os roteadores são equipamentos que permitem interligar redes diferentes e escolher a melhor rota para que uma informação chegue ao destino. Esse dispositivo encaminha ou direciona pacotes de dados entre redes de computadores, geralmente funcionando como uma ponte entre redes diferentes. Hoje em dia,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



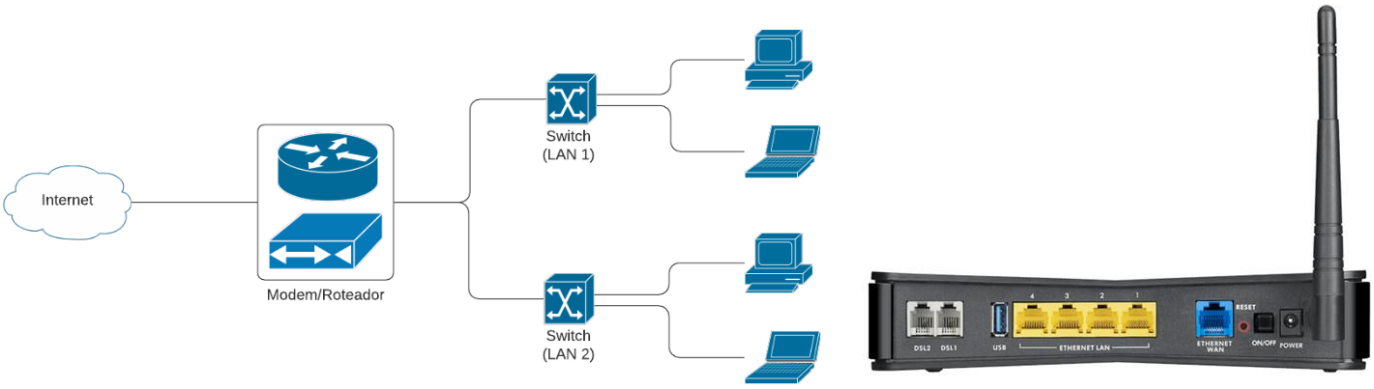
[6] Cada porta do switch possui um buffer (uma espécie de banco de memória) em que os dados são armazenados/enfileirados, não ocorrendo colisões, portanto não necessitando utilizar o Protocolo CSMA/CD.

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



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

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



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

No modo Hotspot, o roteador tem o simples objetivo de oferecer acesso à internet. *Como assim, Diego?* Vamos imaginar que você enjoou de estudar informática em casa e resolveu levar seu

notebook e estudar em uma cafeteria. Você chama o garçom, pede um espresso, uma água e... a senha do wi-fi! Vamos supor que a rede local da cafeteria é composta por cinco computadores, uma impressora e um banco de dados conectados em rede.

Ora... se o roteador wireless da cafeteria estiver configurado em modo hotspot, eu terei acesso simplesmente à internet, mas não terei acesso a notebooks de outros clientes ou aos computadores, impressora e banco de dados da cafeteria. **O hotspot é – apenas e tão somente – um local onde uma rede sem fio está disponível para ser utilizada.** Alguns estabelecimentos oferecem de forma gratuita (bares, restaurantes, etc) e outros são pagos (aeroportos e hotéis).



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

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

Apesar dessa diferença, é importante mencionar que popularmente é comum o tratamento de Hotspot e Access Point como sinônimos (inclusive em algumas provas). Por fim, esse roteador wireless pode também ser configurado como repetidor de sinais. *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?*

FIQUE ATENTO!

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.

7.6 – Modem

INCIDÊNCIA EM PROVA: MÉDIA



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

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

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



O Modem é um dispositivo eletrônico de entrada/saída de dados que modula um sinal digital em um sinal analógico a ser 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 Modens ADSL.**

Empresas de telefonia fixa ofereciam acesso em banda larga[7] 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...

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).

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

8 – 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)[8]
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)

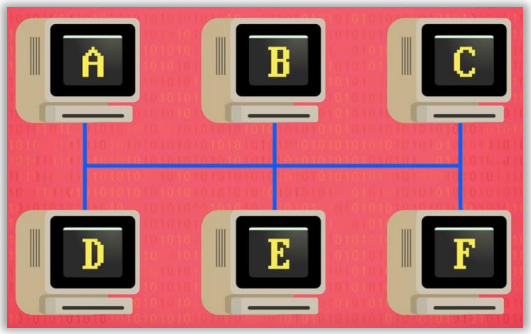
8.1 – Padrão Ethernet (IEEE 802.3)

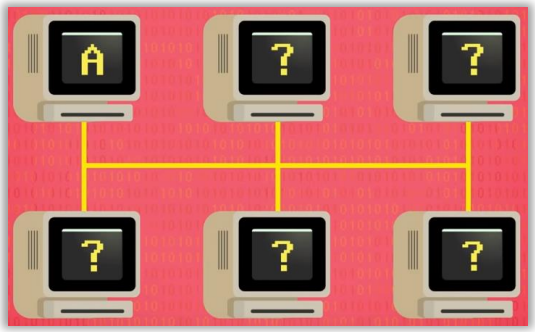
INCIDÊNCIA EM PROVA: ALTA

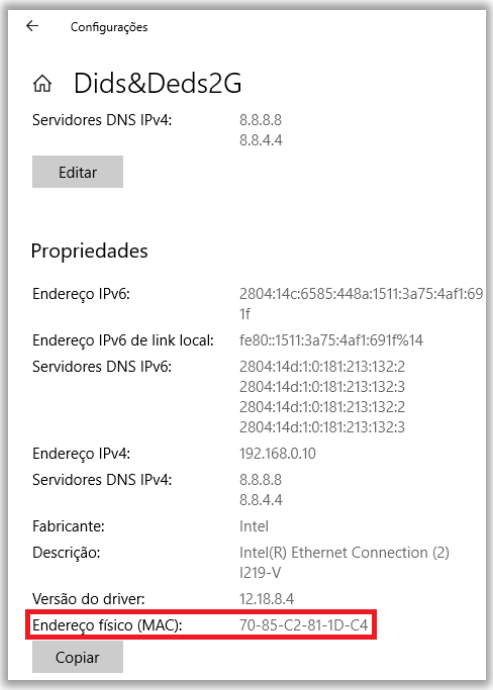
Ethernet é um conjunto de tecnologias e padrões que permite que dois ou mais computadores se comuniquem utilizando meios cabeados em uma Rede de Área Local (LAN). Notem que eu afirmei que é um conjunto de tecnologias e padrões, portanto nós vamos estudá-los por partes. Em relação à topologia utilizada, 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?*

[8] Para lembrar da numeração do Padrão Ethernet (que é o mais importante), lembre-se de: **ETHERNET → 3TH3RN3T**; e para lembrar da numeração do Padrão Wi-Fi (que também cai bastante), lembre-se de: **WI-FI → W1-F1**.



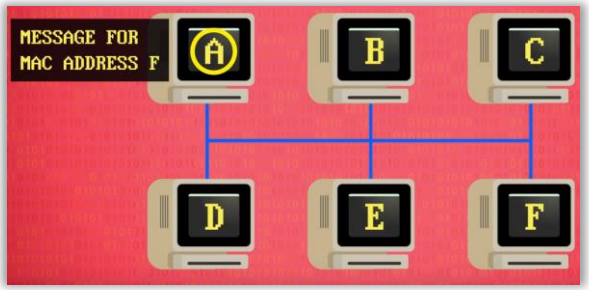


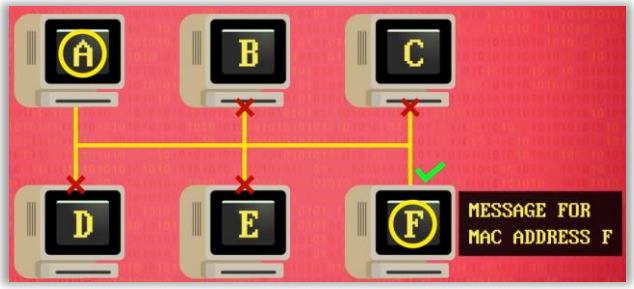


Na imagem acima, temos o *backbone* em azul porque nenhum sinal está sendo transmitido; e na imagem abaixo, temos o *backbone* em amarelo onde o sinal está sendo transmitido. **Notem que o *backbone* está todo amarelo porque – como a transmissão ocorre em *broadcast* – todas as máquinas o recebem.**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

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

Dessa forma, computadores na rede continuam recebendo os dados, mas só os processam quando eles verificam que é o endereço deles que está contido no prefixo. Vejam abaixo que o Computador A deseja enviar uma mensagem para o Computador F. Para tal, ele coloca o Endereço MAC do Computador F no prefixo da mensagem, que será processada por esse computador e 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 Mutiple Access* (CSMA), também conhecido como Acesso Múltiplo com Detecção de Portadora. Em outras palavras, trata-se de um protocolo utilizado na Ethernet para monitorar o meio de transmissão e evitar colisões quando ocorrem múltiplos acessos. Nós já estudamos esse problema no tópico de topologia em barramento, mas agora vamos detalhar um pouco mais.



