Estratégia Concursos

Aula 00

ANTT - Informática

Autor:
Diego Carvalho

07 de Setembro de 2025

Índice

1) Redes de Computadores - Parte 1 3

2) Resumo - Redes de Computadores - Parte 1 149

3) Mapas Mentais - Redes de Computadores - Parte 1 163

4) Questões Comentadas - Redes de Computadores - Parte 1 - CESPE 170

5) Lista de Questões - Redes de Computadores - Parte 1 - CESPE 205

REDES DE COMPUTADORES

Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

REDES DE COMPUTADORES

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





Uma rede de computadores é simplesmente um grupo de dispositivos conectados entre si, seja por cabos ou por conexões sem fio, permitindo que eles troquem informações e compartilhem recursos. Esses dispositivos podem ser computadores, celulares, impressoras, servidores, sensores, entre outros. Com essa comunicação, os usuários conseguem acessar arquivos, mandar mensagens, usar programas que dependem da internet e até imprimir documentos, mesmo que os equipamentos estejam em lugares diferentes.

Existem redes de vários tamanhos, desde uma rede pequena dentro da sua casa até grandes redes que cobrem o mundo todo, como a Internet. Para que tudo funcione direitinho, as redes seguem regras conhecidas como protocolos, como o famoso TCP/IP, que garantem que os dados cheguem certinho ao destino. As redes podem usar diferentes tipos de cabos (como par trançado, cabo coaxial ou fibra óptica) ou ainda funcionar sem fio, usando sinais de rádio, como acontece no Wi-Fi.

As redes de computadores são essenciais para quase tudo hoje em dia. Elas permitem desde navegar na internet, assistir a vídeos, fazer compras online, conversar por videochamadas até realizar operações complexas como a computação em nuvem. A eficiência, segurança e confiabilidade de uma rede afeta diretamente a comunicação e a produtividade das pessoas e empresas, sendo, por isso, uma parte fundamental da nossa vida moderna.

Saiba mais:

Uma rede de computadores pode ser comparada ao sistema rodoviário de uma cidade. Imagine cada computador como uma casa ou prédio e os dados como veículos que precisam circular rapidamente de um ponto a outro. As estradas, ruas e avenidas seriam os cabos e conexões sem fio que interligam esses prédios e permitem o tráfego organizado dos veículos, ou seja, os dados.

Assim como uma cidade necessita de sinalização, semáforos e regras de trânsito para garantir a fluidez e segurança dos veículos, as redes de computadores usam protocolos e equipamentos como roteadores e switches para direcionar e organizar o fluxo das informações, evitando congestionamentos ou colisões. Além disso, grandes avenidas e rodovias, que ligam bairros distantes rapidamente, seriam as conexões de alta velocidade da rede, como as conexões por fibra óptica.

Dessa maneira, da mesma forma que ruas conectam lugares distintos para permitir que pessoas troquem produtos, serviços e mensagens rapidamente, uma rede conecta computadores e dispositivos eletrônicos para que possam compartilhar dados, recursos e informações de forma rápida, eficiente e organizada.

Vejamos os principais benefícios de uma rede de computadores:

BENEFÍCIOS DE REDES DE COMPUTADORES	DESCRIÇÃO
COMPARTILHAMENTO DE RECURSOS	Permite que usuários compartilhem equipamentos como impressoras, scanners, softwares e armazenamento, reduzindo custos e evitando redundância.
COMUNICAÇÃO EFICIENTE	Facilita comunicação rápida e segura através de e-mails, mensagens, videoconferências e transferência de arquivos.
ACESSO À INFORMAÇÃO	Possibilita acesso rápido e organizado a informações compartilhadas, facilitando decisões ágeis e embasadas.
CENTRALIZAÇÃO DE DADOS	Armazenamento centralizado, simplificando backups, gerenciamento e aumentando a segurança das informações.
REDUÇÃO DE CUSTOS	Otimiza o uso dos recursos existentes, reduz gastos operacionais e facilita processos administrativos.
FLEXIBILIDADE E MOBILIDADE	Permite trabalho remoto e acesso móvel, aumentando a produtividade e facilitando o acesso à informação em qualquer lugar.
ESCLABILIDADE E INTEGRAÇÃO	Facilita integração de novos dispositivos e usuários, permitindo adaptação rápida ao crescimento e evolução tecnológica.

As redes de computadores têm um papel fundamental no compartilhamento de recursos, proporcionando maior eficiência, economia e praticidade na utilização de dispositivos e informações. Por meio das redes, diversos equipamentos, como impressoras, scanners, discos rígidos externos e outros periféricos podem ser compartilhados entre usuários diferentes, evitando a necessidade de adquirir equipamentos individuais para cada estação de trabalho.

Além disso, as redes facilitam o acesso a recursos informacionais, permitindo que arquivos, softwares e bancos de dados estejam acessíveis a múltiplos usuários simultaneamente. Essa centralização da informação simplifica o gerenciamento e permite maior segurança, consistência e controle dos dados armazenados, possibilitando uma colaboração mais eficaz e aumentando a produtividade nas organizações. Isso gera redução significativa de custos e otimiza a utilização dos recursos existentes.

Saiba mais:

Imagine o seguinte cenário de uma empresa sem uma rede de computadores: cada funcionário teria que possuir sua própria impressora, scanner e dispositivo de armazenamento externo. Isso significaria um alto custo para adquirir equipamentos individuais, além do aumento no consumo de energia elétrica e dificuldades de manutenção.

Agora imagine com uma rede de computadores: a empresa pode conectar uma única impressora multifuncional à rede, permitindo que todos os funcionários utilizem esse mesmo equipamento para imprimir e digitalizar documentos diretamente de seus computadores pessoais. Além disso, arquivos importantes podem ser salvos em um servidor centralizado ou na nuvem, garantindo acesso simultâneo, rápido e seguro a todos os colaboradores.

(PROF. DIEGO / INÉDITA – 2025) Redes de computadores consistem em um conjunto de dispositivos eletrônicos interconectados para compartilhar recursos e informações.

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

(PROF. DIEGO / INÉDITA – 2025) As redes de computadores são sistemas centralizados que não permitem a comunicação distribuída.

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

(PROF. DIEGO / INÉDITA – 2025) As redes de computadores representam uma infraestrutura de comunicação que possibilita a troca de dados apenas em nível local.

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

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

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

Comentários: (a) Errado. Time Sharing é uma técnica de compartilhamento de tempo de processamento de um computador entre vários usuários, não um conjunto de processadores interconectados; (b) Correto. Redes de Computadores interligam unidades processadoras (computadores), permitindo o compartilhamento de recursos como impressoras e discos de forma eficiente; (c) Errado. Compartilhamento do Windows refere-se a uma funcionalidade específica de um sistema operacional, não a uma definição geral de interligação de processadores; (d) Errado. Interligação de Redes de Computadores (interconexão de redes) refere-se à conexão entre redes distintas, não diretamente à definição de compartilhamento entre processadores em uma única rede (Letra B).

Tipos de Conexão/Enlace

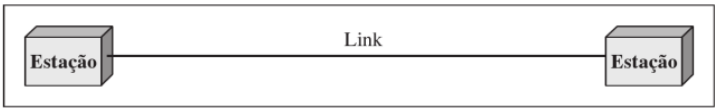
INCIDÊNCIA EM PROVA: BAIXÍSSIMA

TIPOS DE CONEXÃO/ENLACE

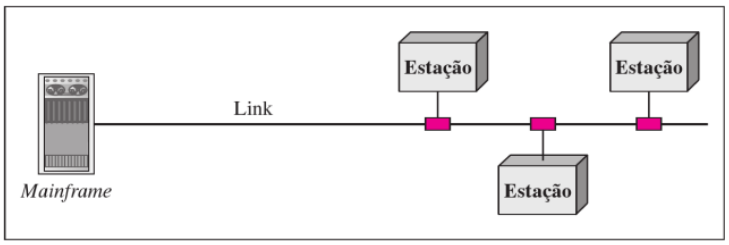
Um link, conexão ou enlace refere-se ao meio físico ou lógico que conecta dois ou mais dispositivos, permitindo a transmissão de dados entre eles. Este link pode ser estabelecido usando uma variedade de mídias, como cabos de fibra óptica, fios de cobre, ou através de conexões sem fio como Wi-Fi ou rádio.

As redes de computadores são formadas por dois ou mais dispositivos que se conectam entre si através de links. Um link, também chamado de enlace, é como um caminho ou canal que permite que os dados viajem de um dispositivo para outro. Para imaginar melhor, pense em um link como uma linha reta ligando dois pontos. Para que a comunicação aconteça, todos os dispositivos envolvidos precisam estar conectados a esse caminho ao mesmo tempo.

Existem dois tipos principais de conexão em redes: ponto-a-ponto e ponto-multiponto. Na conexão ponto-a-ponto, o link é dedicado, ou seja, ele é exclusivo entre dois dispositivos – somente eles usam aquele caminho para trocar informações.



Já na conexão ponto-multiponto, o link é compartilhado por vários dispositivos ao mesmo tempo. Um exemplo: quando acessamos a internet, estamos usando um link compartilhado, pois os cabos que nos conectam (como os submarinos) também são usados por muitas outras pessoas ao redor do mundo.



Quando você acessa a internet, você está numa conexão compartilhada. Já quando usamos um controle remoto para mudar o canal da TV, estamos em uma conexão ponto-a-ponto, pois o controle fala diretamente e exclusivamente com o televisor. Em conexões ponto-multiponto, mais de dois dispositivos compartilham o mesmo link. Essa divisão pode acontecer de duas formas: se todos usarem o canal ao mesmo tempo (compartilhamento espacial) ou se cada um esperar a sua vez para usar (compartilhamento temporal). No dia a dia, o modo mais comum é o compartilhamento no tempo, em que cada dispositivo aguarda sua vez para se comunicar.

Saiba mais:

Imagine que uma rede de computadores funciona como uma estrada que liga casas, escritórios e lojas em uma cidade. Essa estrada representa o link ou enlace, o caminho por onde veículos – que neste caso são os dados – trafegam de um local para outro. Para que duas casas consigam trocar pacotes ou mensagens, ambas precisam estar conectadas à mesma estrada. Existem dois tipos principais de estrada:

| **Estrada exclusiva (ponto-a-ponto):** seria como construir uma rua particular que liga apenas duas casas, permitindo que somente os moradores dessas casas trafeguem nela. Ninguém mais pode usar essa rua. Isso é semelhante a um enlace dedicado, exclusivo para dois dispositivos. Um exemplo seria o feixe de luz entre um controle remoto e uma televisão.

| **Estrada compartilhada (ponto-multiponto):** é como uma avenida movimentada, usada por várias casas, lojas e prédios. Todos compartilham a mesma via para enviar e receber pacotes. Assim, quando acessamos a internet, usamos essa avenida compartilhada com milhares de outros usuários, semelhante ao uso coletivo de cabos submarinos.

Se muitos carros trafegarem ao mesmo tempo na avenida (conexão espacial), todos compartilham a via ao mesmo tempo. Se for necessário que os veículos passem um de cada vez para evitar congestionamento (conexão temporal), cada carro espera sua vez para usar a estrada.

TIPOS DE CONEXÃO	DESCRIÇÃO	CARACTERÍSTICAS
PONTO-A-PONTO	Conexão direta entre dois dispositivos por meio de um link dedicado.	- Comunicação exclusiva - Link não compartilhado - Ex: Controle remoto e TV
PONTO-MULTIPONTO	Um único link é compartilhado por mais de dois dispositivos.	- Comunicação compartilhada - Link dividido entre vários dispositivos - Ex: Redes Wi-Fi públicas

(PROF. DIEGO / INÉDITA – 2025) Uma conexão ponto-a-ponto é aquela em que vários dispositivos compartilham o mesmo meio de transmissão, e a comunicação ocorre diretamente entre dois dispositivos, sem a necessidade de compartilhar o meio com outros.

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

(PROF. DIEGO / INÉDITA – 2025) Uma conexão ponto-multiponto permite a comunicação direta entre dois dispositivos, sem a necessidade de compartilhar o meio de transmissão com outros.

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

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

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

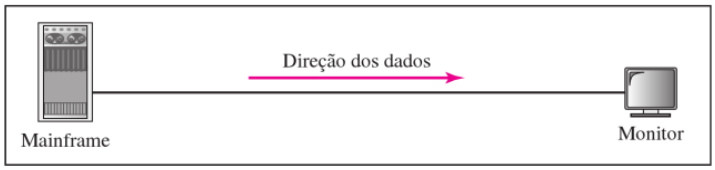
Direções de Transmissão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

DIREÇÃO DE TRANSMISSÃO

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

Simplex

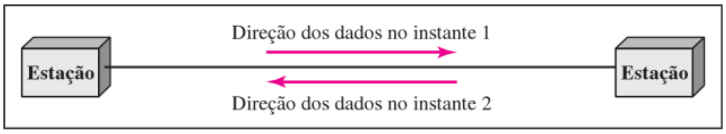


O enlace é utilizado apenas em um dos dois possíveis sentidos de transmissão
Exemplo: TV, Rádio AM/FM, Teclado, etc.

Uma comunicação é dita simplex quando há um transmissor de mensagem, um receptor de mensagem e esses papéis nunca se invertem no período de transmissão. Quando você vê TV, sua antena recebe um sinal de um satélite, mas ela jamais envia/transmite sinais para o satélite. Logo, o satélite é o transmissor, sua antena é o receptor, e esses papéis não são trocados – o mesmo serve para Rádio AM/FM ou para o teclado de um computador.



Half-Duplex

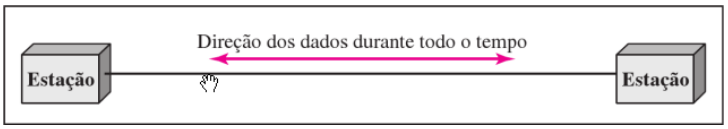


O enlace é utilizado nos dois possíveis sentidos de transmissão, porém apenas um por vez
Exemplo: Walk&Talk e Nextel

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



Full-Duplex



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

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



Saiba mais:

Imagine a comunicação como uma estrada por onde passam carros (dados) entre duas cidades (dispositivos):

| Simplex: é como uma estrada de mão única, isto é, os carros podem ir apenas em uma direção, da Cidade A para a Cidade B, sem possibilidade de retorno da Cidade B para a Cidade A pela mesma estrada.

| Half-Duplex: é como uma estrada de mão dupla, mas muito estreita, permitindo apenas que os carros trafeguem em uma direção por vez. Primeiro, os carros vão da Cidade A para a Cidade B; depois, os carros da Cidade B podem vir para a Cidade A, mas nunca ao mesmo tempo.

| Full-Duplex: é como uma estrada larga com várias pistas, permitindo que os carros trafeguem simultaneamente nos dois sentidos. Assim, a Cidade A envia carros para a Cidade B enquanto recebe outros carros de volta ao mesmo tempo.

DIREÇÕES DE TRANSMISSÃO	DESCRIÇÃO	CARACTERÍSTICAS

SIMPLEX	A comunicação ocorre em apenas um sentido; um dispositivo apenas envia e o outro apenas recebe.	- Comunicação unidirecional - Sem resposta ou retorno de dados - Ex: transmissão de TV
HALF-DUPLEX	A comunicação ocorre nos dois sentidos, mas apenas um dispositivo pode transmitir por vez.	- Comunicação bidirecional alternada - Um fala enquanto o outro escuta - Ex: rádios comunicadores (walkie&talk)
FULL-DUPLEX	A comunicação ocorre simultaneamente nos dois sentidos, permitindo envio e recebimento ao mesmo tempo.	- Comunicação bidirecional simultânea - Alta eficiência - Ex: chamadas telefônicas

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

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

Comentários: (a) Errado. Simples (ou simplex) é a comunicação em apenas uma direção, sem possibilidade de inversão dos papéis entre transmissor e receptor; (b) Errado. Monoplex é sinônimo de transmissão simples, ou seja, comunicação em apenas um sentido fixo, sem troca de papéis; (c) Correto. Half Duplex permite a comunicação nos dois sentidos, mas não simultaneamente; os papéis de transmissor e receptor podem ser invertidos alternadamente; (d) Errado. Full Duplex permite a comunicação simultânea nos dois sentidos, não apenas a inversão de papéis; (e) Errado. Auto Duplex não é um termo técnico padrão em redes de computadores para descrever modos de transmissão (Letra C).

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

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

Comentários: (a) Errado. "Duplex" é um termo genérico que se refere à comunicação em ambos os sentidos, podendo ser full ou half, sem especificar se é simultânea ou alternada; (b) Errado. No modo Simplex, a comunicação ocorre apenas em um sentido, sem possibilidade de resposta pelo receptor; (c) Errado. No modo Full-Duplex, a transmissão e a recepção ocorrem simultaneamente entre as estações; (d) Correto. No modo Half-Duplex, as estações podem transmitir e receber dados, mas não simultaneamente; a comunicação ocorre alternadamente (Letra D).

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

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

e) Simplex

Comentários: (a) Errado. No half-duplex, a transmissão é bidirecional, mas ocorre de forma alternada, não sendo exclusivamente unidirecional; (b) Errado. No full-duplex, a transmissão é bidirecional e simultânea entre os dispositivos; (c) Errado. "Full-simplex" não é uma nomenclatura padrão em redes de comunicação de dados; (d) Errado. "Duplex" é um termo genérico para comunicação bidirecional, podendo ser half ou full, não indicando comunicação unidirecional; (e) Correto. No modo Simplex, a comunicação é unidirecional: um dispositivo apenas transmite e o outro apenas recebe, sem inversão de papéis (Letra E).

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

Comentários: no modo half-duplex, a estação pode transmitir e receber, mas não ao mesmo tempo; a comunicação ocorre em ambos os sentidos, porém de forma alternada – o modo como cada estação pode, simultaneamente, transmitir e receber é conhecido como full-duplex (Errado).

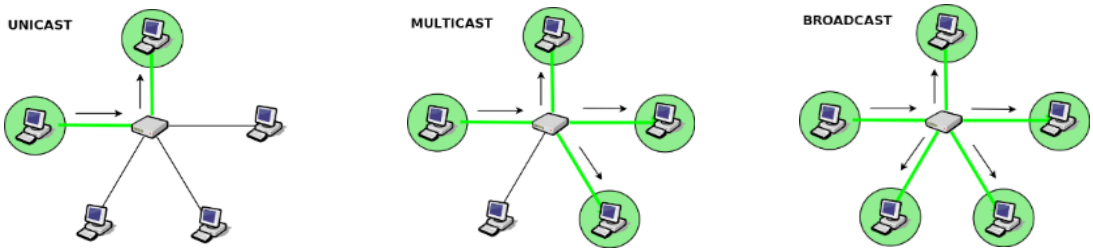
Modos de Transmissão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

MODOS DE TRANSMISSÃO

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

A transmissão de dados em uma rede de computadores pode ser realizada em três modos diferentes: *Unicast*, *Multicast* e *Broadcast*[1]. Vamos vê-los em detalhes:



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

Nessa comunicação, uma mensagem só pode ser enviada para um destino. Notem que a primeira estação de trabalho está enviando uma mensagem endereçada especificamente para a 2ª estação de trabalho.

Multicast [*multi* = vários e *cast* = transmitir]

Nessa comunicação, uma mensagem é enviada para um grupo de destino. Observem que a primeira estação de trabalho está enviando uma mensagem endereçada para o grupo da 2ª, 3ª e 4ª estações.

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.

FIQUE ATENTO!

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

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

Saiba mais:

Vamos imaginar agora uma situação o Whatsapp:

Unicast: seria como quando você manda uma mensagem diretamente para um amigo em uma conversa privada. Só ele recebe a mensagem – é uma comunicação de um para um, exatamente como um dispositivo enviando dados diretamente para outro na rede.

Multicast: seria como quando você cria uma lista de transmissão no WhatsApp. Você envia uma mensagem para várias pessoas ao mesmo tempo, mas apenas quem está na lista recebe – é o envio de dados para um grupo selecionado de dispositivos, sem atingir todos.

Broadcast: seria como se você postasse uma mensagem no seu Status do WhatsApp. Todos os seus contatos podem ver aquela mensagem, logo seria equivalente a enviar dados para todos os dispositivos conectados, independentemente de quem realmente precisa da informação.

MODOS DE TRANSMISSÃO	DESCRIÇÃO	CARACTERÍSTICAS
UNICAST	Envio de dados de um dispositivo diretamente para outro dispositivo específico.	- Comunicação um-para-um - Destinatário único - Ex: Mensagem privada no WhatsApp
MULTICAST	Envio de dados de um dispositivo para um grupo específico de dispositivos.	- Comunicação um-para-vários - Economia de banda - Ex: Transmissão de vídeo para inscritos
BROADCAST	Envio de dados de um dispositivo para todos os dispositivos da rede.	- Comunicação um-para-todos - Todos recebem a mensagem - Ex: Anúncio em grupo de WhatsApp

(PROF. DIEGO / INÉDITA – 2025) Unicast é um modo de transmissão onde os dados são enviados para vários destinatários ao mesmo tempo.