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

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

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

Esse período poderia ser, por exemplo, um segundo! *Professor, se todos os computadores esperarem um segundo, isso não vai resultar no mesmo problema anterior?* 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**.

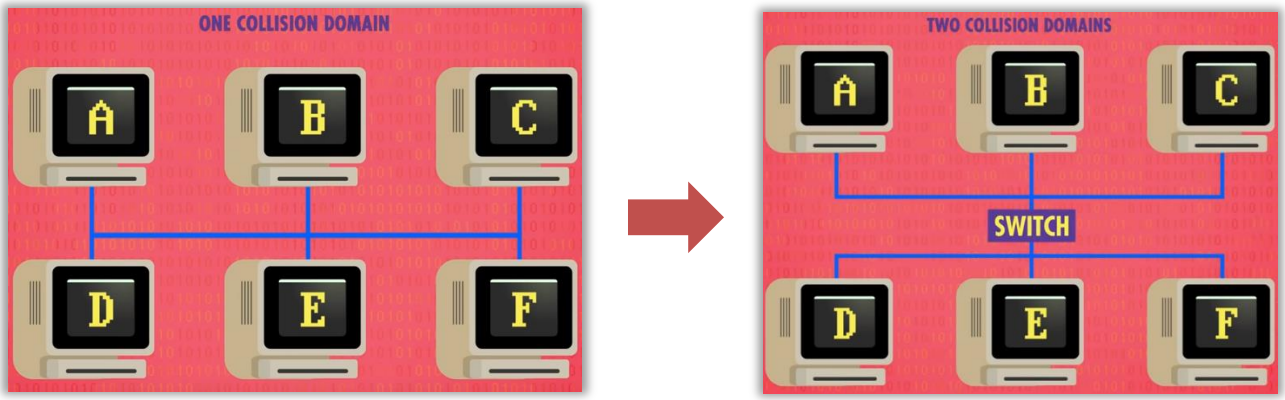
Lembrem-se que – para o mundo dos computadores – essa diferença de 0,2 segundos é uma eternidade. Logo, o primeiro computador verá que o meio de transmissão não está sendo utilizado e pode transmitir seus dados. 0,2 segundos depois, o segundo computador verá que o meio de transmissão não está sendo utilizado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

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

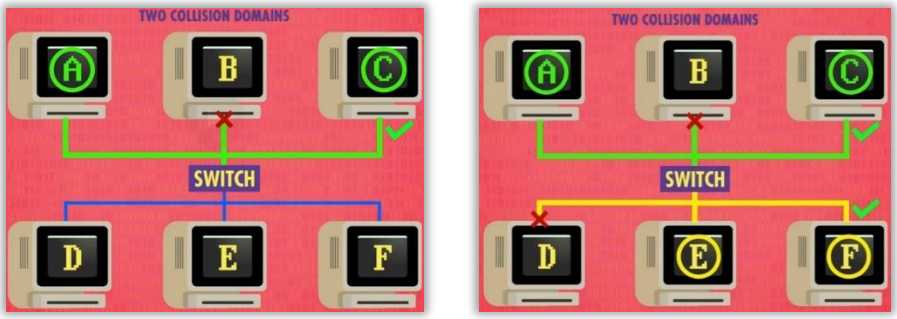
colisão, pode ser que a rede esteja congestionada, logo ele não esperará mais um segundo, esperará dois segundos. Se mesmo assim houver colisão, esperará quatro segundos. **Se continuar havendo colisões, esperará oito segundos, e assim por diante até conseguir transmitir**.

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

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



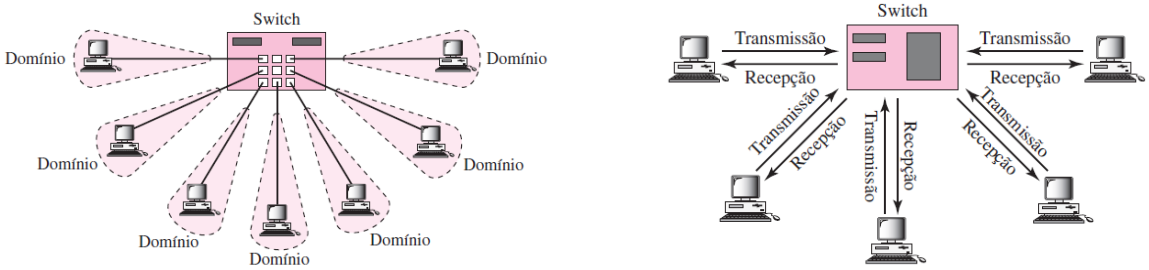
No exemplo anterior, nós tínhamos seis computadores conectados em um único meio de transmissão compartilhado, logo nós tínhamos um único domínio de colisão. Para reduzir a probabilidade de colisões, nós podemos segmentar a rede em dois domínios de colisão. *Como, Diego?* Nós podemos utilizar uma topologia em estrela com uso de um switch[9]. **Ele segmentará nossa rede em duas partes e ficará posicionado entre elas**.



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

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

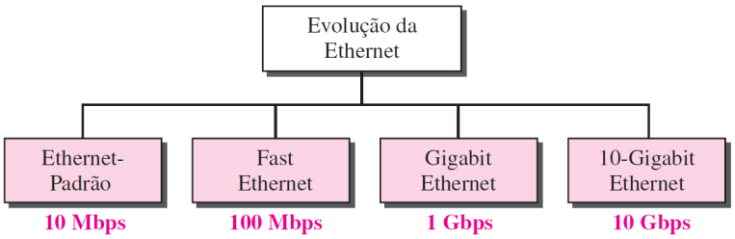
Notem que, se o Computador E quiser transmitir dados para o Computador F ao mesmo tempo que o Computador A transmite dados para o Computador C, a rede estará livre e as duas transmissões poderão ocorrer simultaneamente porque temos duas comunicações ocorrendo em dois domínios de colisão diferentes –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



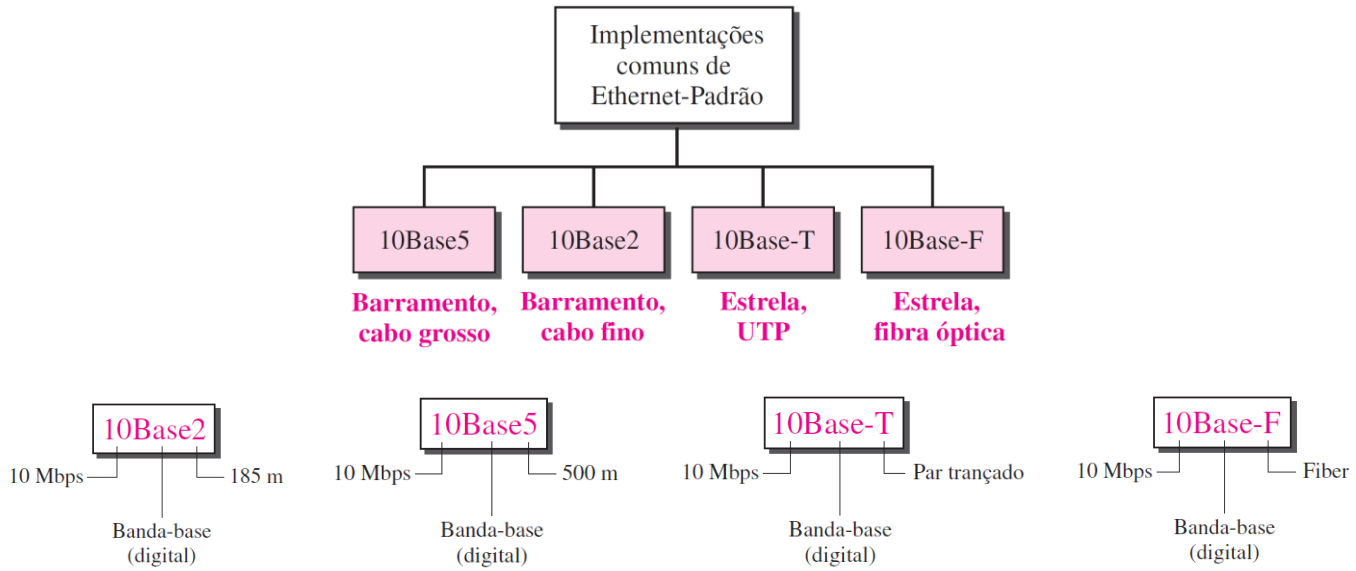
E digo mais: é possível criar um domínio de colisão para cada uma das portas de um switch (conforme apresenta à esquerda). Dessa forma, é possível eliminar toda e qualquer colisão! **Além disso, lembremos que o switch trabalha em full-duplex, ou seja, é capaz de enviar e receber dados simultaneamente,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

8.2 – Padrão Token Ring (IEEE 802.5)

INCIDÊNCIA EM PROVA: MÉDIA

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

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

8.3 – Padrão Wireless (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 Wireless – 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 Wireless 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 altas. 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-hoc[10].**

EVOLUÇÃO DO PADRÃO WI-FI (802.11)		
PADRÃO	FREQUÊNCIA	TAXA 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 +

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

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

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

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.

8.4 – Padrão Bluetooth (IEEE 802.15)

INCIDÊNCIA EM PROVA: BAIXA

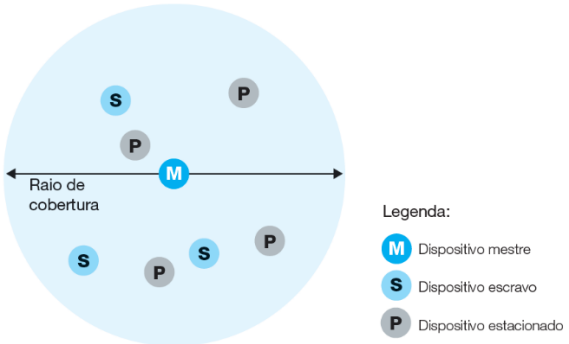


O Padrão Bluetooth tem o objetivo de integrar equipamentos periféricos. **Utilizado em Rede WPAN (Wireless Personal Area Network) – eles padronizam uma rede de baixo custo, curto alcance, baixas taxas de transmissão e sem fio**. Eles operam na faixa de 2.4 Ghz de forma ad-hoc por meio de sua unidade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

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

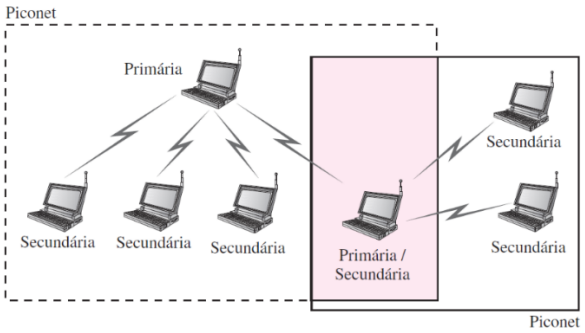
Além dos dispositivos escravos, a piconet também pode conter até 255 dispositivos estacionados. *Como assim, Diego?* Um dispositivo estacionado não pode se comunicar até que o dispositivo mestre altera seu estado de inativo para ativo. **Um dispositivo escravo que se encontre no estado estacionado permanece 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.



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

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



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

8.5 – 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).

INTERNET

1 - 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 diferente, 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.**

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

Antigamente havia um emprego que hoje em dia não existe mais: telefonista! *Quem aí já ouviu falar?* Pois é! Naquela época, quando alguém queria ligar para um amigo, era necessário ligar primeiro para uma central telefônica. Nesse local, havia centenas de operadoras que recebiam a sua ligação, perguntavam para quem você queria ligar, e só então conectavam você ao telefone do seu amigo[13]. **Essa comunicação funcionava por meio da comutação por circuito!**

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...

---

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

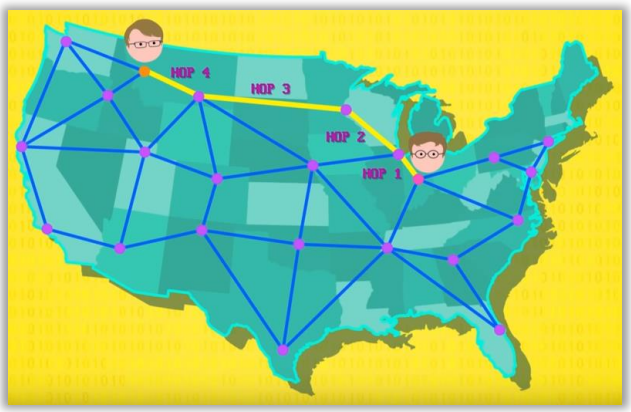
O principal problema é o desperdício de recursos! **Poxa... quando um dispositivo de origem estabelece uma conexão com um dispositivo de destino, fecha-se uma conexão e ambas as linhas permanecem dedicadas mesmo que não esteja havendo comunicação.** Imaginem que eu estou falando com um amigo no telefone,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

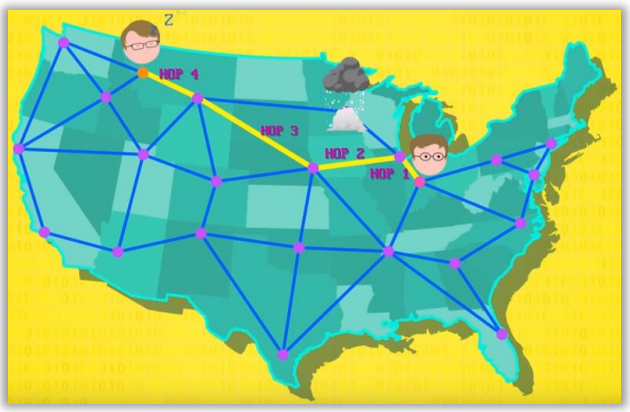
Além disso, a comutação por circuito só permite que eu telefone para uma única pessoa simultaneamente – eu não consigo conversar com dois amigos simultaneamente. *Já imaginaram se a internet funcionasse assim?* Nesse caso, seu computador só poderia se conectar a um único dispositivo ao mesmo tempo. **Seria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

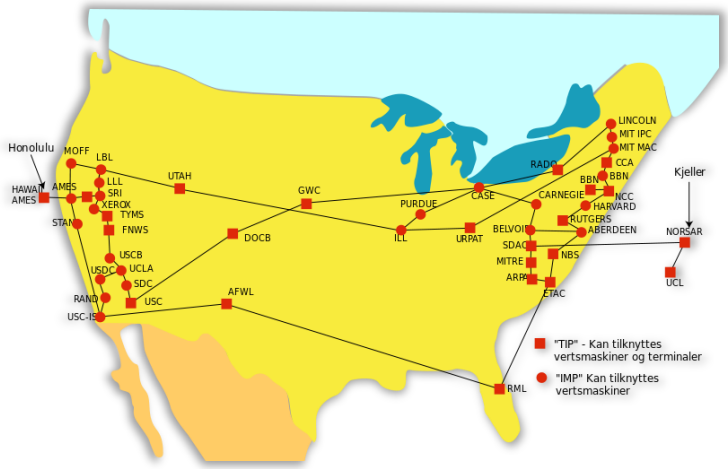


Quando se envia dados pela internet, não é possível prever o caminho percorrido pelo pacote até chegar ao seu destino final. Cada pacote enviado pode seguir por uma rota diferente chegando em ordem diferente da ordem enviada (claro que, após todos os pacotes chegarem, o arquivo é remontado na forma original).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

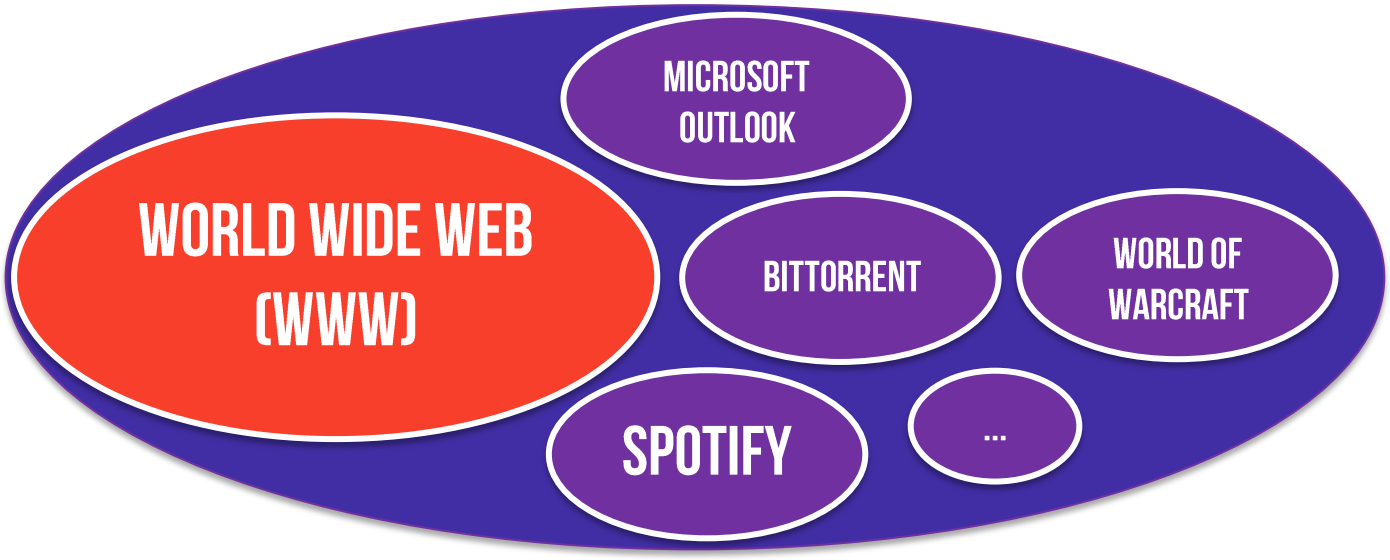
Esses são os serviços principais, mas existem muitos outros oferecidos via Internet (Ex: grupos de discussão, mensagens instantâneas, bate-papo, redes sociais, computação em nuvem, etc).