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

(PROF. DIEGO / INÉDITA – 2025) Multicast é um modo de transmissão em que os dados são enviados de um único remetente para um grupo específico de destinatários que se inscreveram no grupo multicast.

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

(PROF. DIEGO / INÉDITA – 2025) Anycast é um modo de transmissão em que os dados são enviados de um único remetente para o destinatário mais próximo em um grupo de destinatários com o mesmo endereço IP.

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

(PROF. DIEGO / INÉDITA – 2025) Unicast é amplamente utilizado em redes de difusão de streaming de vídeo para alcançar muitos assinantes ao mesmo tempo.

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

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

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

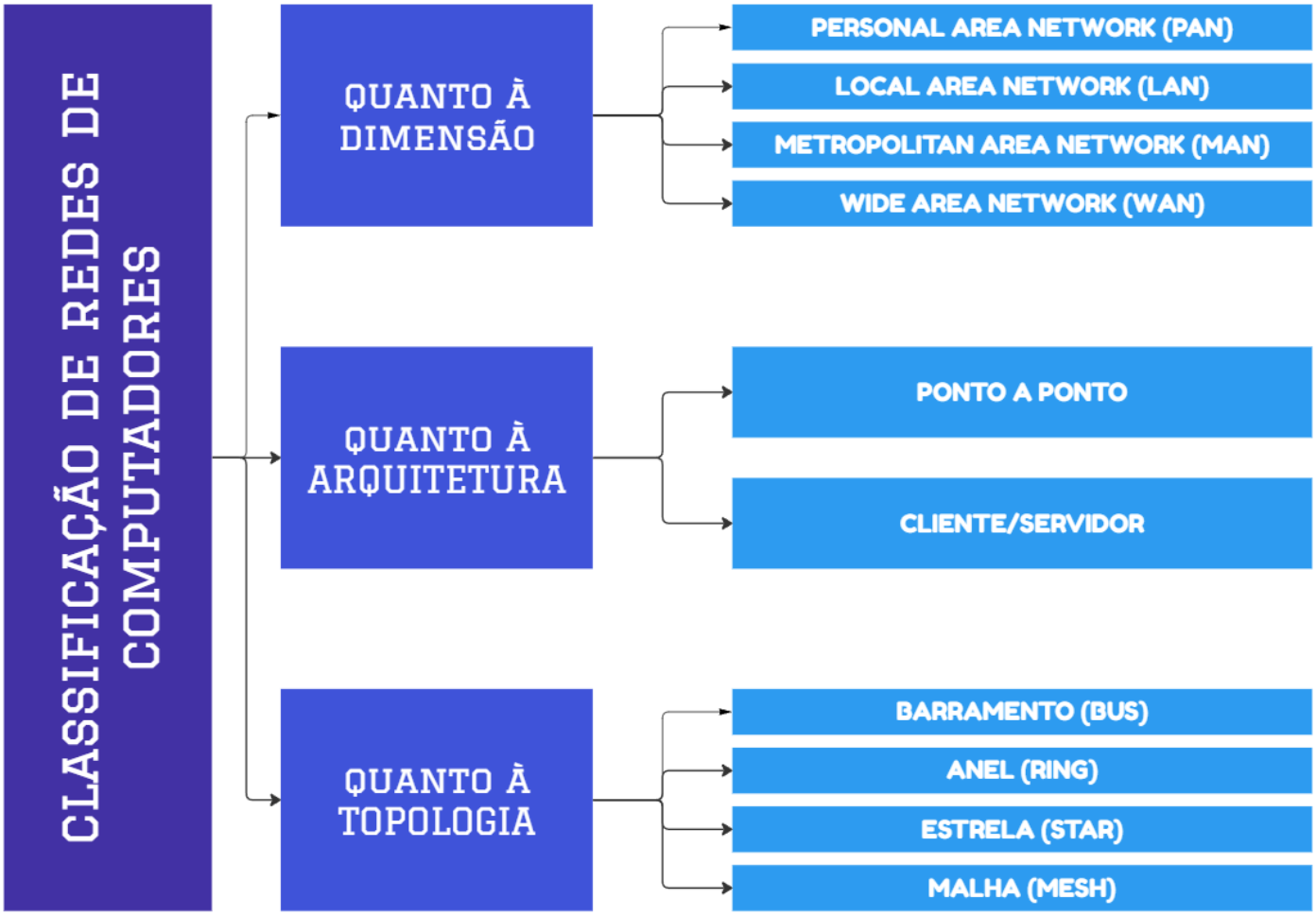
(FCC / TRE-AM – 2010) Uma única mensagem gerada pelo emissor que é destinada a todos os elementos da rede caracteriza uma mensagem:

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

Comentários: (a) Correto. Broadcast é o envio de uma única mensagem para todos os dispositivos da rede, sem distinção de destinatário; (b) Errado. Multicast é o envio de uma mensagem para um grupo específico de dispositivos, não para todos; (c) Errado. Unicast é a comunicação ponto a ponto, ou seja, de um emissor para um único receptor; (d) Errado. Anycast envia a mensagem para o nó mais próximo, entre vários possíveis destinos; (e) Errado. Fullcast não é um termo técnico utilizado em redes para descrever tipos de envio de mensagem (Letra A).

Classificação de Redes

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



Quanto à Dimensão, Tamanho ou Área Geográfica

ABRANGÊNCIA GEOGRÁFICA

Em redes de computadores, a classificação de redes de acordo com a área de abrangência se refere ao tamanho e à extensão geográfica que a rede cobre, ou seja, é a maneira de agrupar redes conforme o espaço físico que elas interligam.

Uma rede de computadores pode ser classificada quanto à dimensão, tamanho ou abrangência de área geográfica. Atenção: apesar de existir um certo consenso, não existem números exatos.

PAN (Personal Area Network)

INCIDÊNCIA EM PROVA: BAIXA



DISTÂNCIA

ALGUNS CENTÍMETROS A POUCOS METROS

Trata-se de uma rede de computadores de alcance muito limitado, geralmente restrita a poucos metros, destinada à comunicação entre dispositivos pessoais de um único usuário. Ela conecta equipamentos como smartphones, tablets, laptops, fones de ouvido, smartwatches e impressoras, utilizando tecnologias como Bluetooth, infravermelho ou conexões USB. Seu principal objetivo é facilitar o compartilhamento rápido de dados e o uso de recursos entre dispositivos próximos, promovendo mobilidade, praticidade e integração no dia a dia do usuário.

Saiba mais:

Um exemplo clássico de Personal Area Network (PAN) é quando uma pessoa conecta seu smartphone ao seu fone de ouvido Bluetooth para ouvir música ou atender chamadas sem fio. Nesse caso, a comunicação ocorre em um espaço pessoal, de curta distância, usando tecnologia sem fio, e envolve apenas dispositivos pertencentes ao mesmo usuário.

Vejamos uma tabela com as principais características desse tipo de rede de computadores:

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

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

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

Comentários: (a) Errado. LAN (Local Area Network) conecta dispositivos em áreas pequenas como edifícios ou escritórios, mas cobre distâncias maiores que o Bluetooth; (b) Errado. WAN (Wide Area Network) abrange grandes áreas geográficas, como cidades ou países, muito além do alcance do Bluetooth; (c) Correto. PAN (Personal Area Network) é voltada para a comunicação em curtas distâncias, geralmente alguns metros, como no caso do Bluetooth; (d) Errado. MAN (Metropolitan Area Network) cobre áreas urbanas inteiras, como bairros ou cidades, não se aplicando ao alcance limitado do Bluetooth (Letra C).

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

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

Comentários: (a) Errado. Wide Area Network (WAN) conecta redes em grandes distâncias geográficas, como cidades ou países, não sendo focada em curto alcance; (b) Errado. Storage Area Network (SAN) é uma rede dedicada para o armazenamento de dados, sem relação direta com redes de curto alcance e conexão de periféricos; (c) Correto. Personal Area Network (PAN) é destinada à conexão de dispositivos próximos, como computador e impressora, geralmente sem fio e de curto alcance; (d) Errado. Metropolitan Area Network (MAN) cobre áreas urbanas maiores, como uma cidade inteira, não sendo usada para conexões pessoais de curto alcance; (e) Errado. Regional Area Network (RAN) não é uma classificação padrão de redes na literatura técnica de redes de computadores (Letra C).

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

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

Comentários: (a) Errado. LAN (Local Area Network) cobre redes de pequeno a médio porte, como redes domésticas ou empresariais, mas com alcance maior que o descrito; (b) Errado. CAN (Campus Area Network) interliga redes em uma área como um campus universitário ou base militar, com alcance bem superior ao de poucos metros; (c) Correto. PAN (Personal Area Network) conecta dispositivos pessoais em curta distância, utilizando tecnologias como Bluetooth para comunicação sem fio; (d) Errado. MAN (Metropolitan Area Network) abrange áreas urbanas inteiras, conectando redes de diferentes edifícios em uma cidade (Letra C).

LAN (Local Area Network)

INCIDÊNCIA EM PROVA: ALTÍSSIMA



DISTÂNCIA

DE ALGUMAS CENTENAS DE METROS A ALGUNS QUILÔMETROS

Trata-se de uma rede de computadores limitada a uma área geográfica restrita, como uma residência, um escritório, um laboratório, um prédio inteiro ou um campus universitário, permitindo que dispositivos compartilhem dados e recursos de forma rápida e eficiente. As LANs são normalmente compostas por computadores, impressoras, servidores e outros equipamentos interconectados por cabos ou por conexões sem fio, apresentando baixa taxa de erros e elevada confiabilidade.

Saiba mais:

Um exemplo clássico de Local Area Network (LAN) é a rede interna de uma empresa, onde todos os computadores dos funcionários, impressoras e servidores estão conectados entre si dentro do

mesmo escritório, permitindo o compartilhamento de arquivos, impressões e acesso à internet de forma rápida, segura e confiável.

Vejamos uma tabela com as principais características desse tipo de rede de computadores:

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

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

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

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

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

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

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

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

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

Comentários: (a) Errado. WAN (Wide Area Network) é usada para interligar redes em grandes áreas geográficas, como cidades ou países, não sendo apropriada para um único prédio; (b) Errado. MAN (Metropolitan Area Network) conecta redes em uma área metropolitana, como entre diferentes prédios em uma cidade, e não é necessária para um único laboratório; (c) Correto. LAN (Local Area Network) é ideal para conectar estações de trabalho em uma área restrita, como um prédio, permitindo compartilhamento seguro de arquivos entre usuários locais; (d) Errado. PAN (Personal Area Network) é voltada para comunicação entre dispositivos pessoais em curtíssimas distâncias, como Bluetooth entre fones de ouvido e celulares (Letra C).

MAN (Metropolitan Area Network)

INCIDÊNCIA EM PROVA: ALTÍSSIMA



DISTÂNCIA

ALGUMAS DEZENAS DE QUILÔMETROS

Trata-se de uma rede de computadores que interliga diversos dispositivos e redes locais dentro de uma área geográfica maior, geralmente abrangendo uma cidade. Seu objetivo é conectar múltiplas redes próximas para permitir a troca rápida de dados e o compartilhamento de recursos em uma região metropolitana. Elas possuem abrangência maior que a de uma rede local e menor que a de uma rede extensa – que veremos a seguir.



Elas podem ser utilizadas, por exemplo, para integrar as unidades de uma mesma empresa espalhadas pela cidade, instituições de ensino ou órgãos públicos, utilizando infraestruturas como cabos de fibra óptica ou conexões sem fio de alta capacidade. Na imagem anterior, temos uma foto aérea de Brasília com a localização de dezenas de filiais do Giraffas – essas filiais podem se conectar formando uma única rede de área metropolitana espalhada em diferentes locais dentro de uma mesma cidade ou metrópole.

Saiba mais:

Um exemplo clássico de Metropolitan Area Network (MAN) é a rede que interliga todas as unidades de uma universidade espalhadas por diferentes bairros de uma mesma cidade.
Outro exemplo é a rede de câmeras de monitoramento urbano que conecta diversos pontos de uma cidade à central de controle da prefeitura.

Vejamos uma tabela com as principais características desse tipo de rede de computadores:

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

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

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

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

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

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

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

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

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

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

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

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

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

WAN (Wide Area Network)

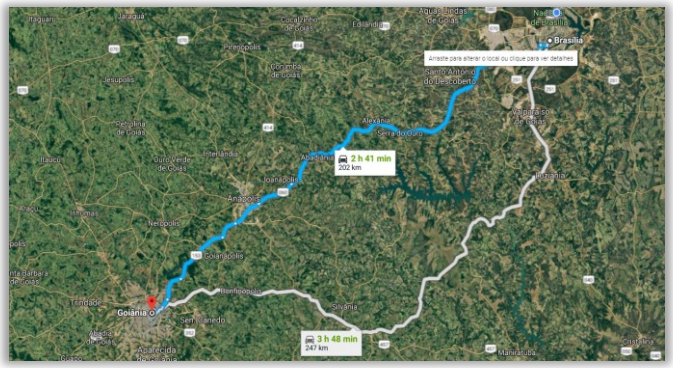
INCIDÊNCIA EM PROVA: ALTÍSSIMA



DISTÂNCIA

CENTENAS A MILHARES DE QUILÔMETROS

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





Seu principal objetivo é possibilitar a comunicação e o compartilhamento de dados entre dispositivos localizados a grandes distâncias. As WANs utilizam infraestruturas públicas e privadas, como linhas telefônicas, cabos submarinos, satélites e redes de fibra óptica, e geralmente contam com provedores de serviços de telecomunicações para a transmissão de dados.

Saiba mais:

Um exemplo clássico de Wire Area Network (WAN) é a própria Internet. A Internet conecta milhões de redes e dispositivos ao redor do mundo, permitindo a comunicação e o compartilhamento de informações entre pessoas e organizações localizadas em diferentes países e continentes.

Vejamos uma tabela com as principais características desse tipo de rede de computadores:

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

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

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

Comentários: (a) Errado. PAN (Personal Area Network) é destinada a conexões de dispositivos pessoais em curtas distâncias, como Bluetooth, não abrangendo grandes áreas geográficas; (b) Errado. MAN (Metropolitan Area Network) cobre áreas de tamanho intermediário, como uma cidade, e não um país ou continente; (c) Errado. LAN (Local Area Network) conecta dispositivos em uma área local limitada, como um escritório ou prédio, sem alcance continental; (d) Correto. WAN (Wide Area Network) abrange grandes áreas geográficas, como países ou continentes, sendo o tipo de rede da Internet (Letra D).

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

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

(AOCP / UFFS – 2019) Para que possa ser implementada uma correta e adequada interconexão de redes de computadores, é muito importante definir que tipo de rede será construída e utilizada para a comunicação. Dentro desse cenário, a rede a ser desenvolvida possui as seguintes características: deve cobrir áreas geograficamente dispersas, abrangendo uma grande

área; deve possuir a interconexão de várias sub-redes de comunicação; e deve conter inúmeras linhas de transmissão. Com base nas características apresentadas, qual é o melhor tipo de rede para implementação?

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

Comentários: (a) Errado. MAN cobre áreas de tamanho médio, como uma cidade ou campus, não sendo adequada para áreas geograficamente muito dispersas; (b) Errado. LAN é usada para conectar dispositivos em uma área pequena e local, como um prédio, sem abranger grandes distâncias; (c) Correto. WAN (Wide Area Networks) é ideal para cobrir áreas geográficas extensas, interligando várias sub-redes com múltiplas linhas de transmissão; (d) Errado. PAN conecta dispositivos pessoais em curtíssimas distâncias, como fones de ouvido e celulares, sendo inadequada para interconexões amplas; (e) Errado. VLAN é uma rede virtual criada dentro de uma LAN para segmentar grupos de dispositivos, não para cobrir grandes áreas (Letra C).

(CEBRASPE / 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: (a) Errado. VoIP é uma tecnologia para transmissão de voz pela Internet, não um tipo de rede de comunicação entre empresas; (b) Errado. PGP é uma ferramenta de criptografia para proteger dados, não um tipo de rede para conexão entre empresas; (c) Errado. LAN conecta dispositivos em áreas locais pequenas, como escritórios ou prédios, não entre países e continentes; (d) Errado. SSL é um protocolo de segurança para transmissão de dados, não um tipo de rede de interligação geográfica; (e) Correto. WAN (Wide Area Network) é o tipo de rede adequado para conectar empresas em diferentes países e continentes, permitindo o compartilhamento de dados (Letra E).

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

TIPO DE REDE	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.



Essa classificação representa tipos de redes classificadas pela área geográfica que cobrem. Quando falamos em redes sem fio, acrescentamos o prefixo "W" (de Wireless), mas – em questões de concurso – geralmente não se exige esse rigor técnico. É muito comum enunciados simplesmente falarem "LAN" mesmo se tratando de uma rede Wi-Fi doméstica, por exemplo, sem citar "WLAN". Nós temos PAN e WPAN, LAN e WLAN, MAN e WMAN e WAN e WWAN.

Saiba mais:

A título de curiosidade, existem diversas outras classificações menos tradicionais (sua cobrança é raríssima em prova). Vejamos algumas delas:

| BAN (Body Area Network): refere-se a uma rede de sensores ligados ao corpo humano ou vestíveis (wearables), como smartwatches, monitores cardíacos, sensores de glicose, etc. A comunicação geralmente ocorre via Bluetooth ou tecnologias semelhantes, e o objetivo é monitorar e transmitir dados corporais em tempo real.

| CAN (Campus Area Network): refere-se a uma rede que interliga diversas redes domésticas (LANs) dentro de um mesmo campus, como em uma universidade, hospital ou complexo empresarial. Em regra, esse tipo de rede de computadores é maior que uma LAN, mas menor que uma MAN.

| SAN (Storage Area Network): refere-se a uma rede especializada em conectar servidores a dispositivos de armazenamento, em alta velocidade e segurança, normalmente usada em data centers. (Apesar de ter "Area Network" no nome, não se refere a uma área geográfica, mas sim a uma área lógica de armazenamento.)

| GAN (Global Area Network): refere-se a uma rede que conecta diferentes redes ao redor do globo, sendo até mesmo maior que uma Wide Area Network (WAN). Em algumas oportunidades, a própria internet pode ser chamada de Global Area Network (GAN) em contextos técnicos mais específicos.

| IAN (Interplanetary Area Network): refere-se a uma rede de internet espacial projetada para comunicação entre planetas, espaçonaves e estações espaciais. *Sabe a Curiosity?* Ela é um veículo-sonda que está percorrendo a superfície de Marte desde 2012 e enviando dados para a Terra em uma rede de área interplanetária de alguns milhões de quilômetros.

Quanto à Arquitetura de Rede ou Forma de Interação

ARQUITETURA DE REDE OU FORMA DE INTERAÇÃO

Em redes de computadores, a arquitetura de rede ou forma de interação é a maneira como os dispositivos (computadores, impressoras, servidores, celulares, entre outros) se organizam e interagem entre si dentro de uma rede – ela define quem faz o quê durante a comunicação e o compartilhamento de dados.

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, entre outros). Já os dispositivos finais são aqueles que fazem a interface entre o usuário e a rede de computadores (Ex: computadores, notebooks, smartphones, entre outros).



Na imagem anterior, 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.

Saiba mais:

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

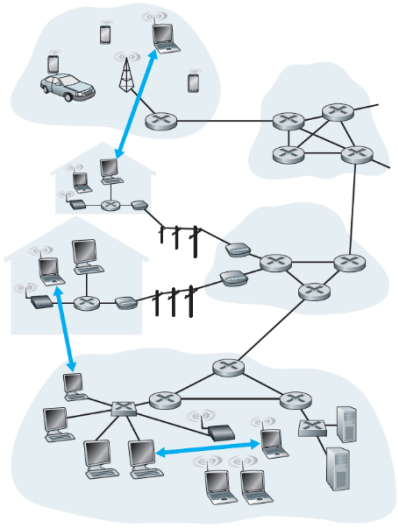
Ora, raramente alguém precisa de uma impressora só para si, portanto o compartilhamento de recursos otimizava bastante os custos e processos de uma organização. No entanto, outros recursos podiam ser compartilhados, como softwares, backups, e-mails e – principalmente – dados. Uma forma eficiente de compartilhar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

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

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

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. Essa classificação 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[2].