2 – 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).



3 – 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!

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

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



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 comum[14], 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.

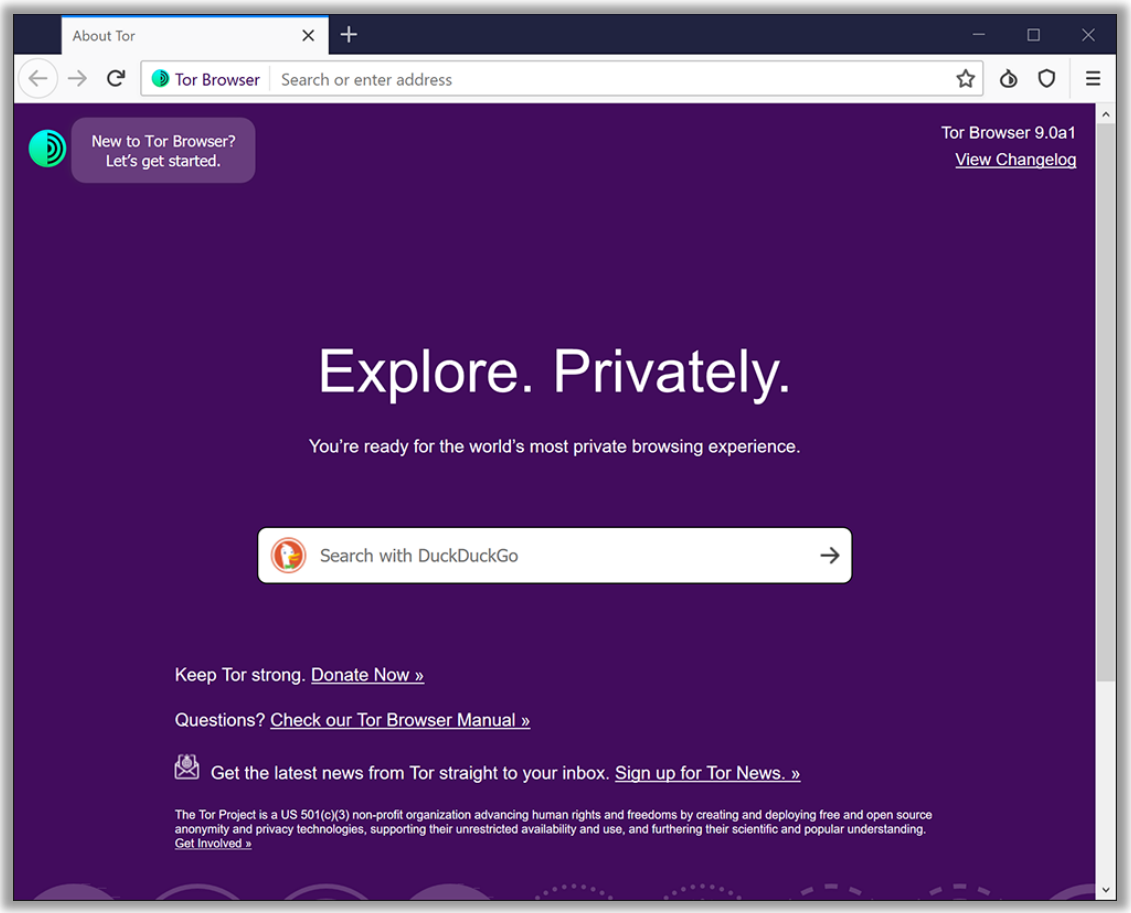
Eita, professor... deixa eu acessar rapidinho aqui essa tal de Rede Tor! Nope, você não conseguirá! A Dark Web não é acessível por meio de navegadores comuns, tais como Chrome, Firefox, entre outros (exceto com configurações específicas de proxy). Para acessar a Rede Tor, é necessário utilizar um navegador 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**[15]. Vocês não precisam entender como isso funciona, vocês só precisam entender que os dados passam por uma série de camadas de encriptação de modo que seja praticamente impossível identificar de onde veio a requisição.

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

[14] **Exemplo:** *http://3g2upl4pq6kufc4m.onion* ou *http://msydqstlz2kzerdg.onion*.

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

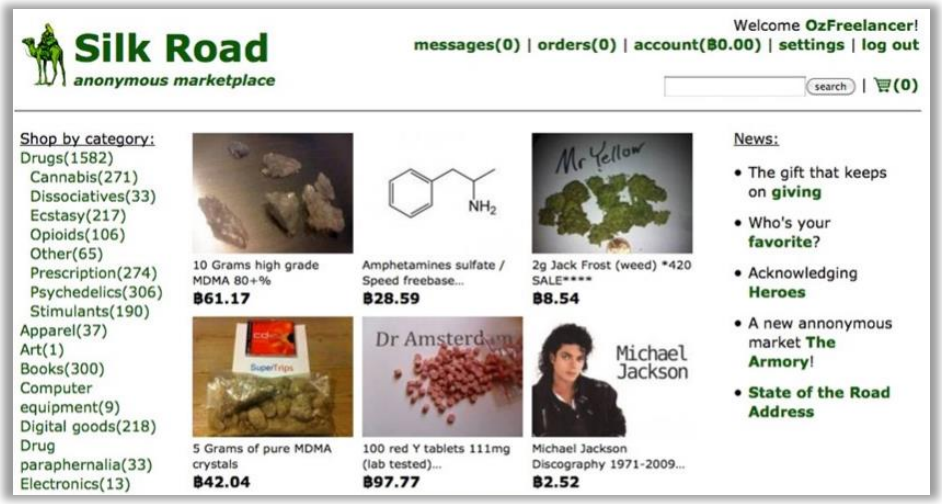


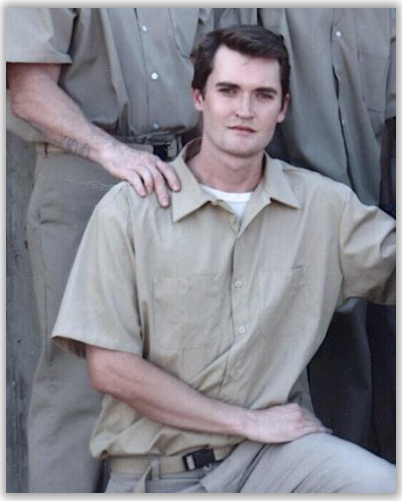
Professor, você disse que as pessoas acessam a Dark Web por motivos legítimos e ilegítimos. Eu estou agoniado, desembucha logo e fala o que é que tem de ilegítimo lá!

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.

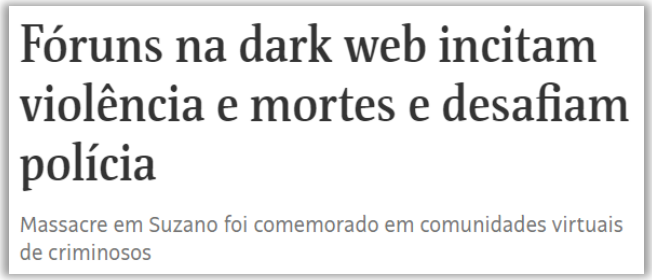
Eu sei que essa aula atiça a curiosidade de várias pessoas, mas eu já adianto que não recomendo que vocês acessem esses sites. Saibam que se trata de um ambiente em que é possível encontrar um bocado de hackers, cibercriminosos e outros profissionais desse tipo. Eu já recebi perguntas de alunos perguntando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

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





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



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 :)

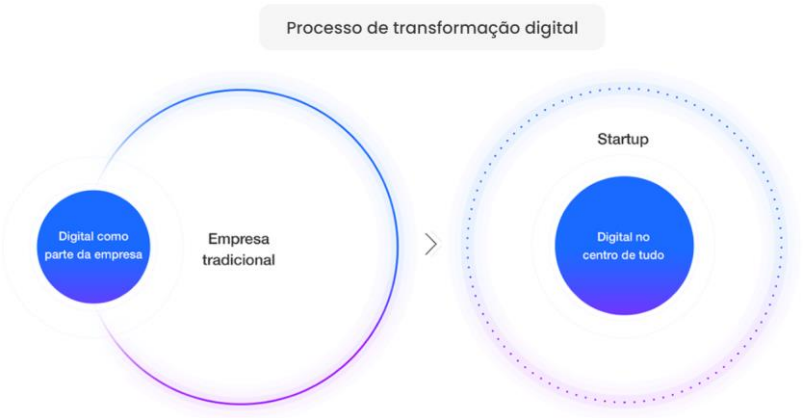
4 – Internet das Coisas (IoT)

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.

Galera, 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, pecurária, hospitais, escolas, fábricas, transporte público, lojas, serviços públicos, logística, entre outros.

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?*

5 – Tecnologias de Acesso

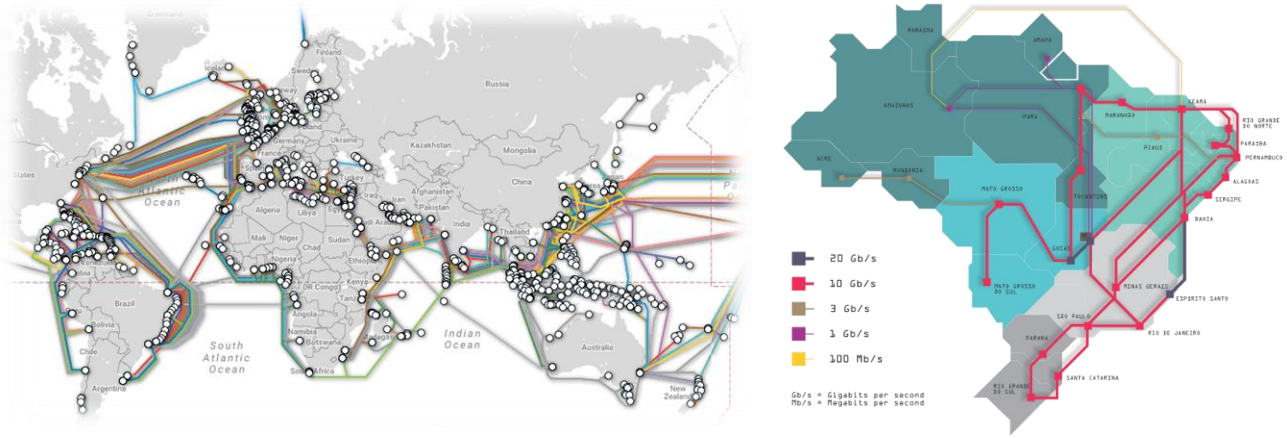
Galera, até o início da década de noventa, só quem sabia o que era internet eram pesquisadores ligados a universidades, ao governo ou à indústria. No entanto, quando um físico chamado Tim Berners-Lee criou a Web (WWW), houve uma mudança nessa realidade e a internet ganhou milhões de novos usuários sem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

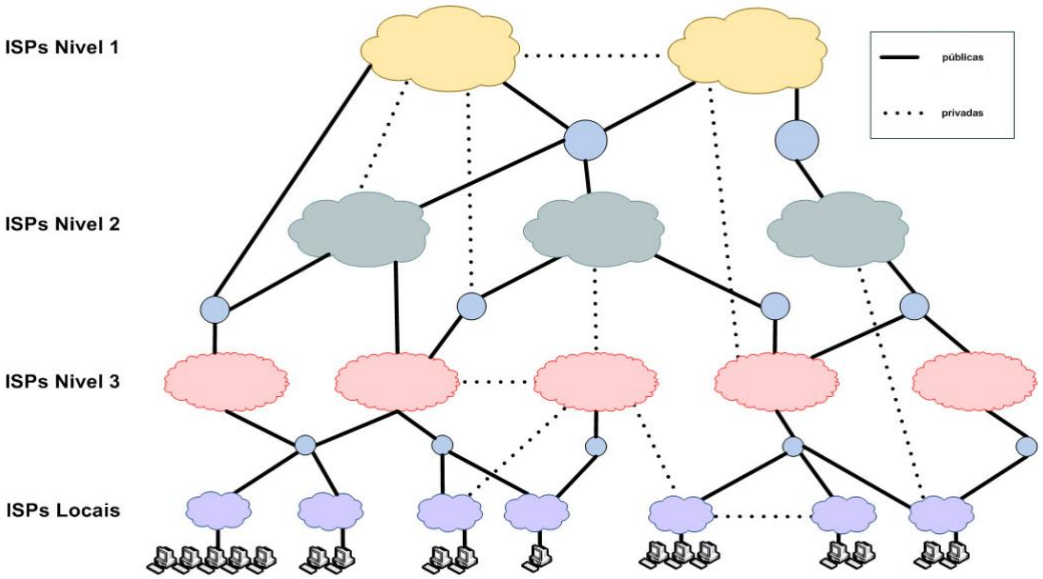
Vamos detalhar isso melhor! A internet pode ser fornecida por meio de satélites, ondas de rádio ou uma rede de milhares de cabos de fibra óptica terrestres ou submarinos, que conectam diversos países, respondendo por 80% de toda a comunicação. **Essa infraestrutura de redes – que forma a espinha dorsal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

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



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

Existem três níveis de 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).



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:

5.1 – Dial-Up

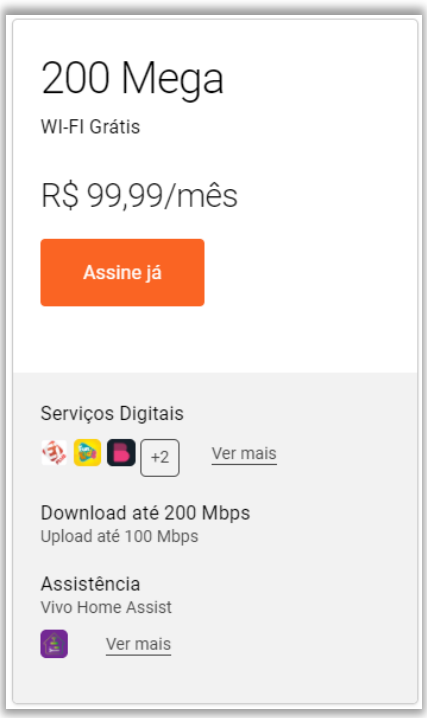
INCIDÊNCIA EM PROVA: MÉDIA

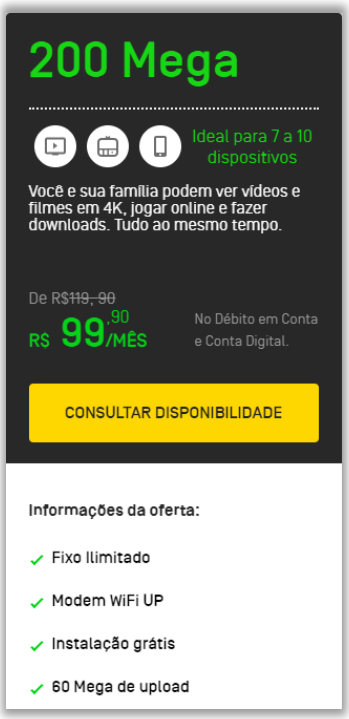
Trata-se de uma conexão discada através de um modem e uma linha de telefonia fixa. Era a maneira mais popular de acesso da década de 90, hoje encontra-se em desuso. Apresenta um alto custo de implementação, é bastante instável e possui baixas taxas de transmissão. *Era banda larga?* Não, era banda estreita – 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!

5.2 – ADSL

INCIDÊNCIA EM PROVA: MÉDIA

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





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

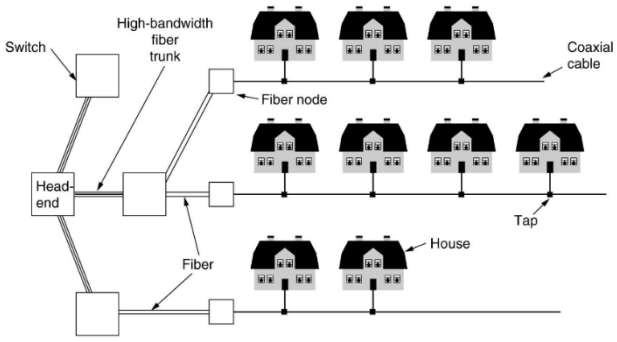
Vejam no exemplo anterior que a taxa de download à esquerda é de 200 mbps e a taxa de upload é de 100 mbps; a taxa de download à direita é de 200 mbps e a taxa de upload é 60 mbps. *Isso faz diferença, Diego?* Dependerá do seu perfil de utilização! **Se você costuma apenas fazer navegar na**

web, assistir um filme, baixar aulas – não há nenhum problema; mas se você tem um canal no Youtube e precisa fazer uploads de vídeos grandes – pode ser inconveniente.

5.3 – 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.

5.4 – 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?*

5.5 – 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.