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). Existem diversas aplicações que utilizam a arquitetura ponto-a-ponto para compartilhar arquivos, sendo umas das mais famosas VoIP e o BitTorrent.

Saiba mais:

O BitTorrent é um protocolo de compartilhamento de arquivos peer-to-peer (P2P) que permite a distribuição eficiente de grandes quantidades de dados pela 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. *E por que isso nunca deu certo até hoje?* Se esse serviço utilizasse um modelo cliente/servidor (que veremos a seguir), bastava derrubar o servidor que estava disponibilizando os arquivos aos usuários; porém, em uma rede P2P, todas as máquinas são servidores e clientes.

Imagine que você quer baixar um filme usando o BitTorrent. Nesse caso, você não está pegando o filme inteiro de um único servidor central, como faria em um site de download comum. Em vez disso, o arquivo do filme está dividido em centenas ou milhares de pedaços espalhados nos computadores de várias pessoas que também estão compartilhando esse mesmo filme.

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 esteja 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 hoje em dia 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.

Esse comportamento – onde não há um servidor central controlando tudo e todos os dispositivos funcionam como clientes e servidores ao mesmo tempo – é o que define a Arquitetura P2P.

[2] 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.

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



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 o mesmo, porém tem significados diferentes dependendo do contexto.

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

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

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

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

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

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

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

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

Comentários: (a) Errado. Bluetooth é uma tecnologia de comunicação sem fio de curto alcance, não um modo de compartilhamento de dados pela Internet; (b) Errado. FTP é usado para a transferência de arquivos entre cliente e servidor, não diretamente entre usuários; (c) Errado. POP3 é um protocolo para recebimento de e-mails, sem relação com compartilhamento direto de arquivos entre usuários; (d) Correto. P2P permite que os usuários compartilhem arquivos e dados diretamente entre si, como ocorre no BitTorrent e em aplicativos VoIP; (e) Errado. B2B refere-se a transações comerciais entre empresas, não a um modo de compartilhamento de arquivos (Letra D).

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

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

Comentários: (a) Errado. Em redes peer-to-peer, os nós possuem capacidades e responsabilidades equivalentes, não diferentes; (b) Errado. Em redes peer-to-peer, não há a presença de um único servidor central; todos os nós podem atuar como cliente e servidor; (c) Correto. O gerenciamento descentralizado é uma característica central das redes peer-to-peer, onde todos os nós compartilham recursos entre si sem hierarquia fixa; (d) Errado. Embora frequentemente usadas em redes locais, redes peer-to-peer também podem operar via Internet; (e) Errado. Redes peer-to-peer não se limitam à conexão de apenas dois nós; podem incluir muitos dispositivos interligados (Letra C).

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

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

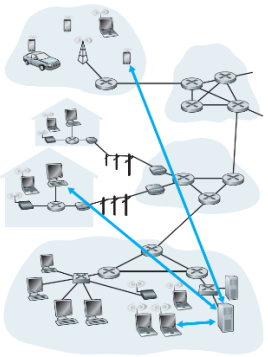
Comentários: (a) Errado. Two-Tier é uma arquitetura cliente-servidor tradicional, com divisão entre cliente e servidor, sem compartilhamento simultâneo de funções; (b) Errado. Three-Tier envolve três camadas (cliente, servidor de aplicação e servidor de dados), também com funções bem separadas; (c) Correto. Na arquitetura Peer-to-Peer, todos os participantes atuam como servidores e clientes ao mesmo tempo, compartilhando recursos diretamente; (d) Errado. Middleware é um software que atua como intermediário entre aplicações, não descrevendo a relação direta entre clientes e servidores; (e) Errado. Multi-Tier refere-se a arquiteturas com múltiplas camadas de separação de responsabilidades, diferente do conceito de compartilhamento simultâneo de funções (Letra C).

Rede Cliente/Servidor

INCIDÊNCIA EM PROVA: MÉDIA

A arquitetura de rede cliente/servidor trata de um modelo hierárquico de redes mais complexo, no entanto potencialmente mais robusto e confiável. Nesse modelo, existe uma máquina especializada, dedicada e geralmente remota, respondendo rapidamente aos pedidos vindos dos demais

computadores da rede – o que aumenta bastante o desempenho de algumas tarefas. É a escolha natural para redes grandes, como a Internet, que funciona tipicamente a partir do Modelo Cliente/Servidor.



Observem na imagem ao lado que há diversos dispositivos clientes se comunicando diretamente com um único servidor – um cliente jamais se comunica diretamente com outro cliente.

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

Saiba mais:

Imagine que você precisa baixar um material de aula em *www.estrategiaconcursos.com.br*. Quando você acessa o site pelo navegador do seu computador ou celular, você é o cliente – ou seja, o dispositivo que solicita um serviço (neste caso, o download do arquivo).

O site do Estratégia Concursos, por sua vez, está hospedado em servidores – computadores robustos que armazenam as páginas da web, os arquivos das aulas, vídeos, PDFs, entre outros. Quando você clica no link para baixar a aula, seu navegador envia um pedido para o servidor do site. O servidor recebe esse pedido, localiza o arquivo solicitado e envia o arquivo de volta para o seu dispositivo. Nesse processo, temos:

| **Cliente:** seu computador ou celular, que pede o arquivo.
| **Servidor:** o computador (servidor web) que armazena o arquivo e atende a solicitação.

Essa relação, em que o cliente apenas consome o serviço e o servidor oferece o serviço, caracteriza a Arquitetura Cliente/Servidor. Tudo é centralizado: se o servidor do Estratégia cair ou ficar fora do ar, nenhum cliente conseguirá acessar ou baixar o arquivo.

ARQUITETURA DE REDES	REDES PONTO-A-PONTO (P2P)	REDES CLIENTE/SERVIDOR
ESTRUTURA	Descentralizada: todos são iguais.	Centralizada: divisão clara entre cliente e servidor.
FUNÇÃO DOS DISPOSITIVOS	Cada dispositivo atua como cliente e servidor.	Clientes consomem serviços; servidores fornecem serviços.
CUSTO	Menor (não requer servidores dedicados).	Maior (exige servidores mais potentes).
GERENCIAMENTO	Difícil (cada dispositivo gerencia seus próprios recursos).	Mais fácil (controle centralizado).
SEGURANÇA	Menor (difícil aplicar políticas uniformes).	Maior (políticas de segurança no servidor).
ESCALABILIDADE	Limitada (dificuldade de crescimento em grandes redes).	Alta (fácil adicionar clientes à rede).
DESEMPENHO EM GRANDE ESCALA	Tende a degradar.	Mantém bom desempenho com servidores adequados.

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

Comentários: em um ambiente cliente-servidor, os clientes solicitam serviços ou recursos (como arquivos, impressoras ou bancos de dados) e os servidores os disponibilizam de forma centralizada (Correto).

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

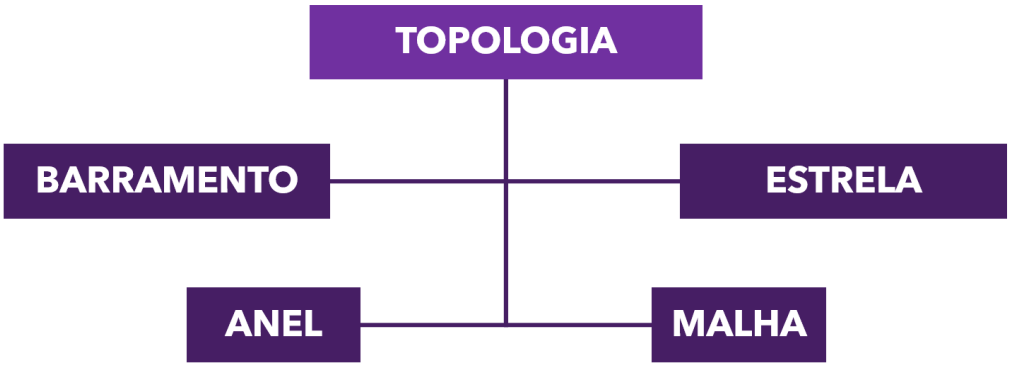
Comentários: na arquitetura cliente-servidor, os principais componentes são os servidores (que fornecem recursos), os clientes (que consomem esses recursos) e a rede que interliga ambos (Correto).

Quanto à Topologia (*Layout*)

TOPOLOGIA DE REDES DE COMPUTADORES

Topologia de rede é a maneira como os dispositivos (nós) estão fisicamente ou logicamente organizados e interconectados dentro da rede. Ela descreve o formato, a estrutura e os caminhos pelos quais os dados trafegam entre os dispositivos.

Quando falamos em topologia, estamos tratando da forma como os dispositivos estão organizados. Dois ou mais dispositivos se conectam a um link; dois ou mais links formam uma topologia. A topologia é a representação geométrica da relação de todos os links e os dispositivos de uma conexão entre si. Existem quatro topologias básicas[3] possíveis: barramento, estrela, anel e malha. No entanto, vamos primeiro entender a diferença entre topologia física e lógica.



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

TIPO DE TOPOLOGIA	DESCRIÇÃO
FÍSICA	Exibe o layout (disposição) dos links e nós de rede.

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

LÓGICA	Exibe o fluxo ou percurso dos dados na rede.

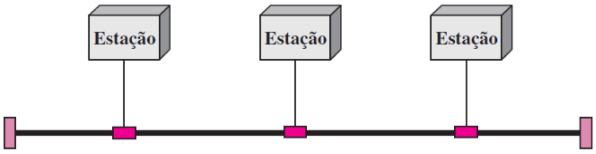
FIQUE ATENTO!

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

Barramento (Bus)

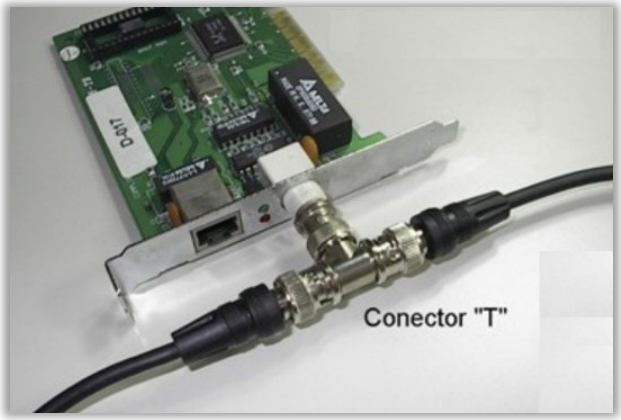
INCIDÊNCIA EM PROVA: ALTA

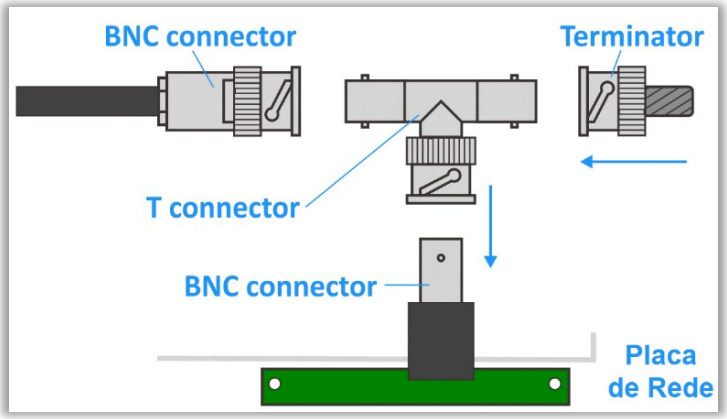
Na topologia em barramento, todas as estações de trabalho (computadores, impressoras, etc.) são conectadas a um único cabo central. Esse cabo é chamado de backbone ou espinha dorsal, e o tipo de cabo mais usado era o coaxial, com conectores especiais chamados BNC. Essa topologia cria uma conexão ponto-multiponto, onde todos compartilham o mesmo caminho para enviar e receber dados.



Quando uma estação envia um dado, esse sinal viaja pelo cabo em ambas as direções e é recebido por todas as estações conectadas. Porém, apenas o computador que for o verdadeiro destinatário vai "pegar" o dado – os outros simplesmente ignoram. Isso acontece porque cada estação tem uma placa de rede que filtra as mensagens e só aceita aquelas que forem destinadas a ela.

Um ponto importante dessa topologia é que apenas uma estação pode enviar dados por vez, funcionando de forma half-duplex (transmissão em um sentido por vez). Se duas estações tentarem enviar ao mesmo tempo, acontece uma colisão, que atrapalha a comunicação – parecido com duas pessoas tentando falar ao mesmo tempo em um walkie-talkie. Além disso, se o backbone se romper em qualquer ponto, toda a rede para de funcionar, inclusive os dispositivos que estavam do mesmo lado do problema.





Saiba mais:

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

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

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

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

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

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

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

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

Comentários: (a) Errado. Na topologia em anel, os dispositivos são conectados em sequência formando um circuito fechado, não utilizando um cabo backbone linear; (b) Errado. Na topologia em estrela, todos os dispositivos são conectados a um dispositivo central, e não a um único cabo backbone; (c) Errado. A topologia hierárquica organiza os dispositivos em níveis, semelhantes a uma árvore, diferente do uso de um único cabo principal; (d) Errado. Na topologia em malha, cada dispositivo se conecta diretamente a todos os outros, sem depender de um cabo backbone único; (e) Correto. Na topologia em barramento, todos os dispositivos são ligados a um único cabo backbone, que é terminado em ambas as extremidades para evitar reflexões de sinal (Letra E).

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

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

Comentários: (a) Errado. Na topologia em árvore, os dispositivos são organizados de forma hierárquica, como ramos de uma árvore, não em uma única linha de transmissão; (b) Errado. Na topologia em anel, os dispositivos são conectados formando um circuito fechado, onde os dados circulam em uma direção; (c) Correto. Na topologia em barramento, todos os computadores compartilham um único cabo de transmissão, geralmente coaxial, sendo uma estrutura simples de montar; (d) Errado. Na topologia em estrela, todos os dispositivos são conectados a um ponto central (como um switch ou hub), não a um único cabo (Letra C).

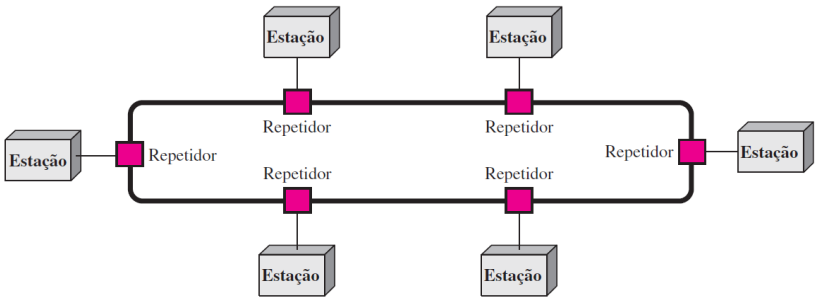
(QUADRIX / CRA-PA – 2019) Na topologia em barramento, apenas os computadores das extremidades (pontas) é que podem enviar dados para quaisquer computadores, pois, nesse tipo de topologia, eles são os gerenciadores da rede.

Comentários: na topologia em barramento, qualquer computador conectado ao cabo pode transmitir dados, e não há gerenciadores específicos nas extremidades; todos compartilham igualmente o meio de transmissão (Errado).

Anel (Ring)

INCIDÊNCIA EM PROVA: MÉDIA

Na topologia em anel, cada dispositivo é ligado diretamente a outros dois computadores vizinhos, formando um círculo. A comunicação entre eles acontece em apenas uma direção, o que chamamos de transmissão simplex. Quando um computador quer enviar uma mensagem, essa mensagem vai passando de um a um, de vizinho para vizinho, até chegar no destinatário correto. Depois que a mensagem dá a volta no anel e retorna para o computador que enviou, o caminho fica livre para o próximo a usar.



Funciona assim: o computador que quer enviar dados manda a mensagem para o vizinho. Esse vizinho verifica se a mensagem é para ele. Se não for, ele apenas passa a mensagem adiante para o próximo computador. Isso se repete até o destinatário certo receber a mensagem. Quando o computador certo recebe os dados, ele envia um aviso de volta para o remetente informando que tudo chegou certinho.

Como a mensagem passa por todos os computadores do anel, podemos dizer que o envio acontece em modo broadcast, mas só quem for o destinatário certo vai realmente pegar a informação. Um ponto importante dessa topologia é que não ocorrem colisões de dados (quando duas mensagens "batem" uma na outra). *E sabe por quê?* Porque existe um controle chamado Token. O Token é como se fosse um "passe" que circula pelo anel. Só quem estiver com o Token pode enviar uma mensagem. Parece até uma corrida de revezamento, onde o corredor só pode correr se estiver segurando o bastão!

Quando um computador quer mandar uma mensagem, ele pega o Token, coloca os dados dentro dele e manda para o próximo. A mensagem vai passando de computador em computador até chegar ao destino. O destinatário pega os dados e manda um aviso dentro do mesmo Token de que a mensagem foi recebida. O Token então continua circulando no anel até voltar ao computador que enviou. Depois disso, o Token fica livre para outro computador usar e enviar novas mensagens.

Essa topologia tem algumas vantagens: é relativamente fácil de instalar e configurar, já que para adicionar ou remover um computador basta mexer em poucas conexões. Também é mais simples identificar falhas, porque se um computador não confirmar que recebeu os dados, o problema é detectado rapidamente. No entanto, existem desvantagens: se o cabo do anel se romper ou se um computador parar de funcionar, toda a rede pode parar.

Saiba mais:

Imagine uma corrida de revezamento, onde quatro atletas correm em círculo em uma pista. Cada atleta só pode correr quando recebe o bastão do colega anterior. O bastão vai passando de mão em mão, sempre na mesma direção, até completar a volta. Na topologia em anel, funciona de forma parecida:

- Cada computador da rede com topologia em anel é como um atleta, ligado diretamente ao próximo em um círculo.

- As informações (dados) são como o bastão: elas passam de um computador para o outro em uma única direção.

- O computador só pode enviar dados quando "pega o bastão", ou seja, quando tem o controle do token (um sinal que autoriza a transmissão).

- Quando o computador termina de enviar sua informação, ele passa o token adiante para que outro possa transmitir.

Essa organização evita que dois computadores tentem falar ao mesmo tempo (não acontecem colisões), mas também significa que, se algum ponto do anel quebrar, toda a comunicação pode ser interrompida – como numa corrida em que um corredor deixa o bastão cair.

Além disso, se houver muitos computadores, o envio das mensagens pode ficar mais lento. Para melhorar, surgiram tecnologias como o FDDI, que usam dois anéis para garantir mais segurança e rapidez.

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

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

Comentários: na topologia em anel, a comunicação entre os nós pode ocorrer tanto no sentido horário quanto anti-horário, dependendo da configuração da rede e da tecnologia utilizada (Errado).

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

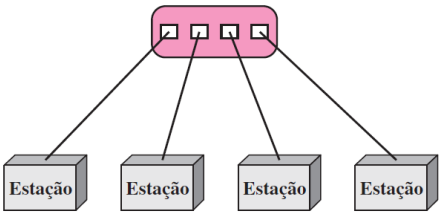
Comentários: na topologia em anel de uma rede de computadores, os dispositivos não estão conectados a um hub central. Na verdade, cada dispositivo está conectado diretamente ao dispositivo vizinho, formando um circuito fechado, seja fisicamente (anel físico) ou logicamente (anel lógico). Não há um hub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

Estrela (*Star*)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Na topologia em estrela, todos os computadores (ou estações de trabalho) são conectados diretamente a um nó central[4] – que pode ser um switch ou um hub. Cada conexão entre o computador e o nó central é ponto-a-ponto, ou seja, exclusiva, mas isso não significa que a arquitetura da rede seja ponto-a-ponto! Apenas o cabo entre o computador e o nó é dedicado. Quando uma estação quer enviar dados para outra, a informação sempre passa primeiro pelo nó central.

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



Essa é a topologia mais utilizada atualmente, porque é muito fácil de adicionar ou remover computadores. Se quiser colocar um novo computador na rede, basta conectá-lo a uma porta disponível no nó central. Da mesma forma, se um cabo quebrar ou um computador der problema, apenas aquele computador fica fora do ar – a rede toda continua funcionando normalmente. Isso também facilita muito a identificação de falhas, pois fica fácil descobrir qual conexão deu problema.

Saiba mais:

Imagine uma central de táxis. Todos os taxistas da cidade se comunicam apenas com a central, e não diretamente entre si. Quando um passageiro precisa de um táxi, ele liga para a central, que então localiza um taxista e passa a chamada para ele. Na topologia em estrela, funciona do mesmo jeito:

- Cada computador (como um taxista) está ligado diretamente a um nó central (como a central de táxis), que é normalmente um switch ou hub.

- Quando um computador quer enviar dados, ele não se conecta diretamente ao destino. Ele envia a informação para o nó central, que então encaminha para o computador de destino.

- Se o cabo de um computador quebrar, apenas aquele computador é afetado – o resto da rede continua funcionando.

- No entanto, se a central (o nó central) falhar, toda a comunicação para e ninguém mais consegue se falar.

Por outro lado, a topologia em estrela tem uma desvantagem importante: o nó central é um ponto único de falha. Se ele parar de funcionar, toda a rede fica comprometida. Para evitar esse problema, muitas redes usam dispositivos redundantes, ou seja, equipamentos extras que assumem a função caso o principal falhe, garantindo que tudo continue funcionando sem interrupções.

CARACTERÍSTICAS DA ESTRELA	DESCRIÇÃO
DEFINIÇÃO	Uma topologia de rede onde todos os dispositivos estão conectados a um ponto central, como um hub ou switch.
ESCALABILIDADE	Alta, fácil de adicionar novos dispositivos sem afetar significativamente a rede existente.
CONFIABILIDADE	Alta, uma vez que a falha em um dispositivo geralmente não afeta os outros.
DESEMPENHO	Bom, pois o tráfego de dados é gerenciado pelo ponto central, reduzindo congestionamentos.
MANUTENÇÃO	Relativamente fácil, pois problemas geralmente se limitam a dispositivos individuais e são fáceis de isolar.
COMPLEXIDADE	Baixa a moderada, devido à simplicidade da configuração e gerenciamento da rede.

LATÊNCIA	Geralmente baixa, especialmente em redes com switches modernos que gerenciam o tráfego de forma eficiente.
SEGURANÇA	Boa, pois é mais fácil monitorar e controlar o acesso à rede através do ponto central.
ISOLAMENTO DE PROBLEMAS	Excelente, falhas em dispositivos individuais geralmente não impactam o resto da rede.
TIPOS DE APLICAÇÃO	Adequada para redes domésticas e empresariais onde a facilidade de manutenção e a confiabilidade são prioritárias.

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

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

Comentários: (a) Errado. Na topologia em barramento, todos os dispositivos são conectados a um único cabo compartilhado, e não a um ponto central; (b) Errado. Na topologia hierárquica, os dispositivos são organizados em camadas ou níveis, e não diretamente a um ponto central; (c) Errado. Na topologia em anel, os dispositivos formam um circuito fechado, sem um ponto central; (d) Correto. Na topologia em estrela, todos os hosts são conectados a um ponto central, como um switch ou hub, que gerencia a comunicação; (e) Errado. Na topologia em malha, os dispositivos se conectam diretamente uns aos outros, não passando por um único ponto central (Letra D).

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

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

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



Do ponto de vista físico, essa topologia é conhecida por

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

Comentários: (a) Errado. A topologia em anel (ou cíclica) conecta os dispositivos em um circuito fechado, sem um ponto central, diferente do que a imagem mostra; (b) Errado. Na topologia em malha (mesh), todos os dispositivos se conectam diretamente uns aos outros, e não a um único ponto central; (c) Errado. Uma topologia distribuída ou descentralizada não apresenta um elemento central como o mostrado na imagem; (d) Errado. A topologia em árvore (ou hierárquica) se organiza de forma ramificada em níveis, e não com conexões diretas a um centro; (e) Correto. A imagem mostra a topologia estrela, onde todos os dispositivos estão conectados a um ponto central, caracterizando uma estrutura radial (Letra E).

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

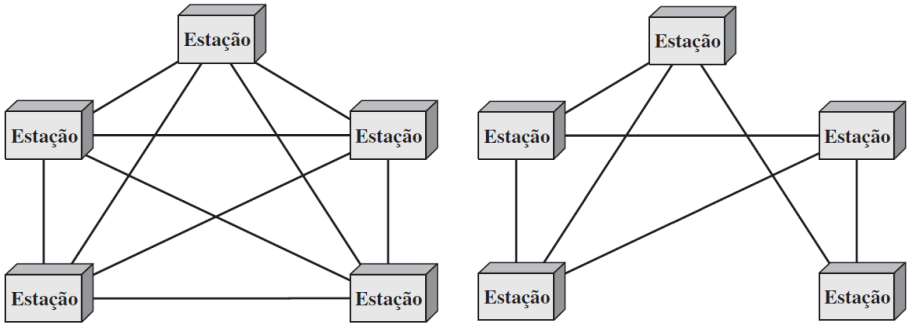
a) Mesh
b) Estrela
c) Híbrida
d) Barramento

Comentários: (a) Errado. Na topologia Mesh (malha), todos os dispositivos se conectam diretamente uns aos outros, sem um ponto central único de falha; (b) Correto. Na topologia Estrela, todos os dispositivos são conectados a um elemento central (hub ou switch); se esse dispositivo falhar, toda a rede é comprometida; (c) Errado. A topologia Híbrida combina características de duas ou mais topologias diferentes, podendo ou não ter um único ponto de falha; (d) Errado. Na topologia Barramento, todos os dispositivos compartilham um único cabo principal, sem um elemento central de comunicação.

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].



[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 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. Já as desvantagens 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! 😱

Em redes WAN, é comum o uso de uma malha parcial para fornecer redundância entre pontos críticos, mas não é a topologia predominante para conexões simples de matriz e filial, que geralmente usam uma topologia em estrela. Por outro lado, a topologia em malha encontrou sua principal aplicação prática e popularidade nas redes wireless (WLAN), onde os nós se interconectam sem fio para formar uma rede de grande cobertura e resiliente, como nos sistemas Wi-Fi Mesh para ambientes domésticos e corporativos.

Saiba mais:

Imagine que você mora em um bairro onde todas as casas estão ligadas umas às outras por caminhos exclusivos. Cada casa tem uma trilha direta que leva a todas as outras casas do bairro. Se você quiser visitar um vizinho, não precisa passar pela casa de ninguém — você já tem um caminho direto e exclusivo até ele. Na topologia em malha, funciona do mesmo jeito:

- Nesse contexto, cada computador está conectado diretamente a todos os outros computadores da rede.

- Se um caminho ficar bloqueado (por exemplo, se uma trilha quebrar), você ainda pode chegar ao seu destino por outro caminho.

- Isso garante que a comunicação seja rápida, segura e muito confiável, porque existem várias alternativas para enviar as informações.

O lado ruim é que construir tantas trilhas dá muito trabalho e gasta muito material – do mesmo jeito que, na rede em malha, seria caro e complicado fazer cabos para ligar todo mundo diretamente a todo mundo.

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



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

Na prática, sempre que você se mover pela casa ou escritório, você terá que ir trocando de rede para ter o melhor sinal possível. Já em redes *mesh*, isso não é necessário: ela identifica onde está o nó com o sinal mais forte e se conecta automaticamente à medida que você vai se movendo pela casa. Enfim... trata-se de um belo investimento para quem tem problema de sinal (eu tenho um e garanto!).

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

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

TOPOLOGIA FÍSICA	DIREÇÃO DE TRANSMISSÃO	TIPO DE ENLACE	MODOS DE TRANSMISSÃO
BARRAMENTO	Half-Duplex	Multiponto	Broadcast

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

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

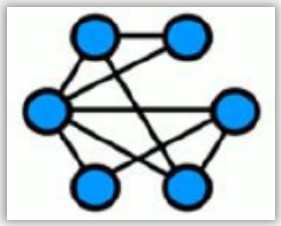
a) Anel (ring).
b) Estrela (star).
c) Malha (mesh).
d) Barramento (bus).

Comentários: (a) Errado. Na topologia em anel, os dispositivos são conectados em um circuito fechado, mas não diretamente a todos os outros dispositivos; (b) Errado. Na topologia em estrela, os dispositivos são conectados a um ponto central, e não diretamente uns aos outros; (c) Correto. Na topologia em malha (mesh), cada dispositivo é conectado diretamente a todos os outros, proporcionando alta confiabilidade e robustez; (d) Errado. Na topologia em barramento, todos os dispositivos compartilham um único cabo, e não se conectam diretamente entre si (Letra C).

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

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

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



A topologia representada na imagem acima é a:

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

Comentários: (a) Errado. A topologia em barramento conecta todos os dispositivos a um único cabo central, o que não é mostrado na imagem; (b) Errado. Topologia mista combina características de duas ou mais topologias, mas a imagem mostra conexões diretas

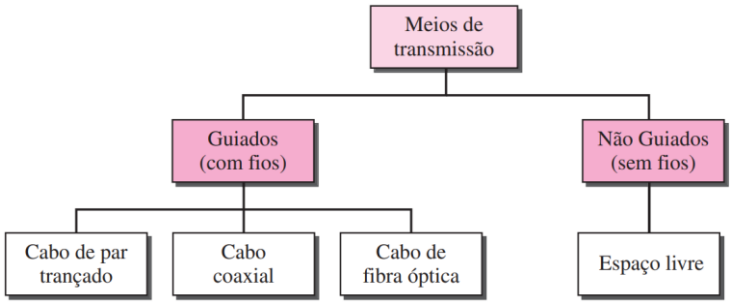
entre todos os nós; (c) Correto. A topologia em malha (mesh) é caracterizada pela conexão direta entre todos os dispositivos, como ilustrado na imagem; (d) Errado. A topologia em árvore organiza dispositivos em uma estrutura hierárquica, semelhante a galhos, o que não corresponde à imagem; (e) Errado. Na topologia em estrela, todos os dispositivos se conectam a um único ponto central, diferente das conexões múltiplas mostradas (Letra C).

Meios de Transmissão

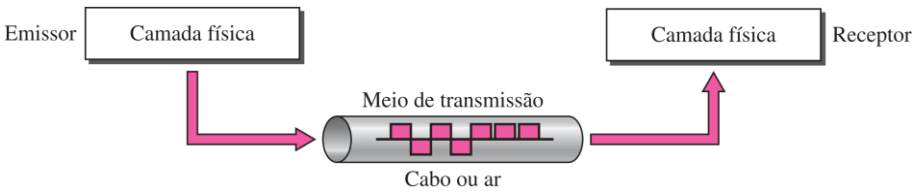
MEIOS DE TRANSMISSÃO

Em redes de computadores, meios de transmissão são os caminhos físicos ou lógicos por onde os dados viajam de um dispositivo a outro dentro da rede. Em outras palavras, são os meios que carregam as informações (sinais elétricos, ondas de rádio, luz, entre outros) de um ponto até outro.

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



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



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

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

Comentários: (a) Errado. O cabo de par trançado é um meio guiado (físico), enquanto ondas de rádio são não guiadas; portanto, a alternativa mistura tipos diferentes; (b) Errado. O cabo coaxial é um meio guiado, enquanto micro-ondas são não guiadas; logo, também há mistura de tipos; (c) Errado. O cabo de fibra ótica é um meio guiado, enquanto micro-ondas são não guiadas; novamente, mistura de tipos; (d) Errado. O cabo de par trançado é um meio guiado, enquanto micro-ondas são não guiadas; mistura de meios;

(e) Correto. Ondas de rádio e micro-ondas são meios de transmissão não guiados, pois propagam sinais pelo ar sem a necessidade de cabos físicos (Letra E).

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

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

Comentários: (a) Correto. Cabo coaxial, cabo de par trançado e cabo de fibra óptica são exemplos clássicos de meios de transmissão guiados, pois utilizam um meio físico para transportar os sinais; (b) Errado. Transmissão via satélite e via rádio utilizam meios não guiados, propagando sinais pelo ar sem fio; (c) Errado. Embora o cabo de fibra óptica seja um meio guiado, a alternativa limita a resposta a apenas ele, ignorando outros meios guiados como o par trançado e o coaxial; (d) Errado. O cabo de par trançado é um meio guiado, mas a transmissão via satélite é não guiada; (e) Errado. A transmissão via rádio é um meio não guiado, pois ocorre pelo ar (Letra A).

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

Comentários: o cabo UTP (par trançado) e as fibras ópticas são exemplos de meios de transmissão guiados, pois os dados são transportados através de um meio físico definido (Errado).

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

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

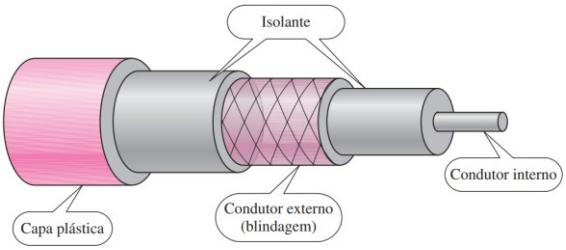
Comentários: (a) Errado. A fibra óptica é um meio guiado, pois conduz sinais de luz em um meio físico (cabo); (b) Errado. O cabo de par trançado é um meio guiado, utilizando fios para transportar sinais elétricos; (c) Correto. Uma rede sem fio utiliza meios não guiados, como ondas de rádio, para transmitir dados pelo ar sem a necessidade de cabos; (d) Errado. A Internet é uma rede que utiliza diversos meios (guiados e não guiados), não sendo, por si, um tipo específico de meio de transmissão; (e) Errado. O cabo coaxial é um meio guiado, que transporta sinais elétricos em seu interior (Letra C).

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

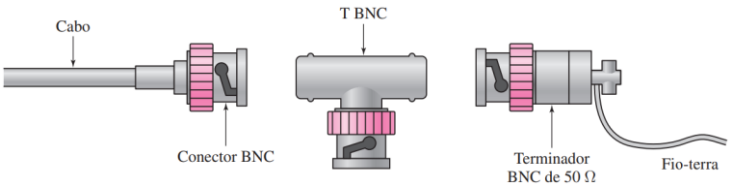
Comentários: cabos de par trançado, coaxial e fibras ópticas são populares meios de transmissão de dados guiados, ou seja, são materiais que conduzem a informação enviada do transmissor ao receptor (Errado).

Cabo Coaxial

INCIDÊNCIA EM PROVA: BAIXA



Consiste em um fio central de cobre, envolvido por uma blindagem metálica. Isolantes de plástico flexível separam os condutores internos e externos e outras camadas do revestimento que cobrem a malha externa. Esse meio de transmissão é mais barato, pouco flexível e muito resistente à interferência eletromagnéticas graças a sua malha de proteção. Ele cobre distâncias maiores que o cabo de par trançado e utiliza um conector chamado BNC[6].



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



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

FIQUE ATENTO!

A **Taxa de Transferência (Throughput)** mede a quantidade de dados real que é transferida em uma quantidade específica de tempo. Em outras palavras, mede a velocidade da transmissão de dados. Obviamente, quanto maior a taxa de transferência, melhor, pois mais rapidamente dados poderão ser transferidos na rede.

Exemplo: em uma rede com largura de banda de 100 Mbps, a taxa de transmissão pode ser apenas de 70 Mbps devido a fatores como atrasos na rede e sobrecarga de comunicação.

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

Já a **Largura de Banda (Bandwidth)** é uma medida da capacidade de transmissão teórica de uma rede e refere-se à quantidade máxima de dados que pode ser transmitida por um canal de comunicação em um determinado período de tempo.

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

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

(PROF. DIEGO / INÉDITA – 2025) Cabos coaxiais são mais finos e flexíveis em comparação com cabos de fibra óptica.

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

(PROF. DIEGO / INÉDITA – 2025) Cabos coaxiais geralmente usam conectores do tipo BNC (Bayonet Neill-Concelman) para estabelecer conexões.

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

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

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

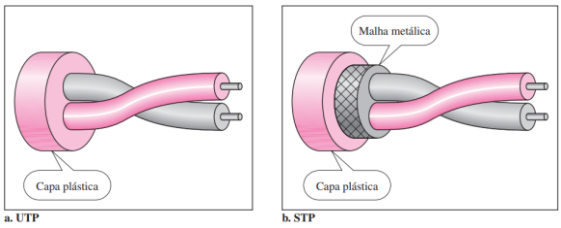
(CEBRASPE / FUB – 2015) O cabo coaxial, meio físico de comunicação, é resistente à água e a outras substâncias corrosivas, apresenta largura de banda muito maior que um par trançado, realiza conexões entre pontos a quilômetros de distância e é imune a ruídos elétricos.

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

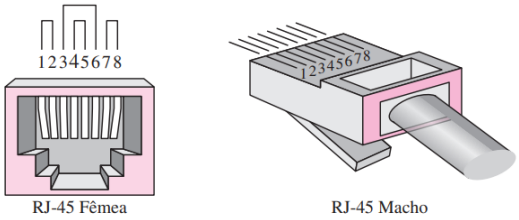
O Cabo Coaxial não é imune a ruídos elétricos (apesar de ser muito resistente). Ademais, ele é relativamente resistente a substâncias corrosivas, mas não vai resistir – por exemplo – a ácido sulfúrico. Por fim, ele realmente apresenta uma largura de banda maior que o cabo de par traçado, apesar de ter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

Cabo de Par Trançado

INCIDÊNCIA EM PROVA: ALTA

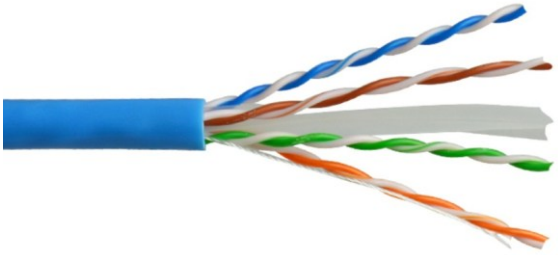


Consiste em quatro pares de fios trançados blindados ou não, e envolto de um revestimento externo flexível. Eles são trançados para diminuir a interferência eletromagnética externa e interna – quanto mais giros, maior a atenuação. Este é o cabo mais utilizado atualmente por ser o mais barato de todos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



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 DE CABOS	TAXA MÁXIMA DE TRANSMISSÃO	LARGURA DE BANDA	DISTÂNCIA MÁXIMA
CAT3	Até 10 Mbps	16 MHz	100 Metros
CAT4	Até 16 Mbps	20 MHz	100 Metros
CAT5	Até 100 Mbps	100 MHz	100 Metros
CAT5e	Até 1000 Mbps (1G)	100 MHz	100 Metros
CAT6	Até 10000 Mbps (10G)	250 MHz	100 Metros
CAT6A	Até 10000 Mbps (10G)	500 MHz	100 Metros
CAT7	Até 10000 Mbps (10G)	600 MHz	100 Metros
CAT7A	Até 10000 Mbps (10G)	1000 MHz	100 Metros
CAT8	Até 40000 Mbps (40G)	2000 MHz	100 Metros





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

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

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

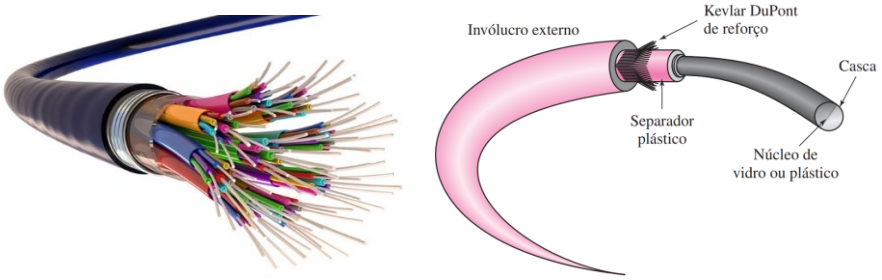
Comentários: (a) Errado. O cabo coaxial possui um único condutor central rodeado por uma blindagem, e não quatro pares de fios trançados; (b) Correto. O cabo de par trançado é composto por quatro pares de fios de cobre trançados e é amplamente utilizado em redes locais (LANs) para interligações de até 100 metros; (c) Errado. A fibra ótica transmite sinais de luz e não utiliza fios de cobre trançados; (d) Errado. Comunicação serial refere-se ao modo de transmissão dos dados, não a um tipo de cabo específico com fios trançados; (e) Errado. Comunicação paralela também descreve uma forma de transmissão de dados, não um cabo com características de par trançado (Letra B).

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

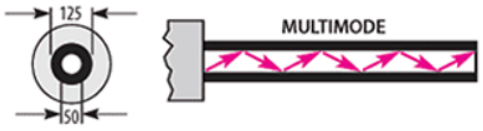
Comentários: o cabo de par trançado sem blindagem é mais comum, dado que a blindagem é um revestimento que torna o cabo mais caro e é mais útil em ambientes que tendem a sofrer maior interferência eletromagnética (Correto).