5.6 – Radiodifusão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



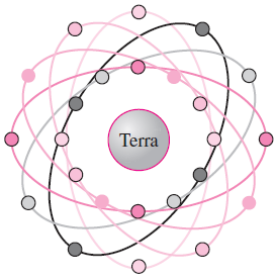
Trata-se da tecnologia que permite o acesso à internet banda larga via radiofrequência. As ondas de rádio, em sua maior parte, são omnidirecionais, isto é, quando uma antena transmite ondas de rádio, elas se propagam em todas as direções em broadcast. Elas podem percorrer grandes distâncias e podem atravessar paredes, não necessitando que antenas transmissoras estejam completamente alinhadas. No entanto, não pode haver grandes obstáculos entre o emissor e o receptor de sinal, como montanhas.

Trata-se de uma boa alternativa quando não é possível utilizar uma rede cabeada, no entanto existem também diversas desvantagens: ondas de rádio podem sofrer interferências de outras ondas; a geografia entre as antenas pode ser um impeditivo; está bastante sujeito a intempéries climáticas como tempestades e vendavais; entre outros. **Não é muito utilizado em meios urbanos, mas é uma boa alternativa para meios rurais, onde cabos não estão disponíveis.**

5.7 – 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.**

5.8 – 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).
2ª 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 cellular. 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).

QUESTÕES COMENTADAS - CESPE

1. **(CESPE / Câmara dos Deputados – 2014)** A Internet foi criada a partir de um órgão conhecido como ARPAnet, que estava vinculado diretamente ao departamento de defesa americano.

Comentários:

A internet foi criada por uma agência governamental chamada ARPA (*Advanced Research Projects Agency*), que realmente estava vinculada ao departamento de defesa americano. Já ARPANET foi a rede de computadores que deu origem a Internet. Em outras palavras, a questão só trocou o nome do órgão pelo nome da rede.

Gabarito: Errado

---

2. **(CESPE / TJ-AM – 2019)** Apesar de a Internet ser uma rede mundial de acesso amplo e gratuito, os usuários domésticos a utilizam por meio de algum provedor de acesso à Internet, isto é, uma empresa privada que cobra pelo acesso ao serviço.

Comentários:

Essa questão é polêmica e, para mim, deveria ser anulada por ambiguidade. *Por que, Diego?* Galera, o acesso à internet é público, mas não é gratuito. Em outras palavras, todo mundo pode acessá-la, desde que pague a um provedor de acesso. Logo, apesar de a Internet ser uma rede mundial de acesso amplo ou público, ela não tem acesso gratuito. Dessa forma, discordo do gabarito!

Gabarito: Correto

---

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

Comentários:

Perfeito! A unidade básica do Bluetooth é realmente a Piconet. Ela contém um nó e até sete escravos ativos. Por fim, a distância realmente depende da potência dos transmissores.

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

Gabarito: Correto

4. **(CESPE / TELEBRÁS – 2015)** Redes de comunicação do tipo ponto a ponto são indicadas para conectar, por exemplo, matriz e filiais de uma mesma empresa, com altas taxas de velocidade de conexão.

Comentários:

Essa foi uma questão um pouco polêmica, porque termo "ponto-a-ponto" pode ser utilizado em dois contextos diferentes: pode ser ponto-a-ponto como um contraponto ao modelo de rede cliente-servidor ou pode ser ponto-a-ponto como um contraponto ao tipo de enlace ponto-multiponto. Como eu vou saber a qual deles a questão se refere? A única maneira é por meio da avaliação do termo 'redes de comunicação'.

Se fosse *'redes de computadores'*, nós poderíamos presumir que se tratava do modelo de rede ponto-a-ponto, mas como ele diz *'redes de comunicação'*, que tem um sentido mais amplo que 'redes de computadores', nós podemos inferir que se trata do tipo de enlace. A questão fala em um enlace capaz de conectar matrizes e filiais, logo ele não é compartilhado por outras redes - apenas as matrizes e as filiais dessa rede podem ser comunicar por esse enlace.

Assim, ele é capaz de fornecer altas taxas de velocidade de conexão, visto que o enlace (também chamado de link) não é compartilhado com outras máquinas de fora da rede.

Gabarito: Correto

5. **(CESPE / MPU – 2013)** Um equipamento de interconexão de redes com três hosts a ele conectados, em que um host envia um frame unicast para o outro, e o terceiro nó age passivamente, capturando a comunicação, é um hub ou um switch.

Comentários:

Essa questão tem várias nuances: 1. Hub reconhece bits e, não, frames porque ele trabalha na camada física e, não, na camada de enlace; 2. Como o terceiro nó capturou a comunicação, faz sentido ser um hub - ele recebeu dados que seriam unicast, mas como ele trabalha apenas em broadcast, todos os outros nós receberam; 3. Em princípio, não faz sentido ser um switch porque o switch isola o tráfego nas portas, portanto o terceiro nó não receberia o frame; 4. Agora vem o grande lance da questão: enquanto o switch ainda não identificou os nós, isto é, sua tabela que armazena os endereços físicos dos equipamentos ainda não possui dados que identificam os dispositivos conectados a ele, é possível que o terceiro nó receba o frame (justamente para ajudar a montar a tabela de endereçamento). Há outras possibilidades também, como Port Mirroring, mas não vou entrar nesses detalhes.

Enfim... questão pesada e que cobra uma exceção, mas está correta.

Gabarito: Correto

---

6. **(CESPE / Polícia Federal – 2012)** O uso de dispositivos bluetooth em portas USB necessita de driver especial do sistema operacional. Em termos de funcionalidade, esse driver equivale ao de uma interface de rede sem fio (wireless LAN), pois ambas as tecnologias trabalham com o mesmo tipo de endereço físico.

Comentários:

Nada melhor do que a justificativa da própria banca para o item:

Normalmente, o driver de um dispositivo bluetooth usa um driver especial fornecido pelo fabricante do hardware em questão, que pode ou não estar embutido na lista de drivers do sistema operacional. Logo o driver não é especial do sistema operacional. É um driver externo ao sistema operacional e fornecido pelo fabricante do hardware, que pode ou não ser incorporado ao sistema operacional. Em termos de funcionalidade, bluetooth é amplamente diferente de uma interface Wlan, principalmente em termos de restrições de uso. Alguns exemplos são: a largura de banda do bluetooth é pequena, enquanto de Wlan é alta. O alcance do bluetooth está restrito a alguns metros, enquanto que Wlan chega até a 300 metros. Além do que são tecnologias de rede sem fio diferentes. Logo o item está errado.

Gabarito: Errado

---

7. **(CESPE / BRB – 2011)** O acesso à Internet em alta velocidade por meio de conexão dial-up, via linha telefônica, também conhecido como serviço ADSL, dispensa o uso de modem, visto que, nesse caso, a conexão ocorre diretamente a partir de infraestrutura das empresas de telefonia fixa ou móvel (celular).

Comentários:

O serviço ADSL não se dá por meio de conexão dial-up, via linha telefônica. Ademais, ele necessita do uso de um Modem ADSL (diferente do modem convencional para acesso discado), porém não precisa converter o sinal de digital para analógico porque o sinal é sempre digital (*Asymetric Digital Subscriber Line*). Por fim, ele ocorre a partir da infraestrutura das empresas de telefonia fixa e, não, móvel.

Gabarito: Errado

---

8. **(CESPE / Polícia Federal – 2018)** Situação hipotética: Múltiplos hospedeiros devem ser conectados a LANs sem fio, a redes por satélite e a redes de fibra (HFC). Para isso, deve-se escolher entre dois tipos de canais distintos, em função das características da camada de enlace:

difusão (broadcast) ou ponto a ponto. Assertiva: Nessa situação, deve-se fazer a conexão dos hospedeiros por meio de difusão.

Comentários:

Vamos por partes: a questão afirma que múltiplos hospedeiros devem ser conectados a LANs sem fio, a redes por satélite e a redes de fibra (HFC). Dessa forma, a situação hipotética traz diversas máquinas que devem ser conectadas por tecnologias de acesso à internet diferentes. Uma LAN sem fio é também chamada de WLAN; uma rede via satélite é aquela que conecta satélites orbitando a Terra; e uma rede HFC é aquela que combina cabos de fibra óptica e cabo coaxial.

A questão afirma que, para conectar os múltiplos hospedeiros, deve-se escolher dois tipos de canais distintos: difusão ou ponto-a-ponto. Se eu conectar vários hospedeiros a uma rede local sem fio, a transmissão será em difusão porque toda transmissão enviada será recebida por todos os outros hospedeiros; se eu conectar vários hospedeiros a uma rede via satélite, a transmissão também será em difusão porque toda transmissão enviada será recebida por todos os outros hospedeiros.

A grande dúvida da questão está relacionada à Rede HFC. Nós vimos em aula que o cabo coaxial que sai do receptor óptico forma um barramento compartilhado, portanto a transmissão também será em difusão porque toda transmissão enviada será recebida por todos os outros hospedeiros.