Cabo de Fibra Óptica

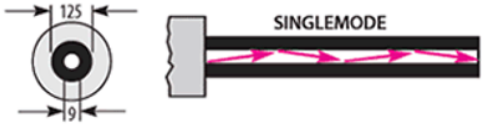
INCIDÊNCIA EM PROVA: MÉDIA



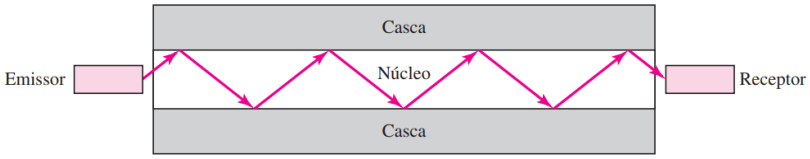
O cabo de fibra óptica consiste em uma casca e um núcleo (de vidro, mais comum; ou plástico) para transmissão de luz. Esse tipo de cabo é normalmente encontrado em backbones de redes por apresentar excelente relação entre ampla largura de banda e custo. Hoje em dia, podemos transferir dados à velocidade de até 1.600 Gbps. A tecnologia atual suporta dois modos para propagação da luz ao longo de canais ópticos, cada um dos quais exigindo fibras ópticas com características físicas diferentes:



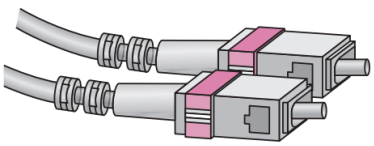
A Fibra Multimodo leva o feixe de luz por vários modos ou caminhos, por uma distância menor, com menores taxas de transmissão, mais imprecisa, diâmetro maior e alto índice de refração e atenuação, mas possui construção mais simples, é mais barata e utilizada em LANs.

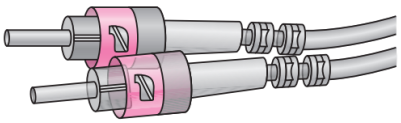


A Fibra Monomodo leva o feixe de luz por um único modo ou caminho, por uma distância maior, com maiores taxas de transmissão, mais precisa, diâmetro menor e baixo índice de refração e atenuação, mas possui construção mais complexa, é mais cara e utilizada em WANs.



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


Conector SC


Conector ST

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

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

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

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

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

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

Estão corretas:

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

Comentários: (I) Correto. A fibra óptica utiliza feixes de luz (geralmente lasers ou LEDs) para transmitir dados com alta velocidade e eficiência; (II) Correto. A fibra óptica é imune a interferências eletromagnéticas, pois transmite sinais por meio de luz, não por corrente elétrica; (III) Correto. O custo da fibra óptica, tanto para aquisição quanto para instalação, é maior que o dos cabos metálicos, como o de par trançado (Letra A).

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

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

Saiba mais:

Imagine uma empresa grande, com várias áreas separadas: o prédio administrativo, o galpão de armazenamento e a sala do datacenter.

| Cabo coaxial: no galpão de armazenamento, a empresa ainda usa câmeras de segurança antigas que transmitem imagens para a central de monitoramento através de cabos coaxiais. Esses cabos são resistentes a interferências e, antigamente, eram muito usados para esse tipo de transmissão.

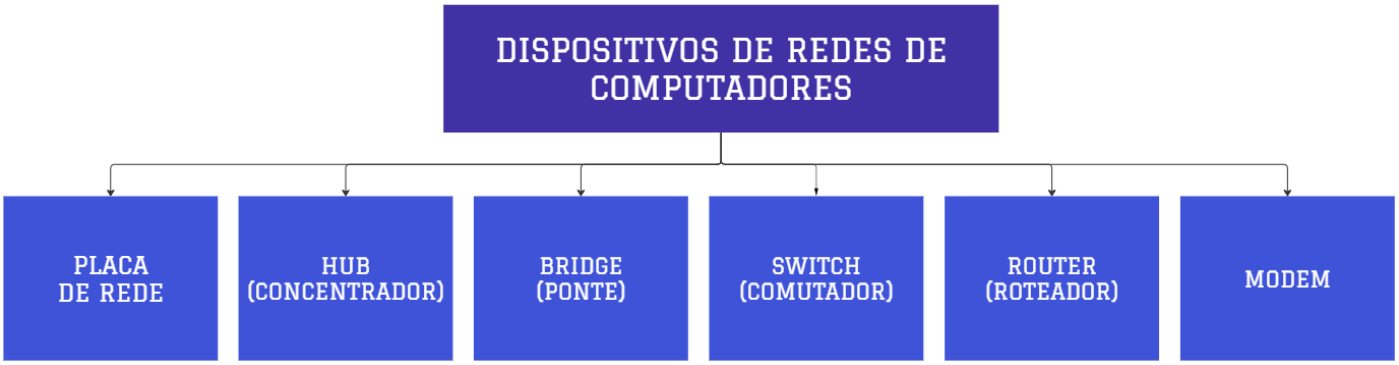
| **Cabo de Par Trançado:** no prédio administrativo, todos os computadores dos escritórios estão conectados à rede local (LAN) usando cabos de par trançado (como cabos de rede Ethernet com conectores RJ-45). Esses cabos são baratos, fáceis de instalar e ideais para conexões dentro de ambientes internos.

| **Cabo de fibra óptica:** para interligar o prédio administrativo ao datacenter, que fica a alguns quilômetros de distância, a empresa instalou um cabo de fibra óptica. A fibra permite uma transmissão de dados em altíssima velocidade e sem perdas de qualidade, mesmo em grandes distâncias.

CARACTERÍSTICAS	CABO COAXIAL	PAR TRANÇADO	FIBRA ÓPTICA
DESCRIÇÃO	Cabo com um fio condutor central, isolado por uma malha metálica	Dois fios de cobre entrelaçados para reduzir interferências	Fios de vidro ou plástico que transmitem dados na forma de luz.
VELOCIDADE	Média (até 1 Gbps, dependendo do tipo)	Média a alta (até 10 Gbps ou mais)	Altíssima (dezenas a centenas de Gbps)
ALCANCE	Médio (poucas centenas de metros)	Curto (até 100 metros sem repetição)	Muito longo (vários quilômetros sem perda significativa)
IMUNIDADE	Boa (devido à blindagem)	Moderada (melhor se blindado - STP)	Excelente (não sofre interferência eletromagnética)
CUSTO	Médio	Baixo	Alto (mas vem caindo com o tempo)
USO TÍPICO	Redes locais antigas, TV a cabo	Redes locais (LANs), cabeamento estruturado	Redes backbone, redes de alta velocidade, longas distâncias
INSTALAÇÃO	Moderada	Fácil	Mais complexa (delicada e precisa)

Equipamentos de Redes

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, entre outros); no segundo caso, trata-se daqueles que compõem a infraestrutura de uma rede (Hub, Bridge, Switch, Router, entre outros). Nós vamos focar agora nos dispositivos intermediários. Venham comigo...



Network Interface Card (Placa/Adaptador de Rede)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

ADAPTADOR/PLACA DE REDE

Trata-se de um hardware que permite a um dispositivo se conectar a uma rede, seja por cabo (Ethernet) ou sem fio (Wi-Fi). Ela atua como um intermediário entre o computador e a rede, garantindo que os dados sejam transmitidos corretamente.





Um dispositivo muito importante nas redes de computadores é a placa de rede, também chamada de placa NIC (Network Interface Card). Trata-se de um equipamento eletrônico, que pode ser interno ou externo ao computador, contendo circuitos que permitem que uma estação de trabalho se conecte a uma rede. Em outras palavras, a placa de rede é o hardware responsável por fazer a ponte entre o computador e o meio físico da rede, seja usando cabos ou através de uma conexão sem fio.

As placas de rede podem ser instaladas diretamente dentro do computador – que é a forma mais comum – ou podem ser dispositivos externos, como pequenos adaptadores USB. Se você observar a parte de trás do gabinete de um computador de mesa, provavelmente verá uma placa de rede conectada a um cabo de par trançado. Já em notebooks, além da placa cabeada, normalmente existe uma placa wireless, que possibilita a conexão via Wi-Fi.

Essas placas permitem uma comunicação bidirecional, ou seja, possibilitam tanto a transmissão quanto o recebimento de dados entre os dispositivos da rede. Sem a placa de rede, não seria possível que um computador acessasse a internet ou se conectasse a uma rede local. Por isso, elas são essenciais em desktops, notebooks, servidores e vários outros equipamentos conectados.

Além disso, as placas de rede podem suportar diferentes tipos de tecnologias, como conexões Ethernet (cabeadas) ou conexões sem fio (Wi-Fi). A função principal delas é converter os dados gerados pelo computador em sinais que possam ser transmitidos pela rede e também receber sinais da rede para convertê-los novamente em dados que o computador consiga entender.

Agora vem um detalhe muito importante: toda placa de rede possui um identificador único chamado Endereço MAC (Media Access Control). Esse endereço é gravado na placa de rede já na fábrica e, de forma geral, não pode ser alterado (salvo em situações muito específicas). O endereço MAC é formado por uma sequência de 12 dígitos hexadecimais, o que corresponde a 48 bits. Normalmente, ele é escrito separando os números em pares, como neste exemplo:

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

O endereço MAC é fundamental para o funcionamento da comunicação dentro da rede. Ele é usado para identificar de maneira única cada dispositivo em uma rede local, evitando confusão e garantindo que os dados enviados cheguem exatamente ao destinatário certo. Cada fabricante de placas de rede recebe uma faixa exclusiva de endereços MAC para gravar nos seus equipamentos, o que evita conflitos de identificação entre dispositivos em todo o mundo.

Tabela Resumo

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

(PROF. DIEGO / INÉDITA – 2025) Uma placa de rede não é necessária em um computador para conexão com a Internet, pois os modems modernos desempenham essa função.

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

(PROF. DIEGO / INÉDITA – 2025) Placas de rede são adequadas apenas para redes com fio e não podem ser usadas em redes sem fio (Wi-Fi).

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

Ethernet com cabos, enquanto placas de rede sem fio são usadas em redes Wi-Fi, que funcionam de maneira wireless (sem fio) (Errado).

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

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

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

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

Comentários: (a) Correto. O endereço MAC (Media Access Control) é o endereço físico único atribuído pelo fabricante à placa de rede, tanto para redes cabeadas quanto para redes sem fio; (b) Errado. O endereço IP é um identificador lógico atribuído para comunicação em redes baseadas no protocolo IP, podendo ser alterado; (c) Errado. DHCP (Dynamic Host Configuration Protocol) é o protocolo que atribui endereços IP dinamicamente na rede; (d) Errado. DNS (Domain Name System) é o sistema que traduz nomes de domínio em endereços IP, não relacionado a endereços físicos; (e) Errado. UDP (User Datagram Protocol) é um protocolo de transporte utilizado na comunicação de dados, sem relação com endereçamento físico (Letra A).

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

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

Comentários: (a) Errado. Endereço WWW refere-se a endereços de sites na web e não a um identificador físico de uma placa de rede; (b) Errado. Endereço IP é um endereço lógico usado para comunicação na rede, podendo ser alterado e não é fixo como o endereço da placa de rede; (c) Correto. O endereço MAC (Media Access Control) é um número único gravado na placa de rede pelo fabricante, identificando o dispositivo fisicamente; (d) Errado. Endereço de e-mail é usado para comunicação eletrônica de mensagens, não tem relação com identificação física de dispositivos de rede (Letra C).

Hub (Concentrador)

INCIDÊNCIA EM PROVA: MÉDIA

HUB (CONCENTRADOR)

Trata-se de um dispositivo de rede que funciona como um ponto central de conexão, permitindo que vários dispositivos se comuniquem dentro de uma mesma rede local (LAN). Ele recebe os dados de um dispositivo e os transmite para todos os outros conectados, sem filtrar ou direcionar a informação.



Antes de mais nada, é importante saber que existem dois tipos de hubs: ativos e passivos. Um hub passivo funciona basicamente como um conector: ele apenas reúne e conecta vários cabos que vêm de diferentes pontos da rede. Ele não precisa ser ligado à tomada, porque não tem energia elétrica e não faz nenhum tipo de processamento no sinal que passa por ele. Em provas e questões de concurso, se o enunciado não disser claramente que se trata de um hub passivo, podemos assumir que está falando de hub ativo.

Tipos de Hubs

O hub ativo é um dispositivo que serve para interligar computadores, concentrar os cabos e, principalmente, aumentar o alcance da rede local. Dentro de uma rede, os sinais que carregam dados conseguem viajar apenas até uma certa distância. Depois disso, o sinal vai ficando fraco (se atenua) e corre o risco de se perder, causando problemas na transmissão dos dados. É aí que o hub ativo entra: ele recebe o sinal digital e regenera esse sinal, reforçando-o antes que fique fraco ou corrompido. Em outras palavras, o hub ativo funciona como um tipo de repetidor – ele renova o sinal e o manda adiante.

Por isso, o hub ativo é considerado um repetidor multiportas: ele recebe o sinal em uma porta, "dá um gás" nele, e transmite para as outras portas. Antigamente, ele era bastante usado, mas hoje em dia está praticamente obsoleto, substituído por equipamentos mais inteligentes. Um ponto importante: o hub é conhecido como um dispositivo "burro". *Por quê?* Porque ele não sabe para onde enviar os dados.

Quando um dado chega, o hub simplesmente envia a informação para todas as portas – não importa quem é o verdadeiro destinatário. Isso é chamado de broadcast. Dessa forma, só uma máquina pode transmitir dados por vez para evitar colisões, e o funcionamento do hub é half-duplex, ou seja, os dados vão em uma direção de cada vez (não é possível enviar e receber ao mesmo tempo). A representação de um Hub é apresentada abaixo:



FIQUE ATENTO!

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

Aproveitando para revisar o que aprendemos sobre topologias: a topologia física mostra como os cabos e dispositivos estão fisicamente organizados na rede. Já a topologia lógica mostra como os dados realmente circulam entre os dispositivos. Pensando nisso: se o hub concentra todos os cabos em um único local, fisicamente ele forma uma estrela (topologia física em estrela); mas como ele envia os dados para todos os dispositivos (faz broadcast), logicamente ele se comporta como uma rede em barramento (topologia lógica em barramento).

Tabela Resumo

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

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

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

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

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

Comentários: (a) Errado. Host é qualquer dispositivo conectado à rede, como computadores e servidores, e não um equipamento de interconexão; (b) Errado. Router (roteador) é um dispositivo que direciona pacotes entre redes diferentes, realizando o roteamento de dados de forma inteligente; (c) Correto. O hub atua apenas como um repetidor, enviando dados recebidos para todas as portas, sem capacidade de direcionar a comunicação, motivo pelo qual caiu em desuso; (d) Errado. O switch substituiu o hub por ser capaz de encaminhar dados de forma eficiente apenas para o destino correto na rede (Letra C).

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

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

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

Comentários: fisicamente, o hub conecta todos os dispositivos a um ponto central (estrela), mas logicamente o tráfego é compartilhado como em um barramento, já que todos recebem todos os sinais transmitidos (Correto).

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

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

Comentários: (a) Errado. Parser é um termo usado em programação para analisar sintaxe de textos ou dados, não relacionado a redes de computadores; (b) Correto. O hub é conhecido como concentrador, sua função é interligar computadores em uma rede local e retransmitir os dados para todas as máquinas conectadas; (c) Errado. Router (roteador) direciona pacotes entre redes diferentes, e não apenas retransmite dados dentro de uma rede local; (d) Errado. Bridge conecta duas redes locais (LANs) separadas, operando de forma mais inteligente que um hub; (e) Errado. Gateway atua como ponto de acesso entre redes com diferentes protocolos de comunicação, não como simples concentrador (Letra B).

Bridge (Ponte)

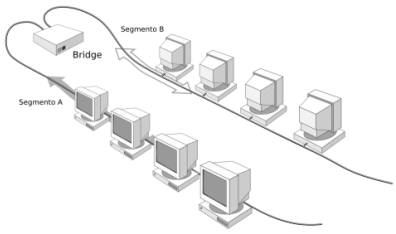
INCIDÊNCIA EM PROVA: BAIXÍSSIMA

BRIDGE / PONTE

Trata-se de um dispositivo de rede que conecta dois ou mais segmentos de uma rede local, permitindo a comunicação entre eles como se fossem uma única rede. Sua principal função é filtrar e encaminhar pacotes com base nos endereços MAC, ajudando a reduzir o tráfego desnecessário e evitando colisões.

Uma bridge é um dispositivo que ajuda na comunicação entre diferentes partes de uma rede, filtrando e direcionando os dados para onde realmente precisam ir. Ao contrário de um hub, que simplesmente distribui tudo para todos, a bridge verifica quem realmente deve receber a informação antes de encaminhá-la. *E como funciona?*

Imagine que a rede seja uma grande sala cheia de pessoas conversando. Se todos falassem ao mesmo tempo, seria confuso, certo? A bridge funciona como um organizador, filtrando as mensagens e garantindo que cada uma chegue ao destinatário correto sem atrapalhar os outros. Ela usa uma tabela de endereços, que associa cada dispositivo da rede a uma porta específica, garantindo que os dados sejam enviados apenas para quem precisa recebê-los.



Uma bridge também pode conectar diferentes segmentos da rede. Um segmento é uma subdivisão da rede, como separar grupos de amigos em diferentes mesas de um restaurante. Isso ajuda a reduzir o tráfego de dados e evita que todos recebam informações que não precisam. Se um computador no Segmento A quiser enviar algo para o Segmento B, a bridge faz esse trabalho, garantindo que os dados não atrapalhem os dispositivos que não estão envolvidos na conversa.

Tipos de Bridges

O principal benefício da bridge é a redução do tráfego. Em uma rede sem controle, como um hub, os dados são enviados para todos os dispositivos, o que pode causar congestionamento e colisões. A Bridge evita esse problema, garantindo que apenas o destinatário correto receba as informações. Existem diferentes tipos de bridges, dependendo da necessidade da rede:

- **Bridge Simples:** tem apenas duas portas e conecta dois segmentos.
- **Bridge Multiporta:** pode conectar vários segmentos ao mesmo tempo.
- **Bridge Transparente:** funciona sem precisar de configuração, como se fosse invisível na rede.
- **Bridge de Tradução:** conecta redes que usam tecnologias diferentes (Ex: Ethernet e Token Ring).

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

Tabela Resumo

BRIDGES	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede utilizada para dividir uma rede em segmentos menores, reduzindo colisões e tráfego de rede desnecessário (está em desuso atualmente).

CAMADA OSI	Camada 2 (Enlace).
VANTAGENS	Filtra o tráfego, melhorando o desempenho; pode conectar diferentes tipos de redes (Ex: Ethernet e Wi-Fi); aumenta a segurança da rede, criando domínios de colisão separados.
DESVANTAGENS	Pode ser mais caro que um hub simples; requer configuração e gerenciamento adequados; limitação da extensão da rede e complexidade de gerenciamento em redes maiores.

(PROF. DIEGO / INÉDITA – 2025) Bridges ajudam a dividir uma rede em segmentos para reduzir o tráfego e melhorar o desempenho.

Comentários: as bridges operam na camada de enlace (nível 2 do modelo OSI) e segmentam a rede, filtrando e encaminhando o tráfego apenas para o segmento necessário, reduzindo o congestionamento e melhorando o desempenho (Correto).

(PROF. DIEGO / INÉDITA – 2025) As pontes são utilizadas – na grande maioria das vezes – para conectar redes com diferentes protocolos de comunicação.

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

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

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

Comentários: (a) Errado. Gateway faz a comunicação entre redes com protocolos diferentes, não unifica LANs físicas em uma só lógica; (b) Errado. Roteador conecta redes distintas e direciona pacotes, não é o responsável por unificar LANs físicas em uma LAN lógica; (c) Errado. Repetidor apenas amplifica sinais, não agrupa LANs; (d) Correto. A bridge conecta várias LANs físicas, formando uma única LAN lógica ao filtrar e encaminhar pacotes na camada de enlace; (e) Errado. Hub apenas replica o sinal para todos os dispositivos e não cria uma LAN lógica única (Letra D).

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

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

Switch (Comutador)

INCIDÊNCIA EM PROVA: MÉDIA

SWITCH / COMUTADOR

Trata-se de um dispositivo de rede que conecta vários dispositivos dentro de uma rede local e gerencia a transmissão de dados de forma eficiente. Diferente de um hub, que simplesmente envia os dados para todos os dispositivos conectados, o switch identifica o destino correto e encaminha os pacotes apenas para o destinatário, reduzindo congestionamentos e melhorando o desempenho da rede.



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. Em outras palavras, quando você conecta um computador ao switch, você não precisa acessar o switch e informá-lo que o computador com endereço X está localizado na porta Y. O switch possui uma tabela dinâmica que automaticamente associa endereços físicos aos computadores conectados.

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

Switch L2 x Switch L3

Por fim, é importante tomar cuidado com a utilização do termo *switch*, visto que pode significar coisas diferentes. A diferença entre um Switch Layer 2 (L2) e um Switch Layer 3 (L3) está na forma como eles operam dentro da rede e na camada do Modelo OSI em que atuam (vamos entender melhor o que são camadas na próxima aula). Vejamos as diferenças:

Saiba mais:

Um Switch L2 é como um porteiro de prédio: ele sabe quem mora no prédio (endereços MAC) e encaminha os visitantes (dados) para os apartamentos corretos dentro do mesmo prédio.

Um Switch L3 é como um carteiro de cidade: ele sabe em qual bairro (rede IP) cada casa está e consegue levar cartas (dados) de um bairro para outro, ou seja, faz roteamento.

CARACTERÍSTICAS	SWITCH L2	SWITCH L3
FUNÇÃO PRINCIPAL	Faz comutação de quadros na camada de enlace (baseado em Endereço MAC) e também faz roteamento de pacotes.	Faz comutação e também roteamento de pacotes na camada de rede (baseado em Endereço IP).
ENDEREÇO UTILIZADO	Endereço MAC.	Endereço IP + Endereço MAC.
DOMÍNIOS	Separa domínios de colisão (um por porta), mas não separa domínios de broadcast.	Separa domínios de colisão e também domínios de broadcast.
COMPLEXIDADE	Simples.	Mais avançado (com funções de roteamento).
EXEMPLOS TÍPICO	Conectar vários computadores de uma mesma rede local.	Conectar diferentes redes LAN em uma empresa, fazendo roteamento interno.



Uma dificuldade muito comum dos alunos é entender a diferença entre Bridge e Switch. Por essa razão, veremos duas analogias que ajudam a explicar essa diferença, mas primeiro vamos analisar as semelhantes: ambos conectam dispositivos em uma rede local; ambos regeneram sinais (não deixam o sinal enfraquecer); ambos filtram dados (não mandam dados para todo mundo sem necessidade); e ambos trabalham manipulando quadros (frames) e utilizam o endereço MAC para decidir para onde enviar os dados.

Agora imagine que temos dois andares de um prédio, sendo que: no primeiro andar, ficam os funcionários do financeiro; e no segundo andar, ficam os funcionários do RH.

Imagine que você está em uma escola com várias salas de aula:

| Bridge: é como um professor que fica na porta entre duas salas, garantindo que só os alunos que precisam ir de uma sala para outra passem por ali. Se alguém da Sala A falar algo que só interessa à Sala A, essa informação não atravessa para a Sala B.

| Switch: é como um professor dentro da sala que conhece cada aluno e suas conversas. Ele sabe exatamente para quem deve repassar uma informação e evita que todos os alunos da sala sejam incomodados com uma mensagem que não diz respeito a eles.

Não entendeu? Então vejamos outra analogia! Imagine agora uma cidade:

| Bridge: é como uma ponte simples que conecta duas cidades. Ela só tem duas entradas e permite que os carros (dados) cruzem de um lado para o outro de forma organizada. A bridge filtra e direciona os dados corretamente, garantindo que apenas os veículos que precisam cruzar de um lado para o outro o façam. Isso ajuda a evitar congestionamentos desnecessários.

| Switch: é mais parecido com um roteador inteligente dentro de uma cidade, que tem várias ruas conectadas e controla a movimentação de veículos dentro da cidade. Ele aprende quais carros pertencem a cada rua e os envia diretamente para o endereço correto, sem precisar passar por todo o caminho de forma indiscriminada.

Em suma, podemos afirmar que:

| Bridge: Conecta dois segmentos de rede e filtra os dados, permitindo uma comunicação eficiente entre partes separadas da rede.

| Switch: Conecta muitos dispositivos, gerencia o tráfego de dados de maneira mais avançada e melhora o desempenho da rede interna.

Essas diferenças fazem com que switches sejam mais utilizados em redes modernas, enquanto bridges ainda têm seu papel em certas situações específicas.

BRIDGE	SWITCH
Foi projetada para conectar dois ou poucos segmentos de rede.	Foi projetado para conectar muitos dispositivos em uma mesma rede.
Costuma ter poucas portas (2, 4, ou 8 portas).	Tem muitas portas (8, 16, 24, 48 portas ou mais).
Funciona de forma mais lenta porque trata o tráfego por software (processamento feito "pensando").	Funciona de forma muito rápida porque trata o tráfego por hardware (processamento feito direto nos chips).
Era muito comum em redes antigas. Hoje caiu bastante em desuso.	É o principal equipamento usado hoje em redes locais (LANs).

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*[7]. A representação de um Switch é apresentada abaixo:

[7] 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.

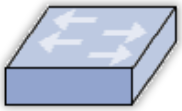


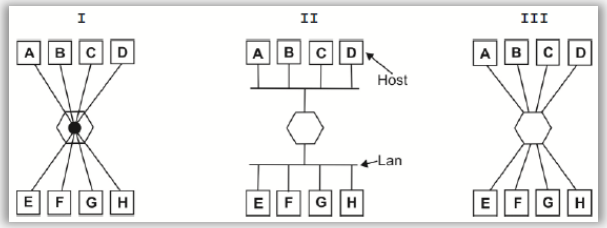
Tabela Resumo

SWITCHES	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede projetado para encaminhar pacotes de dados com base nos Endereços MAC (Media Access Control).
CAMADA OSI	Camada 2 (Enlace).
VANTAGENS	Rápido encaminhamento de pacotes; reduz colisões na rede; segmenta o tráfego da rede em diferentes portas; suporta redes com fio e sem fio; melhora o desempenho da rede.
DESVANTAGENS	Mais caro do que um hub; requer configuração e gerenciamento adequados; pode ter uma curva de aprendizado para administradores de rede.

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

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

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



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

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

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

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

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

Comentários: (a) Errado. Hub atua na camada física (nível 1 do modelo OSI) e apenas replica os sinais para todas as portas, sem segmentar ou comutar dados; (b) Errado. Router (roteador) opera na camada de rede (nível 3 do modelo OSI), direcionando pacotes entre redes diferentes, não na camada de enlace; (c) Errado. Gateway faz a comunicação entre redes que utilizam protocolos diferentes, geralmente operando em todas as camadas do modelo OSI; (d) Correto. Switch é um equipamento de nível 2 (camada de enlace) que realiza a comutação de quadros, segmenta o tráfego e ajuda a reduzir o congestionamento nas redes. (Letra D).

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

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

Comentários: (a) Errado. Gateway conecta redes que utilizam protocolos diferentes e não é o equipamento central usado na topologia em estrela; (b) Correto. O switch é o equipamento utilizado para interligar dispositivos em uma topologia em estrela, funcionando como ponto central de comunicação; (c) Errado. Modem é usado para modulação e demodulação de sinais, permitindo o acesso à internet, não para interligar dispositivos em uma topologia de rede local; (d) Errado. Bridge conecta duas redes locais distintas, não atua como o ponto central típico da topologia em estrela (Letra B).

Router (Roteador)

INCIDÊNCIA EM PROVA: ALTA

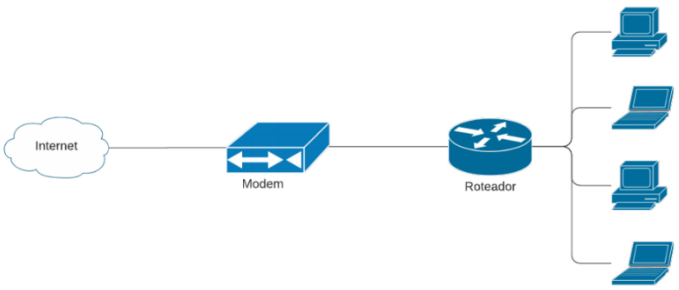
ROTEADOR / ROUTER

Trata-se de um dispositivo de rede que gerencia o tráfego de dados entre diferentes redes, encaminhando pacotes de informações de maneira eficiente. Ele opera na Camada 3 do modelo OSI (Camada de Rede) e é fundamental para conectar dispositivos a redes maiores, como a internet.

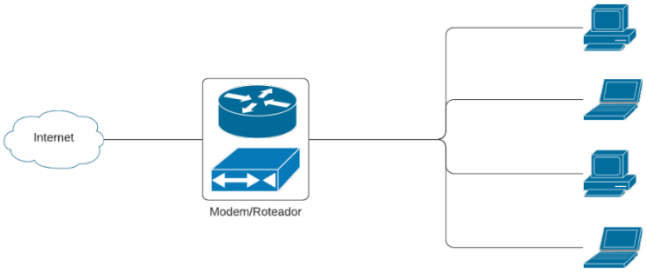


Os roteadores são equipamentos que permitem interligar redes diferentes e escolher a melhor rota para que uma informação chegue ao destino. Esse dispositivo encaminha ou direciona pacotes de dados entre redes de computadores, geralmente funcionando como um elo entre redes diferentes. Hoje em dia, são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

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

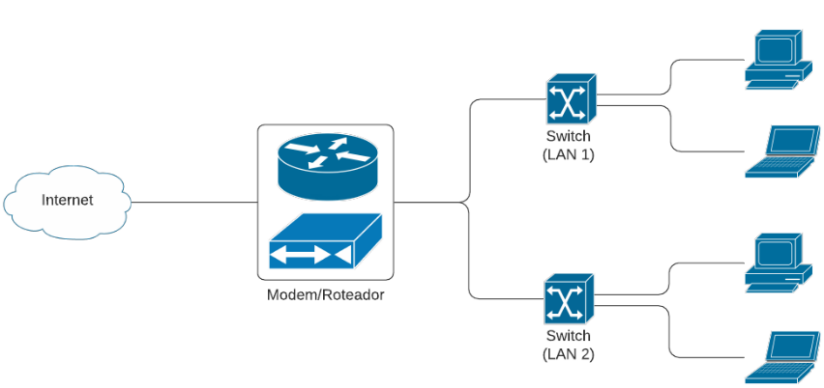


Atualmente, nós estamos na era dos combos, isto é, um único provedor fornece Internet, Telefone e TV a Cabo (Ex: NET/Claro, GVT/Vivo, etc). Nesse caso, um único aparelho condensa as funções de modem e roteador – você provavelmente tem esse aparelho na sua casa! Em geral, um cabo coaxial branco entra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



Primeiro, uma empresa pode ter uma centena de computadores, logo as quatro portas de um roteador não seriam suficientes. Além disso, ela pode ter redes locais diferentes dentro dela por motivos de segurança. É importante 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 operar em outros três modos diferentes: Hotspot, Access Point ou Repetidor de Sinal. Vamos falar sobre cada um deles...

Modos de Operação

No modo Hotspot, o roteador tem o simples objetivo de oferecer acesso à internet. Nesse sentido, 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, entre outros) e outros são pagos (aeroportos e hotéis).



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

O segundo modo de configuração de um roteador wireless é como Access Point. Nesse caso, a ideia é estender os recursos da rede local para a rede sem fio. Quando um roteador wireless é configurado no

modo Hotspot, a ideia era oferecer acesso à internet e, não, aos outros recursos de rede compartilhados. Já quando ele é configurado no modo Access Point, ele oferece – sim – acesso a todos os recursos da rede.

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

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



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.

Tabela Resumo

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

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

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

Comentários: (a) Errado. O modem apenas realiza a modulação e demodulação de sinais para permitir o acesso à internet, não faz roteamento entre redes; (b) Errado. O repetidor apenas amplifica o sinal para estender o alcance da transmissão, sem capacidade de controle de fluxo ou roteamento; (c) Errado. As bridges conectam redes locais (LANs) na camada de enlace, mas não criam rotas nem controlam fluxo entre redes distintas; (d) Errado. O switch atua na camada de enlace, comutando quadros dentro de uma mesma rede local, sem criar rotas entre redes diferentes; (e) Correto. O roteador (router) conecta diferentes redes, controla o fluxo de informações e escolhe rotas mais eficientes para os pacotes de dados (Letra E).

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

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

Comentários: (a) Errado. HDCD é uma tecnologia de áudio, não relacionada a redes de computadores; (b) Errado. Pen drive é um dispositivo de armazenamento portátil, sem função de conexão à Internet; (c) Correto. O roteador é o equipamento responsável por interligar a rede local à Internet, permitindo a comunicação entre os computadores e a rede externa; (d) Errado. Scanner é um periférico de entrada usado para digitalizar documentos, sem função de conexão de rede; (e) Errado. VGA é um padrão de transmissão de vídeo, sem relação com redes de computadores ou acesso à Internet (Letra C).

Modem

INCIDÊNCIA EM PROVA: MÉDIA

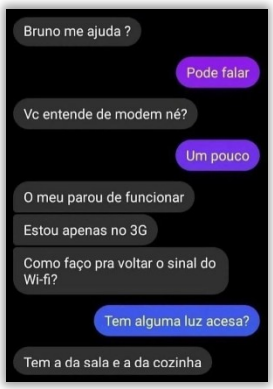
MODEM

Trata-se de um dispositivo de rede que converte sinais digitais em analógicos e vice-versa, permitindo que computadores e outros dispositivos se conectem à internet por meio de linhas telefônicas, cabos ou redes móveis.



Imagine que eu deseje enviar um e-mail. Para tal, é necessário que o e-mail seja transmitido por um meio de comunicação, como fibras ópticas, ondas de rádio ou a infraestrutura de linha telefônica – amplamente disponível. No entanto, computadores utilizam sinais digitais (dígitos binários), enquanto as linhas telefônicas operam com sinais analógicos – é como se um falasse húngaro e o outro aramaico. Como essas "linguagens" são incompatíveis, é necessário um dispositivo que converta os sinais digitais em analógicos e vice-versa para possibilidade a comunicação. *O nome do dispositivo?* Modem!

O modem (abreviação de Modulador-Demodulador) é um dispositivo essencial em redes de computadores que permite a comunicação entre uma rede local (como sua casa ou empresa) e a internet. Sua função básica é converter sinais digitais gerados pelos computadores em sinais analógicos, adequados para serem transmitidos por linhas telefônicas, cabos coaxiais ou redes de fibra óptica, e depois fazer o processo inverso: converter os sinais analógicos recebidos da internet de volta em sinais digitais para que os computadores possam entendê-los.



O seu nome vem justamente dessa dupla função: modular (transformar dados digitais em sinais analógicos para transmissão) e demodular (converter sinais analógicos recebidos em dados digitais para recepção). Além de apenas converter sinais, muitos modems modernos já vêm integrados com outras funções, como roteadores, permitindo que o dispositivo não apenas conecte você à internet, mas também distribua o sinal para vários dispositivos ao mesmo tempo, seja via cabo ou Wi-Fi.

De forma geral, o modem é o "porta de entrada" da sua rede local para o mundo exterior, sendo responsável por conectar a sua casa ou empresa à gigantesca rede global chamada Internet. Vejamos os três tipos de modem:

Modem de Acesso Discado

O Modem de Acesso Discado (também conhecido como modem dial-up) foi muito popular nas décadas de 1990 e início dos anos 2000. Ele utilizava as linhas telefônicas comuns para conectar os computadores à internet, convertendo os sinais digitais em sinais analógicos e vice-versa. O acesso era feito através de uma chamada telefônica, o que significava que, enquanto estivesse conectado à internet, a linha

telefônica ficava ocupada. A velocidade de conexão era muito baixa (em torno de 56 Kbps), e a qualidade do serviço variava bastante, sendo afetada por ruídos e interferências da linha telefônica.

Saiba mais:

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!

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! Ainda bem que ela conseguiu outro transporte e meu sobrinho está hoje com 24 anos e eu estou velho 🙄

Modem ADSL

O Modem ADSL (Asymmetric Digital Subscriber Line) também usa a linha telefônica, mas de forma bem mais eficiente que o dial-up. Com o ADSL, é possível transmitir dados em alta velocidade sem bloquear a linha para ligações telefônicas, já que ele separa a frequência usada para voz da frequência usada para dados. Além disso, o ADSL é "assimétrico", ou seja, permite uma taxa de download maior que a de upload, o que faz sentido para a maioria dos usuários que consomem mais dados do que enviam. Ele foi um dos grandes responsáveis pela popularização da internet banda[8] larga residencial.

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

Cable Modem

O Cable Modem é um tipo de modem que usa a infraestrutura de cabos coaxiais, originalmente criada para transmissão de TV a cabo, para fornecer acesso à internet em alta velocidade. Diferente do ADSL, que depende da distância até a central telefônica, o Cable Modem mantém altas velocidades de conexão mesmo em longas distâncias, embora o desempenho possa variar se muitos usuários do bairro estiverem conectados ao mesmo tempo. Atualmente, muitos serviços de internet a cabo oferecem velocidades muito superiores às antigas tecnologias, e o Cable Modem se tornou uma opção comum em áreas urbanas e suburbanas. *Você tem NET, Claro, etc?*

Essas empresas te oferecem serviços diferentes. Um desses serviços é o combo, que inclui 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.



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!

Enquanto outros dispositivos, como switches e roteadores, trabalham conectando dispositivos ou redes que falam a mesma "língua", o Gateway atua justamente onde as redes são incompatíveis e precisam de uma tradução. Ele não apenas conecta redes, ele também faz a tradução de protocolos para que redes completamente diferentes possam se comunicar.

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

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

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

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

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

Comentários: (a) Correto. O modem é o dispositivo responsável por conectar a linha telefônica e converter sinais digitais em analógicos (e vice-versa) para possibilitar a transmissão de dados; (b) Errado. Barramento é um meio de transmissão de dados entre componentes internos de um computador ou em topologias de rede, não um dispositivo de conexão telefônica; (c) Errado. Switch conecta dispositivos em uma rede local, comutando dados de forma eficiente, mas não utiliza linha telefônica; (d) Errado. Hub é um concentrador que apenas replica sinais entre dispositivos da rede local, sem conexão telefônica; (e) Errado. Transceiver é um transmissor e receptor de sinais, mas não se refere diretamente ao dispositivo de conexão de linha telefônica para dados (Letra A).

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

Comentários: o modem realiza a modulação do sinal digital em analógico para transmissão via linha telefônica e a demodulação do sinal analógico recebido de volta para o formato digital original (Correto).

(CEBRASPE / CET – 2011) O modem:

a) é um tipo de memória semicondutora não volátil.

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

c) é um roteador wireless para redes sem fio.

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

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

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

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

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

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

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

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

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

Comentários: (a) Correto. A tecnologia ADSL oferece conexão permanente à Internet, com custo fixo, permite o uso simultâneo da linha telefônica para chamadas e navegação, e possui velocidade superior às linhas telefônicas tradicionais; (b) Errado. Embora tenha conexão permanente e linha liberada, o custo do ADSL geralmente é fixo, não variável; (c) Errado. No ADSL, a linha telefônica permanece liberada durante a navegação, permitindo simultaneidade de chamadas e acesso; (d) Errado. ADSL oferece conexão permanente e velocidades superiores, diferentemente das linhas tradicionais de conexão discada; (e) Errado. Além de ser permanente, o ADSL também libera a linha telefônica e oferece velocidades maiores que as tradicionais (Letra A).

Padrões de Redes

PADRÕES DE REDES

Trata-se de um conjunto de regras, especificações técnicas e procedimentos estabelecidos por organizações especializadas, com o objetivo de padronizar como dispositivos de diferentes fabricantes se comunicam em uma rede. Esses padrões garantem que equipamentos diversos sejam compatíveis entre si, assegurando interoperabilidade, segurança, eficiência e confiabilidade na transmissão de dados. Eles descrevem aspectos como: formato dos dados, protocolos de comunicação, métodos de acesso ao meio físico, frequências de operação, codificação de sinais, taxas de transmissão, entre outros.

O IEEE (Institute of Electrical and Electronics Engineers) é uma das maiores organizações do mundo dedicadas à evolução da tecnologia, especialmente nas áreas de engenharia elétrica, eletrônica e computação. Seu objetivo é criar normas e padrões que ajudam no desenvolvimento de dispositivos e sistemas, garantindo que funcionem de maneira eficiente e compatível entre si. Dentro do IEEE, existe um grupo chamado Comitê 802, que é responsável pela criação de padrões para redes de computadores.

Esses padrões servem para definir regras sobre como os dispositivos devem se comunicar, garantindo que diferentes marcas e tecnologias funcionem juntas sem problemas. Sem esses padrões, cada empresa poderia criar sua própria tecnologia sem considerar a compatibilidade com outras. Isso resultaria em dificuldades para conectar dispositivos diferentes e tornaria a internet e redes corporativas muito menos eficientes.

Hoje podemos conectar nossos dispositivos à internet sem precisar nos preocupar com compatibilidade, seja em conexões Wi-Fi, cabo Ethernet ou até em sistemas mais avançados usados por grandes empresas.

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

Saiba mais:

Imagine que você está tentando conversar com alguém que fala um idioma completamente diferente do seu. Se não houver uma linguagem comum, será difícil se entenderem, certo? Os padrões de rede funcionam como uma "língua universal" para dispositivos, garantindo que computadores, roteadores, servidores e outros equipamentos consigam se comunicar sem erros.