Gabarito: Correto

---

9. **(CESPE / ME – 2020)** O switch envia os quadros somente para a porta de destino, por meio da análise do quadro e da obtenção do MAC (Media Access Control) destino, o qual é checado em uma tabela interna que contém todos os endereços MAC das interfaces de rede dos computadores da rede.

Comentários:

Perfeito! *O switch envia quadros?* Sim, essa é a unidade adequada. *Ele envia quadros apenas para a porta de destino?* Sim, porque ele é capaz de trabalhar em unicast. *Isso é feito por meio da análise do quadro e do endereço MAC de destino?* Sim, o switch possui uma tabela interna dinâmica que automaticamente associa endereços aos computadores conectados.

Gabarito: Correto

---

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

a) VoIP (voice over IP).
b) PGP (Pretty Good Privacy).

c) LAN (local area network).
d) SSL (secure sockets layer).
e) WAN (wide area network).

Comentários:

Se as empresas estão localizadas em continentes diferentes, trata-se uma Rede WAN.

Gabarito: Letra E

---

11. **(CESPE / PGE-PE – 2019)** Uma topologia de rede híbrida pode combinar características de topologias tanto em barramento quanto em anel, por exemplo.

Comentários:

Perfeito! A topologia híbrida é a combinação de duas ou mais topologias.

Gabarito: Correto

---

12. **(CESPE / FUB – 2018)** Em comparação com os fios de cobre, as fibras ópticas têm como desvantagem a baixa imunidade a interferências eletromagnéticas e à ação corrosiva de alguns elementos químicos presentes na atmosfera.

Comentários:

Na verdade, fibras ópticas possuem maior imunidade a interferências eletromagnéticas e à ação corrosiva de alguns elementos químicos na atmosfera.

Gabarito: Errado

---

13. **(CESPE / SEFAZ-RS – 2018)** Assinale a opção que indica equipamento que permite estabelecer a comunicação entre duas redes LAN (local area network) distintas que empregam cabeamento padrão UTP.

a) hub
b) storage
c) access point
d) roteador
e) conector de fibra óptica

Comentários:

(a) Errado, não conecta redes distintas; (b) Errado, é um equipamento para armazenamento de dados; (c) Errado, é um equipamento utilizado para estender recursos de uma rede local; (d) Correto, é responsável por interconectar redes distintas; (e) Errado, não faz nenhum sentido.

Gabarito: Letra D

---

14. (CESPE / SEFAZ-RS – 2018) Em redes locais, determinados equipamentos concentram o tráfego de dados entre os computadores. Alguns deles replicam os dados para todos os computadores da rede; outros permitem o tráfego de dados somente para o computador destinatário. Assinale a opção que apresenta equipamento utilizado para concentrar e transmitir dados somente ao computador destinatário, sem replicá-los a outros computadores conectados à mesma rede.

a) smartphone
b) hub
c) switch
d) conector RJ-45
e) impressora

Comentários:

(a) Errado, não faz nenhum sentido; (b) Errado, ele transmite os dados para todos os computadores em broadcast; (c) Correto, ele realmente permite transmitir dados em unicast, sem replicá-los a outros computadores; (d) Errado, não faz nenhum sentido; (e) Errado, o examinador viajando!

Gabarito: Letra C

---

15. (CESPE / SEFAZ-RS – 2018) Assinale a opção que apresenta o padrão que especifica a operação de uma rede local sem fio com velocidade acima de 300 Mbps.

a) IEEE 802.11n
b) IEEE 802.11c
c) IEEE 802.11b
d) IEEE 802.11g
e) IEEE 802.11a

Comentários:

Bastava lembrar da nossa tabelinha! Trata-se do IEEE 802.11n.

EVOLUÇÃO DO PADRÃO WI-FI (802.11)		
PADRÃO	**FREQUÊNCIA**	**TAXA 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 +

Gabarito: Letra A

---

16. (CESPE / Polícia Federal – 2018) Por meio de uma LAN sem fio embasada na tecnologia IEEE 802.11, é possível que os usuários transmitam (e recebam) pacotes para (e de) um ponto de acesso conectado a uma rede de computadores com fio conectada à Internet.

Comentários:

Sabendo que LAN Sem Fio = WLAN (IEEE 802.11), é realmente possível existir um Access Point (Ponto de Acesso) conectado a uma rede com fio conectada à internet e, assim, usuários podem transmitir e receber pacotes. Aliás, o objetivo de um Access Point é justamente estender recursos de uma rede local para uma rede sem fio.

Gabarito: Correto

---

17. (CESPE / Polícia Federal – 2018) Em uma rede local que possui a topologia estrela, podem ser utilizados switches para integrar a comunicação entre os computadores.

Comentários:

Perfeito! Switches permitem centralizar a comunicação entre computadores, separando-os em diferentes domínios de colisão.

Gabarito: Correto

---

18. (CESPE / EBSERH – 2018) Um switch camada 2 (layer 2) pode substituir um roteador que interliga três redes de comunicação diferentes, desde que se apliquem as mesmas regras de roteamento que estão configuradas no roteador.

Comentários:

Na verdade, um Switch Camada 3 (Layer 3) pode substituir um roteador que interliga três redes de comunicação diferentes, desde que se apliquem as mesmas regras de roteamento que estão configuradas no roteador. Um Switch Camada 2 não tem essa capacidade!

Gabarito: Errado

---

19. **(CESPE / EBSERH – 2018)** Uma empresa que precise interligar suas filiais, em Brasília e no Rio de Janeiro, por meio de uma mesma rede de comunicação, deverá implantar uma rede do tipo WAN, que disponibiliza serviços de rede acessíveis de forma geograficamente distribuída.

Comentários:

Perfeito! A rede que interliga capitais diferentes é considerada uma Rede WAN.

Gabarito: Correto

---

20. **(CESPE / EBSERH – 2018)** O endereço físico MAC está associado à interface de comunicação que identifica, de forma única, cada dispositivo conectado a uma rede de computadores.

Comentários:

Perfeito! Endereço Físico (também chamado de Endereço MAC) está associado à interface de um dispositivo de rede e possui um identificador único.

Gabarito: Correto

---

21. **(CESPE / STJ – 2018)** O cabo coaxial, se comparado aos cabos de par trançado, tem maior largura de banda e apresenta maior atenuação do sinal.

Comentários:

Perfeito! Ele realmente possui maior largura de banda em relação ao cabo de par trançado, além de apresentar maior atenuação de sinal.

Gabarito: Correto

---

22. **(CESPE / STJ – 2018)** Devido à sua estrutura, em uma rede usando a topologia estrela, o isolamento de falhas é uma tarefa complexa, o que representa uma desvantagem dessa topologia.

Comentários:

Na verdade, o simples isolamento de falhar é uma das vantagens da topologia estrela. Se a rede inteira cair, o problema é no dispositivo central; se apenas uma máquina cair, o problema é nessa máquina ou no enlace que a conecta ao dispositivo central.

Gabarito: Errado

---

23. **(CESPE / STJ – 2018)** A topologia anel tem a fragilidade de tornar a rede inoperável ao tráfego unidirecional. Para transpor essa fragilidade, faz-se necessária a utilização de uma topologia híbrida.

Comentários:

Não faz o menor sentido! A topologia em anel é inerentemente simplex (unidirecional), logo não pode tornar a rede inoperável. Como uma interrupção no anel pode derrubar toda a rede, pode ser considerada frágil, mas há alternativas que permitem mitigar essa fragilidade, como um anel duplo, redundâncias, entre outros.

Gabarito: Errado

---

24. **(CESPE / STJ – 2018)** A rede mostrada na figura a seguir, em que as linhas representam conexões entre computadores, apresenta topologia mesh.



Comentários:

Na verdade, essa figura representa uma topologia em barramento.

Gabarito: Errado

---

25. **(CESPE / STJ – 2018)** Em um roteador, as conexões LAN são dedicadas aos equipamentos da rede interna, enquanto a conexão WAN deve ser conectada ao gateway para garantir acesso à Internet.

Comentários:

Perfeito! Em um roteador, você encontrará provavelmente 4 Portas LAN e 1 Porta WAN. As Portas LAN são dedicadas a conectar equipamentos da rede interna e a Porta WAN é utilizada para conectar o cabo que vem do Modem com o sinal da Internet.



Gabarito: Errado

---

26. (CESPE / STJ – 2018) Diferentemente de roteadores, que encaminham os pacotes apenas aos equipamentos de destino, os switches encaminham os pacotes a todos os equipamentos que estão conectados na rede.

Comentários:

Tanto roteadores quanto switches podem trabalhar em unicast. O equipamento que encaminha pacotes a todos os equipamentos que estão conectados a ele – em broadcast – é o hub.

Gabarito: Errado

---

27. (CESPE / STJ – 2018) Em uma rede local sem fio que utilize equipamentos de access point operando no padrão IEEE 802.11b, o tráfego de dados pode atingir velocidade de até 54 Mbps.