Os padrões de redes são formalmente testados e regulamentados, ou seja, passam por diversas verificações antes de serem aceitos. Eles definem regras sobre como os dados devem ser

enviados, recebidos e interpretados, tornando possível a interoperabilidade – que significa que equipamentos de diferentes fabricantes podem funcionar juntos sem problemas.

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

PADRÃO IEEE	TECNOLOGIA	TIPO DE REDE	MÍDIA DE TRANSMISSÃO	PRINCIPAIS CARACTERÍSTICAS
IEEE 802.3	Ethernet[9]	LAN	Cabo (Par trançado, Fibra óptica)	Comunicação baseada em pacotes, usa o método CSMA/CD para evitar colisões.
IEEE 802.5	Token Ring	LAN	Cabo (Par Trançado)	Uso de um token para controlar acesso à rede, evitando colisões.
IEEE 802.11	Wi-Fi	WLAN	Radiofrequência	Redes sem fio, vários padrões (a/b/g/n/ac/ax) para diferentes velocidades e alcances.
IEEE 802.15	Bluetooth / WPAN	WPAN	Radiofrequência	Comunicação de curto alcance, usada para dispositivos pessoais como fones e sensores.
IEEE 802.16	WiMAX	WMAN	Radiofrequência	Internet sem fio de longo alcance para áreas metropolitanas.
IEEE 802.20	Mobile Broadband	WWAN	Radiofrequência	Conexão de banda larga móvel voltada para dispositivos em movimento, como veículos.

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

Padrão Ethernet (IEEE 802.3)

INCIDÊNCIA EM PROVA: ALTA

PADRÃO ETHERNET (IEEE 802.3)

O IEEE 802.3 é o padrão que define a tecnologia Ethernet, amplamente utilizada para redes locais (LANs). Desenvolvido pelo IEEE, ele especifica as regras para comunicação via cabos (como par trançado e fibra óptica) e determina como os dispositivos trocam informações de forma eficiente.

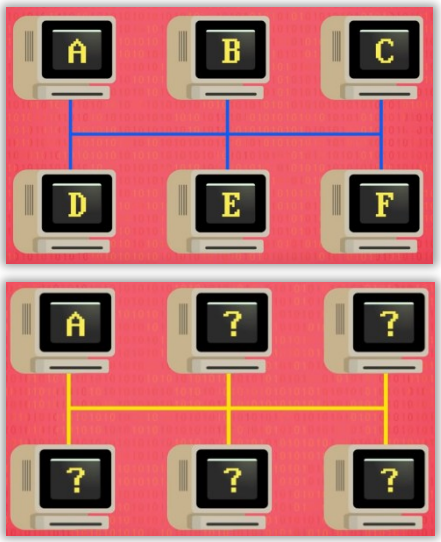
A Ethernet é um conjunto de tecnologias e padrões que estabelece as regras para que dois ou mais computadores possam se comunicar entre si utilizando meios cabeados dentro de uma rede local (LAN). Desenvolvida inicialmente para ambientes corporativos e acadêmicos, a Ethernet tornou-se a tecnologia de rede mais amplamente adotada no mundo devido à sua simplicidade, robustez e baixo custo de implementação. Para compreendermos bem o funcionamento da Ethernet, é importante estudá-la em partes, começando pela topologia física utilizada.

Historicamente, a Ethernet utilizava a topologia em barramento. Nesse modelo, todos os dispositivos da rede eram conectados a um único cabo principal, também chamado de backbone. Esse cabo era o meio físico compartilhado entre todos os nós da rede. Para que a comunicação ocorresse de maneira adequada, ambos os extremos do cabo precisavam ser terminados com resistores chamados terminadores, que evitavam a reflexão dos sinais elétricos no cabo.

Quando um computador conectado à topologia de barramento desejava transmitir dados para outro, ele convertia a informação em sinais elétricos e os enviava para o backbone. Como o cabo era compartilhado por todos os dispositivos, o sinal propagava-se ao longo de todo o cabo, chegando a todos os computadores conectados. Essa forma de transmissão é chamada de broadcast, pois os dados são "anunciados" a todos os dispositivos da rede, independentemente de serem ou não o destinatário da mensagem.

Cada dispositivo, ao receber o sinal, utilizava sua placa de rede (NIC) para analisar o quadro de dados e verificar se o endereço de destino (MAC) correspondia ao seu próprio. Se fosse o destinatário correto, o dispositivo aceitava e processava o quadro; caso contrário, simplesmente o descartava. Essa estratégia, apesar de simples, tinha limitações: como o meio era compartilhado, apenas um dispositivo podia transmitir por vez, e havia o risco de colisões de dados caso dois dispositivos tentassem transmitir simultaneamente. Vamos detalhar isso melhor...

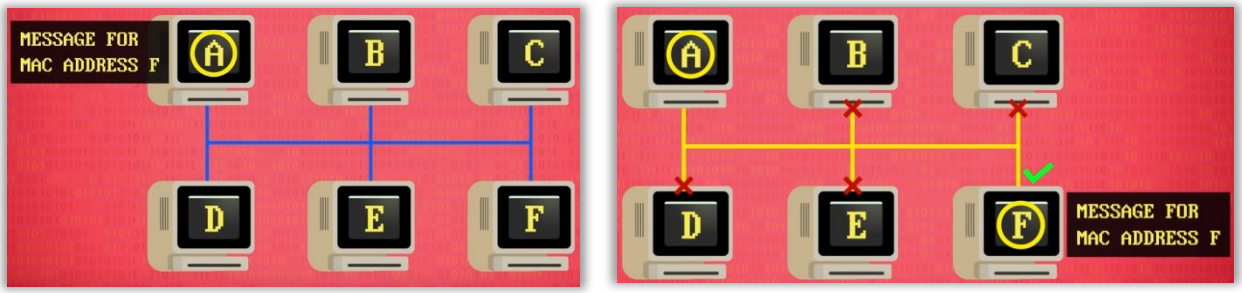




Na imagem acima, o *backbone* será representado em azul para indicar que nenhum sinal está sendo transmitido e em amarelo para indicar onde o sinal está sendo transmitido. Nesse sentido, ao interpretar as imagens apresentadas, podemos concluir que na imagem de cima não está ocorrendo nenhuma transmissão e na imagem de baixo está ocorrendo uma transmissão em broadcast, isto é, todas as máquinas estão recebendo os dados. Apesar disso, apenas o destinatário original poderá processá-los.

E como os computadores vão saber quem é o destinatário original? Para resolver esse problema, a Ethernet requer que cada computador tenha um endereço físico único – também chamado de Endereço MAC (Media Access Control). Esse endereço único é colocado em um prefixo junto com os dados a serem transmitidos. Na imagem anterior, à esquerda, é apresentado o Endereço MAC do meu computador.

Nesse sentido, todos os computadores da rede recebem os dados em broadcast, mas só aqueles que possuem o Endereço MAC de destino contido no prefixo é que podem processá-los. Vejam na imagem 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 – como ele é o destinatário da mensagem, ele a processará e os outros computadores que receberam a mensagem vão ignorá-la. Lembrando que toda placa de rede de um computador possui um Endereço MAC único.



E o que acontece se dois ou mais computadores enviarem dados ao mesmo tempo? Quando dois ou mais computadores enviam dados ao mesmo tempo em uma rede que usa um meio de transmissão compartilhado (como a Ethernet com topologia em barramento ou usando hubs), ocorre uma colisão. A colisão acontece porque os sinais elétricos de ambos os computadores "se misturam" no cabo, resultando em dados corrompidos que não conseguem ser interpretados corretamente pelos destinatários.

Gerenciamento de Colisões

Para lidar com esse problema, a Ethernet utiliza um método chamado 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. O CSMA significa:

- **Carrier Sense (Detecção de Portadora):** antes de transmitir, o computador "escuta" o meio para ver se alguém já está transmitindo.
- **Multiple Access (Acesso Múltiplo):** todos os dispositivos têm o direito de tentar transmitir, mas precisam competir pelo meio.

Quando o tráfego na rede de computadores está baixo, os 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 a famosa colisão. A colisão deixa os dados ininteligíveis, como duas pessoas falando ao telefone ao mesmo tempo – ninguém se entende.

Felizmente, os 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 – o princípio aqui é exatamente o mesmo.

- **Collision Detection (Detecção de Colisão):** se dois dispositivos transmitirem ao mesmo tempo e houver colisão, eles detectam o erro.

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

Comentários: O padrão IEEE 802.3 define as especificações para redes Ethernet e utiliza o método CSMA/CD (Acesso Múltiplo por Escuta de Portadora com Detecção de Colisão) para controlar o acesso ao meio físico. (Correto).

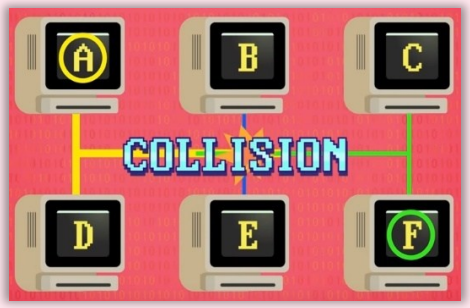
O problema é que o outro computador também vai tentar a mesma estratégia. Além disso, outros computadores da mesma rede podem perceber que o meio de transmissão está vazio e tentar enviar seus dados. *Vocês percebem que isso nos leva a mais e mais colisões?* Pois é, mas a Ethernet possui uma solução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

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

Saiba mais:

Imagine uma Rede Ethernet antiga com cinco computadores conectados a um mesmo cabo. O Computador A quer enviar um arquivo para o Computador F. Antes de transmitir, o Computador A escuta o cabo para ver se está livre. Se estiver, ele começa a enviar o arquivo.

Ao mesmo tempo, o Computador D também quer enviar uma mensagem para o Computador F. O Computador D também escuta o cabo, acha que está livre e começa a transmitir. Resultado: os sinais de A e C colidem no cabo.



Tanto o Computador A quanto o Computador D detectam essa colisão (porque o sinal no cabo ficou bagunçado), param de transmitir e cada um espera um tempo aleatório para tentar de novo. Esse mecanismo evita que eles colidam novamente no próximo envio.

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

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

Lembrem-se de que – para o mundo dos computadores – essa diferença de 0,2 segundos é uma eternidade. Logo, o primeiro computador verá que o meio de transmissão não está sendo utilizado e pode transmitir seus dados. 0,2 segundos depois, o segundo computador verá que o meio de transmissão não está sendo utilizado e poderá transmitir seus dados. Isso resolve uma parte do problema, mas se tivermos centenas de computadores transmitindo dos ao mesmo tempo, o problema permanece.

Pois é, essa é uma das maiores limitações ou desvantagens da topologia em barramento – e uma das razões para essa topologia estar em completo desuso atualmente. Os engenheiros de redes da época tentar uma outra solução: para reduzir o número de colisões e melhorar a eficiência, seria necessário diminuir a quantidade de dispositivos nos meios de transmissão compartilhados. Para tal, uma possibilidade seria utilizar Domínios de Colisão.

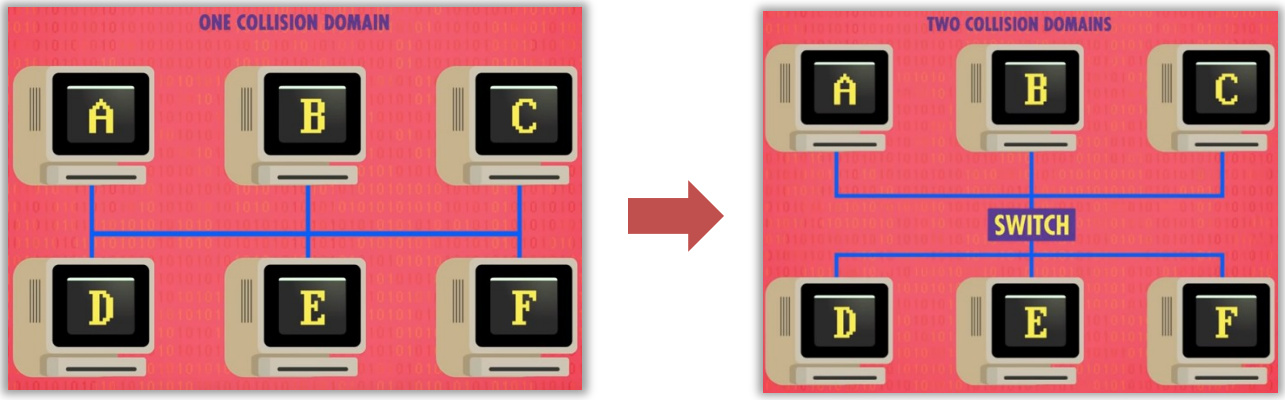
(QUADRIX / CRMV-MS – 2022) Uma das desvantagens das redes ethernet é que todas as estações possuem acesso à rede de maneira diferente, com relação ao tempo de acesso.

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

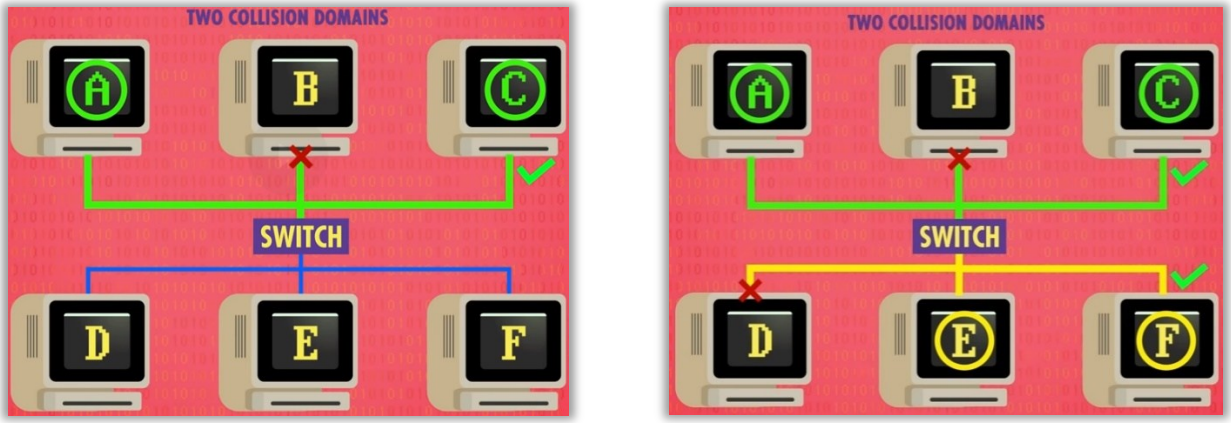
Um domínio de colisão é uma área da rede onde os dispositivos compartilham o mesmo meio físico de transmissão de dados e, portanto, podem ter colisões se tentarem enviar dados simultaneamente. Dentro de um mesmo domínio de colisão, apenas um dispositivo pode transmitir de cada vez porque se dois ou mais transmitirem ao mesmo tempo, ocorre uma colisão. Por essa razão, nós buscamos segmentar a nossa rede em domínios de colisão menores, reduzindo – portanto – a probabilidade de colisões.

Saiba mais:

Imagine um corredor estreito em uma escola, em que somente uma pessoa pode passar de cada vez. Cada aluno representa um dispositivo de rede, como um computador. O corredor é a rede de cabos físicos ou meio compartilhado (Ex: Cabo Ethernet) que permite que os dispositivos se comuniquem entre si. Se duas pessoas tentarem atravessar o corredor ao mesmo tempo, elas batem de frente (colisão). Esse corredor é o domínio de colisão, isto é, enquanto uma pessoa atravessa, as outras precisam esperar.



Na imagem anterior, nós temos seis computadores conectados em um único meio de transmissão compartilhado, logo nós temos um único domínio de colisão. Para reduzir a probabilidade de colisões, nós podemos segmentar a rede em dois domínios de colisão. Para tal, nós podemos utilizar uma topologia em estrela com uso de um switch[10]. Esse dispositivo segmentará nossa rede em duas partes e ficará posicionado entre elas.

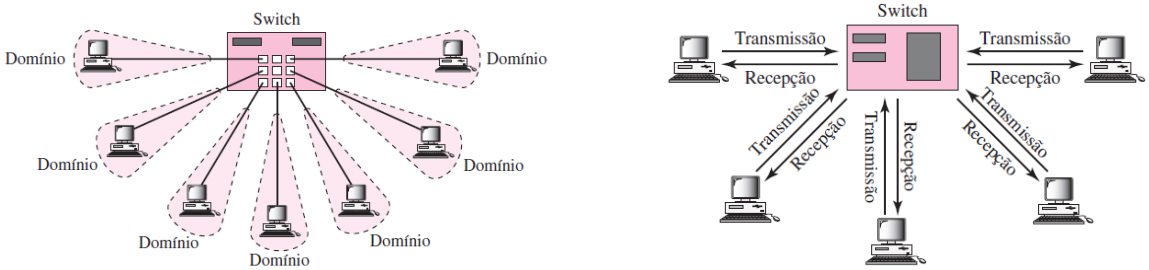


Dessa forma, ele só passará dados para o outro domínio de colisão se a mensagem for destinada a algum computador presente nesse domínio de colisão. Para conseguir fazer esse serviço, ele guarda uma lista de Endereços MAC dos computadores de cada domínio de colisão. Assim, se o Computador A deseja transmitir dados para o Computador C, o switch não encaminhará os dados para o outro domínio de colisão – como mostra a imagem acima à esquerda.

Por outro lado, 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 as duas comunicações estarão 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.

Por didática, nós dividimos a rede em apenas dois domínios de colisão no exemplo. Ocorre que, dessa forma, a probabilidade diminuiu, mas ainda há chance de ocorrer novas colisões. A solução para esse problema é criar um domínio de colisão para cada um dos dispositivos da rede de computadores (conforme é apresentado na imagem seguinte à esquerda).

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



Note que a imagem à esquerda mostra um Switch conectado a vários computadores. Cada linha tracejada representa um domínio de colisão diferente para cada computador. Isso significa que cada porta do switch cria um domínio de colisão separado: se um computador transmitir dados, só ele e o switch compartilham aquele enlace; se outro computador transmitir ao mesmo tempo, não haverá colisão, pois ele está em outro domínio.

Já a imagem à direita também mostra um Switch conectado a vários computadores. No entanto, cada conexão exibe duas setas: uma para transmissão e outra para recepção. Isso indica que a comunicação ocorre em modo full-duplex, isto é, o computador envia dados e recebe dados ao mesmo tempo, sem colisão. Com switches modernos, além de domínios de colisão separados, também é possível fazer transmissão e recepção simultâneas. *O que podemos concluir disso tudo?*

- Antigamente, as Redes Ethernet utilizavam uma topologia em barramento com uso de hubs. Nesse contexto, mesmo com a utilização de algoritmos e protocolos para tentar sanear o problema, havia o risco de colisões caso dois ou mais dispositivos tentassem transmitir dados simultaneamente, dado que o meio de transmissão era compartilhado.

- Atualmente, as Redes Ethernet utilizam uma topologia em estrela com o uso de switches. Nesse contexto, cada computador tem seu próprio caminho até a rede, permitindo comunicações simultâneas e melhorando o desempenho da rede. Além disso, como os switches funcionam em modo full-duplex, o computador é capaz de enviar e receber dados simultaneamente, logo não há mais chance de colisões.