Comentários:

Bastava lembrar da nossa tabelinha! IEEE 802.11b tem taxa de transmissão máxima de 11 Mbps.

EVOLUÇÃO DO PADRÃO WI-FI (802.11)		
PADRÃO	FREQUÊNCIA	TAXA 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 +

Gabarito: Errado

---

28. (CESPE / STJ – 2018) Com a finalidade de interligar duas ou mais redes de dados diferentes, podem-se utilizar roteadores ou switches conhecidos como layer 3 ou camada 3.

Comentários:

Perfeito! Roteadores e Switches Layer 3 são equipamentos cuja função principal é interligar duas ou mais redes distintas.

Gabarito: Correto

---

29. (CESPE / ABIN – 2018) Nas redes locais de difusão do tipo anel, há necessidade de se definir alguma regra para arbitrar os acessos simultâneos ao enlace.

Comentários:

Redes do tipo anel são redes de difusão? Sim, elas trabalham em broadcast – dados enviados são recebidos por todos os outros dispositivos. *Há necessidade de se definir alguma regra para arbitrar os acessos simultâneos ao enlace?* Sim, essa regra é a posse do token!

Gabarito: Correto

---

30. **(CESPE / ABIN – 2018)** Bluetooth é uma tecnologia de substituição de cabos que permite alcance médio com velocidade mais alta e potência maior que a da tecnologia IEEE 802.11.

Comentários:

Tecnologia IEEE 802.11 é o Wi-Fi! Bluetooth realmente é uma tecnologia de substituição de cabos, porém seu alcance é curto, sua velocidade é mais baixa e sua potência é menor que a do Wi-Fi.

Gabarito: Errado

LISTA DE QUESTÕES – CESPE

1. **(CESPE / Câmara dos Deputados – 2014)** A Internet foi criada a partir de um órgão conhecido como ARPAnet, que estava vinculado diretamente ao departamento de defesa americano.

2. **(CESPE / TJ/AM – 2019)** Apesar de a Internet ser uma rede mundial de acesso amplo e gratuito, os usuários domésticos a utilizam por meio de algum provedor de acesso à Internet, isto é, uma empresa privada que cobra pelo acesso ao serviço.

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

4. **(CESPE / TELEBRÁS – 2015)** Redes de comunicação do tipo ponto a ponto são indicadas para conectar, por exemplo, matriz e filiais de uma mesma empresa, com altas taxas de velocidade de conexão.

5. **(CESPE / MPU – 2013)** Um equipamento de interconexão de redes com três hosts a ele conectados, em que um host envia um frame unicast para o outro, e o terceiro nó age passivamente, capturando a comunicação, é um hub ou um switch.

6. **(CESPE / Polícia Federal – 2012)** O uso de dispositivos bluetooth em portas USB necessita de driver especial do sistema operacional. Em termos de funcionalidade, esse driver equivale ao de uma interface de rede sem fio (wireless LAN), pois ambas as tecnologias trabalham com o mesmo tipo de endereço físico.

7. **(CESPE / BRB – 2011)** O acesso à Internet em alta velocidade por meio de conexão dial-up, via linha telefônica, também conhecido como serviço ADSL, dispensa o uso de modem, visto que, nesse caso, a conexão ocorre diretamente a partir de infraestrutura das empresas de telefonia fixa ou móvel (celular).

8. **(CESPE / Polícia Federal – 2018)** Situação hipotética: Múltiplos hospedeiros devem ser conectados a LANs sem fio, a redes por satélite e a redes de fibra (HFC). Para isso, deve-se escolher entre dois tipos de canais distintos, em função das características da camada de enlace: difusão (broadcast) ou ponto a ponto. Assertiva: Nessa situação, deve-se fazer a conexão dos hospedeiros por meio de difusão.

9. **(CESPE / ME – 2020)** O switch envia os quadros somente para a porta de destino, por meio da análise do quadro e da obtenção do MAC (Media Access Control) destino, o qual é checado em uma tabela interna que contém todos os endereços MAC das interfaces de rede dos computadores da rede.

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

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

11. **(CESPE / PGE-PE – 2019)** Uma topologia de rede híbrida pode combinar características de topologias tanto em barramento quanto em anel, por exemplo.

12. **(CESPE / FUB – 2018)** Em comparação com os fios de cobre, as fibras ópticas têm como desvantagem a baixa imunidade a interferências eletromagnéticas e à ação corrosiva de alguns elementos químicos presentes na atmosfera.

13. **(CESPE / SEFAZ-RS – 2018)** Assinale a opção que indica equipamento que permite estabelecer a comunicação entre duas redes LAN (local area network) distintas que empregam cabeamento padrão UTP.

a) hub
b) storage
c) access point
d) roteador
e) conector de fibra óptica

14. **(CESPE / SEFAZ-RS – 2018)** Em redes locais, determinados equipamentos concentram o tráfego de dados entre os computadores. Alguns deles replicam os dados para todos os computadores da rede; outros permitem o tráfego de dados somente para o computador destinatário. Assinale a opção que apresenta equipamento utilizado para concentrar e transmitir dados somente ao computador destinatário, sem replicá-los a outros computadores conectados à mesma rede.

a) smartphone
b) hub
c) switch
d) conector RJ-45
e) impressora

15. **(CESPE / SEFAZ-RS – 2018)** Assinale a opção que apresenta o padrão que especifica a operação de uma rede local sem fio com velocidade acima de 300 Mbps.

a) IEEE 802.11n

b) IEEE 802.11c
c) IEEE 802.11b
d) IEEE 802.11g
e) IEEE 802.11a

16. **(CESPE / Polícia Federal – 2018)** Por meio de uma LAN sem fio embasada na tecnologia IEEE 802.11, é possível que os usuários transmitam (e recebam) pacotes para (e de) um ponto de acesso conectado a uma rede de computadores com fio conectada à Internet.

17. **(CESPE / Polícia Federal – 2018)** Em uma rede local que possui a topologia estrela, podem ser utilizados switches para integrar a comunicação entre os computadores.

18. **(CESPE / EBSERH – 2018)** Um switch camada 2 (layer 2) pode substituir um roteador que interliga três redes de comunicação diferentes, desde que se apliquem as mesmas regras de roteamento que estão configuradas no roteador.

19. **(CESPE / EBSERH – 2018)** Uma empresa que precise interligar suas filiais, em Brasília e no Rio de Janeiro, por meio de uma mesma rede de comunicação, deverá implantar uma rede do tipo WAN, que disponibiliza serviços de rede acessíveis de forma geograficamente distribuída.

20. **(CESPE / EBSERH – 2018)** O endereço físico MAC está associado à interface de comunicação que identifica, de forma única, cada dispositivo conectado a uma rede de computadores.

21. **(CESPE / STJ – 2018)** O cabo coaxial, se comparado aos cabos de par trançado, tem maior largura de banda e apresenta maior atenuação do sinal.

22. **(CESPE / STJ – 2018)** Devido à sua estrutura, em uma rede usando a topologia estrela, o isolamento de falhas é uma tarefa complexa, o que representa uma desvantagem dessa topologia.

23. **(CESPE / STJ – 2018)** A topologia anel tem a fragilidade de tornar a rede inoperável ao tráfego unidirecional. Para transpor essa fragilidade, faz-se necessária a utilização de uma topologia híbrida.

24. **(CESPE / STJ – 2018)** A rede mostrada na figura a seguir, em que as linhas representam conexões entre computadores, apresenta topologia mesh.



25. **(CESPE / STJ – 2018)** Em um roteador, as conexões LAN são dedicadas aos equipamentos da rede interna, enquanto a conexão WAN deve ser conectada ao gateway para garantir acesso à Internet.

26. **(CESPE / STJ – 2018)** Diferentemente de roteadores, que encaminham os pacotes apenas aos equipamentos de destino, os switches encaminham os pacotes a todos os equipamentos que estão conectados na rede.

27. **(CESPE / STJ – 2018)** Em uma rede local sem fio que utilize equipamentos de access point operando no padrão IEEE 802.11b, o tráfego de dados pode atingir velocidade de até 54 Mbps.

28. **(CESPE / STJ – 2018)** Com a finalidade de interligar duas ou mais redes de dados diferentes, podem-se utilizar roteadores ou switches conhecidos como layer 3 ou camada 3.

29. **(CESPE / ABIN – 2018)** Nas redes locais de difusão do tipo anel, há necessidade de se definir alguma regra para arbitrar os acessos simultâneos ao enlace.

30. **(CESPE / ABIN – 2018)** Bluetooth é uma tecnologia de substituição de cabos que permite alcance médio com velocidade mais alta e potência maior que a da tecnologia IEEE 802.11.

GABARITO – CESPE

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

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

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

1. 

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

2. 

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

3. 

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

4. 

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

5. 

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

6. 

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

7. 

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

8. 

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



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