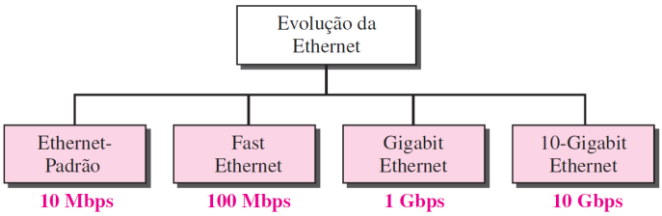
(CONSULPAM / ICTIM-RJ – 2023) Nas redes de computadores, é possível que ocorra uma colisão entre pacotes de dados quando duas ou mais estações pertencentes ao mesmo segmento de rede compartilhado transmitem quadros ao mesmo tempo. Assinale a alternativa que traz CORRETAMENTE um exemplo de domínio de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

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

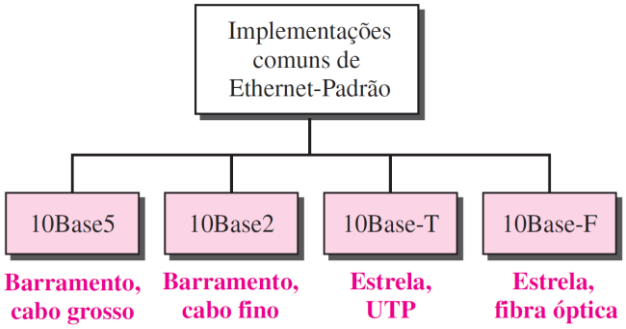
Comentários: (a) Correto. Quando todos os dispositivos estão conectados a um hub Ethernet, eles compartilham o mesmo segmento de rede e fazem parte do mesmo domínio de colisão; (b) Errado. Nesse caso, cada porta do comutador (switch) cria seu próprio domínio de colisão, o que significa que as colisões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

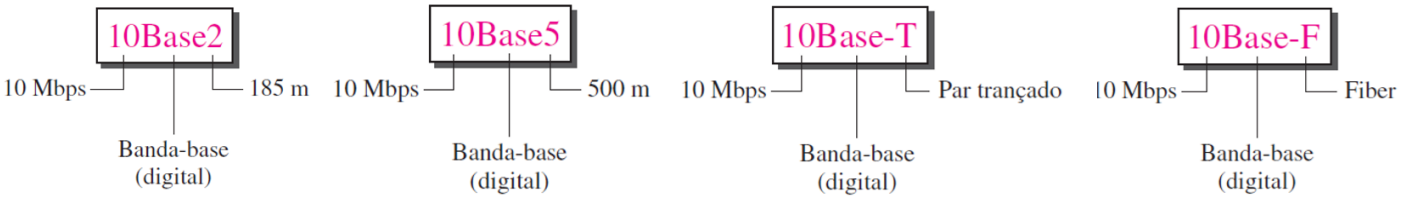
Gerações da Ethernet

Tudo isso que descrevemos até aqui diz respeito ao funcionamento da Ethernet-Padrão, que originalmente operava a 10 Mbps. Com o avanço da tecnologia e a necessidade de maior velocidade de comunicação, surgiram novas gerações da Ethernet: a Fast Ethernet (operando a 100 Mbps), a Gigabit Ethernet (operando a 1 Gbps) e a 10 Gigabit Ethernet (operando a 10 Gbps). Cada nova geração trouxe ganhos significativos de desempenho, mantendo a compatibilidade com os padrões anteriores e solidificando ainda mais a Ethernet como o padrão dominante para redes locais em todo o mundo.



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





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

Saiba mais:

Sabendo que Mega (M) equivale a um milhão (1.000.000) e Giga (G) equivale a um bilhão (1.000.000.000), torna-se mais fácil compreender e memorizar as velocidades associadas às diferentes gerações de tecnologias Ethernet. É importante lembrar também que, no contexto de

redes, 1 Gigabit (1G) corresponde a 1000 Megabits (1000M) – ou seja, 1G = 1000M. Essa conversão simples ajuda a entender as velocidades declaradas nos padrões de rede modernos.

Por exemplo, a tecnologia Gigabit Ethernet opera a uma taxa de 1000 Mbps (megabits por segundo). Isso significa que ela é capaz de transmitir mil milhões de bits por segundo, proporcionando uma velocidade muito superior à da Ethernet tradicional de 10 Mbps ou mesmo da Fast Ethernet de 100 Mbps. A Gigabit Ethernet se tornou padrão em ambientes corporativos e residenciais que demandam maior desempenho, como streaming de vídeos em alta resolução, transferência de grandes volumes de dados e comunicação em redes corporativas robustas.

Já a tecnologia 10 Gigabit Ethernet (10G Ethernet) eleva ainda mais essa capacidade, permitindo transmissões de até 10.000 Mbps – ou seja, dez vezes mais rápida que a Gigabit Ethernet. Com essa velocidade, é possível suportar aplicações de altíssima demanda, como data centers, servidores de alta performance, redes de armazenamento (SANs) e aplicações críticas de negócios que exigem grande largura de banda e baixíssima latência.

Além disso, quando falamos de redes com velocidades ainda maiores, como 100 Gigabit Ethernet (100G Ethernet), estamos falando de uma largura de banda que possibilita transmitir 100 bilhões de bits por segundo (100.000.000.000 bits/segundo). Essa capacidade é utilizada em grandes backbones de internet, interconexão de datacenters, operadoras de telecomunicações e ambientes de computação em nuvem de larga escala. A evolução constante das velocidades Ethernet mostra como a infraestrutura de redes vem se adaptando para atender às exigências cada vez maiores do mundo digital moderno.

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

Comentários: uma largura de banda de 100 Gbps (Gigabits por segundo) permite a transmissão de até 100 bilhões de bits por segundo, e não 100 milhões (Errado).

Vantagens e Desvantagens

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

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

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

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

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

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

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

Comentários: (a) Errado. Fast Ethernet opera a 100 Mbps, Ethernet a 10 Mbps e Gigabit Ethernet a 1000 Mbps, portanto a ordem não corresponde; (b) Correto. Ethernet (tradicional) opera a 10 Mbps, Gigabit Ethernet a 1000 Mbps e Fast Ethernet a 100 Mbps, exatamente na sequência pedida; (c) Errado. Gigabit Ethernet é 1000 Mbps, Ethernet é 10 Mbps, mas Fast Ethernet não corresponde a essa ordem apresentada; (d) Errado. Fast Ethernet é 100 Mbps, Ethernet é 10 Mbps e Gigabit Ethernet é 1000 Mbps; a sequência não corresponde ao que foi solicitado (Letra B).

Padrão Token Ring (IEEE 802.5)

INCIDÊNCIA EM PROVA: MÉDIA

PADRÃO TOKEN RING (IEEE 802.5)

O IEEE 802.5 é um padrão que define a tecnologia Token Ring, utilizada para redes locais (LANs). Esse protocolo foi desenvolvido para controlar o acesso ao meio de comunicação de forma organizada, evitando colisões entre transmissões.

O Padrão Token Ring é outro importante padrão de rede cabeada que, durante muito tempo – especialmente até o início da década de 1990 – foi o principal concorrente da Ethernet no mercado de redes locais. Ele inicialmente oferecia uma taxa de transmissão de 4 Mbps, o que, na época, era bastante competitivo. Mais tarde, surgiram versões de 16 Mbps para tentar acompanhar a evolução da Ethernet. Este padrão apresentava algumas características técnicas bem definidas: comunicação unidirecional (também chamada de simplex), arquitetura ponto-a-ponto entre estações e topologia lógica em anel.

Topologia Lógica e Física

Falando da topologia, é importante entender que, fisicamente, muitas implementações de Token Ring usavam uma disposição semelhante à estrela – com todas as estações ligadas a um concentrador. No entanto, logicamente, a comunicação seguia uma estrutura de anel, ou seja, os dados passavam de uma estação para a seguinte formando um circuito fechado. Isso eliminava um dos problemas que a Ethernet enfrentava na época: as colisões de dados. Na topologia em anel do Token Ring, como o controle de quem pode transmitir é rigidamente organizado, não há risco de colisões.

E por que o nome Token Ring? Isso se deve ao método de controle de acesso que a rede utilizava. Em vez de todos os computadores "brigarem" pelo meio de transmissão, como na antiga Ethernet com CSMA/CD, no Token Ring somente a estação que estiver em posse de um pequeno pacote de controle (chamado *token*) pode transmitir dados. Esse token é um quadro especial que circula continuamente pela rede, passando de uma estação para outra. Quando uma estação precisa transmitir, ela captura o token, anexa os dados que deseja enviar e envia o quadro pela rede. Quando a transmissão termina, o token é liberado para que outra estação possa usá-lo.

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

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

Comentários: (a) Errado. Ethernet normalmente utiliza topologia física em estrela e lógica em barramento, com o método de acesso CSMA/CD, não em anel; (b) Errado. FDDI (Fiber Distributed Data Interface) utiliza topologia em anel, mas é mais voltado para redes de fibra ótica de alta velocidade, e não é o exemplo mais típico para a questão; (c) Correto. Token Ring utiliza uma topologia lógica em anel, onde uma estação deve aguardar a posse do token para poder transmitir, garantindo ordem no acesso ao meio; (d) Errado. Frame Relay é uma tecnologia de comunicação para redes WAN, baseada em comutação de pacotes, não relacionada a topologias em anel; (e) Errado. DSL (Digital Subscriber Line) é uma tecnologia de acesso à Internet via linha telefônica, não um padrão de rede local com topologia em anel (Letra C).

Vantagens e Desvantagens

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

Saiba mais:

Imagine o Token Ring como uma corrida de revezamento. Em uma corrida de revezamento, cada equipe tem um bastão que deve ser passado de um corredor para outro até que todos os corredores da equipe tenham completado uma volta na pista. Nós podemos dizer que um token é basicamente uma espécie de autorização ou envelope que dá ao dispositivo o direito de transmitir dados.

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

Nessa analogia, podemos dizer que: o token é o bastão; o dispositivo que possui o token é o corredor que está com o bastão; os dados que o dispositivo está transmitindo são a mensagem que o corredor está carregando; e os outros dispositivos na rede são basicamente os espectadores da corrida.

(IBADE / Prefeitura de Cujubim-RO – 2018) Um administrador de rede precisa configurar uma rede que funcione na camada física e de enlace dados do modelo OSI, que use um símbolo (que consiste em um sinal de três bytes) que vai circular nos computadores em uma topologia do tipo anel e na qual esses computadores devem aguardar a recepção desse símbolo para transmitir. Essa rede é do tipo:

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

Comentários: (a) Errado. Na topologia em barramento, todos os dispositivos compartilham um único cabo, e o acesso ao meio é controlado pelo método CSMA/CD, não por símbolo circulante; (b) Errado. Ethernet utiliza CSMA/CD para acesso ao meio e geralmente topologias em barramento ou estrela, sem uso de um token; (c) Errado. A topologia física estrela conecta dispositivos a um ponto central, não utilizando token para controle de acesso; (d) Errado. Netware é um sistema operacional de rede (da Novell), não um tipo de topologia ou método específico de acesso; (e) Correto.

Token Ring é uma tecnologia que utiliza uma topologia lógica em anel e um token (símbolo) de controle que circula entre os dispositivos, permitindo a transmissão somente a quem estiver de posse do token (Letra E).

Por fim, vejamos agora uma pequena comparação entre os padrões Ethernet e Token Ring na tabela apresentada a seguir:

CARACTERÍSTICA	PADRÃO TOKEN RING	PADRÃO ETHERNET
TOPOLOGIA	Usa uma topologia em anel, onde os dispositivos são conectados em círculo e os dados são transmitidos em sequência – um dispositivo após o outro.	Usa uma topologia em estrela ou em barramento. Os dispositivos são conectados a um hub ou switch central.
DESEMPENHO	Oferece um desempenho consistente devido à ausência de colisões de dados. A largura de banda é dividida igualmente entre os dispositivos no anel.	Pode ter colisões de dados, especialmente em redes ocupadas. A largura de banda é compartilhada entre todos os dispositivos na rede.
CUSTO	Geralmente é mais caro devido ao hardware específico necessário, como conectores de cabo MAU (*Media Access Unit*).	Geralmente é mais econômico, pois o hardware é amplamente disponível e menos caro.
IMPLEMENTAÇÃO	Requer configuração mais complexa, como a definição de endereços de estação e prioridades de token.	É mais fácil de implementar, com menos requisitos de configuração.
ESCALABILIDADE	Pode ser menos flexível para adicionar ou remover dispositivos sem interromper a rede.	É escalável e permite adicionar dispositivos com facilidade, especialmente em redes comutadas.
POPULARIDADE	Foi popular nas décadas de 1980 e 1990, mas agora é menos comum, pois a Ethernet se tornou dominante.	É a tecnologia de rede mais amplamente usada e suportada, com constante evolução.

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

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

Padrão Wi-Fi (IEEE 802.11)

INCIDÊNCIA EM PROVA: ALTA

PADRÃO WI-FI (IEEE 802.11)

O IEEE 802.11 é o padrão que define as redes Wi-Fi, permitindo a comunicação sem fio entre dispositivos. Criado pelo IEEE, ele especifica como os dispositivos devem se conectar via rádio frequência, garantindo compatibilidade entre diferentes fabricantes.

A comunicação móvel é hoje uma das tendências mais marcantes no mundo da tecnologia, impulsionada pela expectativa de que os usuários estejam conectados à internet o tempo todo, onde quer que estejam. Atualmente, é quase impensável que um hotel, restaurante ou mesmo um transporte público não ofereça algum tipo de acesso online aos seus clientes.

Companhias aéreas já disponibilizam serviços de internet, permitindo que passageiros naveguem enquanto estão a quilômetros de altitude. O aumento da demanda por comunicação móvel despertou grande interesse e investimento no desenvolvimento de tecnologias sem fio (wireless), resultando na criação de padrões para atender às necessidades de mobilidade e conectividade dos usuários.

Para entender melhor essa evolução, pensemos em uma tecnologia sem fio mais antiga e limitada: o controle remoto de televisão. Ele também é um dispositivo wireless, mas funciona por 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 para superar essas limitações que a tecnologia de rádio se tornou dominante para comunicações sem fio. Utilizando antenas e frequências de ondas eletromagnéticas, o rádio permite que os sinais atravessem obstáculos como paredes e portas, embora com alguma perda de qualidade (estou falando de uma parede normal; se for uma parede de um metro de espessura, a perda será grande). Mesmo assim, a comunicação ainda acontece de maneira eficiente.

Diferentemente dos padrões tradicionais, como a Ethernet, que dependem de cabos físicos para a conexão, o Wi-Fi possibilita que os usuários permaneçam conectados enquanto se deslocam dentro de um determinado perímetro – como uma casa, um escritório ou até mesmo uma praça pública. As redes sem fio, baseadas em transmissão por ondas de rádio, trouxeram uma revolução na maneira como interagimos com a tecnologia, permitindo mobilidade, flexibilidade e conveniência. O Wi-Fi define padrões de transmissão e codificação de sinais de rádio para possibilitar a comunicação segura e eficiente entre dispositivos, como notebooks, smartphones, impressoras, entre outros.

Por outro lado, as redes wireless também apresentam algumas limitações. Em geral, as taxas de transmissão em redes sem fio são inferiores às taxas em redes cabeadas. Um exemplo simples é observar que um download feito em um computador conectado diretamente via cabo de rede é, muitas vezes, mais rápido do que o mesmo download realizado via Wi-Fi em um smartphone.

Riscos de Redes Wi-Fi

A segurança em redes wireless exige muito mais atenção: enquanto interceptar dados em uma rede cabeada demanda acesso físico aos cabos, nas redes wireless basta que alguém esteja próximo o suficiente do sinal para tentar capturá-lo. Por isso, proteger sua rede Wi-Fi doméstica com senhas fortes e protocolos de segurança atualizados é fundamental para evitar invasões e roubo de dados.

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

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

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

É importante esclarecer uma dúvida comum: Wireless é um termo genérico que significa qualquer comunicação sem fio, seja via rádio, infravermelho, bluetooth, entre outros. Já Wi-Fi (Wireless Fidelity) é uma marca registrada que representa um conjunto de padrões específicos baseados no IEEE 802.11, voltados para a criação de redes locais sem fio. Logo, todo Wi-Fi é Wireless, mas nem todo Wireless é Wi-Fi. O símbolo do Wi-Fi vem acompanhado do TM (TradeMark), indicando que é uma tecnologia reconhecida comercialmente.

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

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

Protocolos de Segurança

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

PROTOCOLOS DE SEGURANÇA	DESCRIÇÃO
WEP (WIRED EQUIVALENT PRIVACY)	O WEP foi um dos primeiros protocolos de segurança usados em redes Wi-Fi, sendo considerado inseguro (e não recomendado) atualmente. Ele usa uma chave de criptografia compartilhada entre o roteador e os dispositivos para criptografar os dados que são transmitidos, mas tem vulnerabilidades que tornam relativamente fácil para um atacante comprometer a segurança da rede e acessar os dados.
WPA (WI-FI PROTECTED ACCESS)	O WPA foi desenvolvido para substituir o WEP e corrigir suas vulnerabilidades. Ele introduziu melhorias significativas na criptografia e na autenticação, tornando a rede mais segura. No entanto, ao longo do tempo, ele também mostrou algumas vulnerabilidades. Ele usa uma chave de segurança e um método de autenticação mais forte do que o WEP.
WPA2 (WI-FI PROTECTED ACCESS 2)	O WPA2 é uma evolução do WPA e é atualmente um dos protocolos de segurança mais seguros para redes Wi-Fi. Ele utiliza criptografia forte e o padrão IEEE 802.11i para proporcionar uma camada sólida de segurança. O WPA2 oferece autenticação forte e protege os dados transmitidos na rede Wi-Fi de maneira eficaz. É altamente recomendado configurar sua rede Wi-Fi com WPA2 para garantir a segurança.
WPA3 (WI-FI PROTECTED ACCESS 3)	O WPA3 é uma versão mais recente que oferece ainda mais melhorias de segurança, incluindo criptografia mais forte e proteção contra-ataques de força bruta. Dessa forma, ao configurar uma rede Wi-Fi, é aconselhável usar WPA2 ou WPA3, se disponível, para garantir a proteção adequada.

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

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

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

Comentários: (a) Errado. WPA-2 é o padrão mais seguro e mais recente, não foi o primeiro a ser lançado; (b) Errado. WPA é mais seguro que WEP e veio depois; portanto, WPA não foi o primeiro; (c) Correto. O WEP (Wired Equivalent Privacy) foi o primeiro mecanismo de segurança lançado para redes Wi-Fi, mas é frágil e facilmente quebrável. O WPA-2 (Wi-Fi Protected Access 2) é o padrão mais seguro e recomendado atualmente; (d) Errado. WPA não foi o primeiro; foi desenvolvido justamente para substituir o WEP (Letra C).

Modos de Operação

As redes wireless podem operar de duas formas principais: Ad-hoc e Infraestrutura. Cada uma dessas configurações possui características distintas que as tornam mais adequadas para diferentes cenários. A escolha entre elas depende de fatores como topologia da rede, escalabilidade e requisitos de segurança.

A tabela apresentada a seguir oferece uma visão geral das diferenças entre redes wireless ad-hoc[11] e redes wireless de infraestrutura.

CARACTERÍSTICAS	MODO DE OPERAÇÃO AD-HOC	MODO DE OPERAÇÃO INFRAESTRUTURA
DESCRIÇÃO	Comunicação direta entre equipamentos e válida somente naquele momento, conexão temporária, apresentando alcance reduzido (Ex: 5m).	Comunicação que faz uso de equipamento para centralizar fluxo da informação na WLAN (Ex: Access Point ou Hotspot) e permite um alcance maior (Ex: 500m).
TOPOLOGIA DE REDE	Tipo de topologia de malha, onde cada dispositivo se conecta diretamente a outros dispositivos na rede.	Os dispositivos se conectam a um ponto de acesso central, como um roteador, que age como intermediário para encaminhar o tráfego.
CONFIGURAÇÃO DE REDE	Configurada sem a necessidade de um ponto de acesso central. Os dispositivos podem se comunicar diretamente uns com os outros.	Requer um ponto de acesso central (como um roteador) para gerenciar e encaminhar o tráfego na rede.
FLEXIBILIDADE	Mais flexível e útil em cenários onde não há acesso a uma infraestrutura de rede. Pode ser configurada rapidamente para conexões ponto a ponto.	Menos flexível em termos de implantação, pois depende de um ponto de acesso central. Ideal para redes com vários dispositivos em um único local.
ESCALABILIDADE	Menos escalável para grandes redes devido à complexidade de gerenciar muitas conexões ponto a ponto.	Mais escalável para redes maiores, pois o ponto de acesso central gerencia eficientemente as conexões.
SEGURANÇA	Geralmente menos segura, pois não existe um ponto de controle central. As comunicações podem ser vulneráveis a ataques.	Mais segura, pois o ponto de acesso central pode implementar medidas de segurança, como criptografia e autenticação, em nome de todos os dispositivos.
EXEMPLOS DE UTILIZAÇÃO	Redes temporárias de curto prazo, comunicação direta entre dispositivos móveis (por exemplo, compartilhamento de arquivos entre smartphones).	Redes domésticas, redes empresariais, hotspots públicos e ambientes onde múltiplos dispositivos precisam se conectar a uma rede comum.

Saiba mais:

Imagine que você e seus amigos estão em uma roda de conversa, falando diretamente uns com os outros, sem precisar de ninguém organizando a conversa. Cada um pode falar com qualquer outra pessoa da roda, sem intermediários. Isso é o modo ad-hoc: todos os dispositivos se comunicam diretamente entre si, sem precisar de um "chefe" ou "central".

Agora imagine que vocês estão em uma sala, mas só podem conversar passando um bilhete para o professor da sala. Você escreve o bilhete, entrega ao professor, e o professor leva para o colega que você queria atingir. Isso é o modo infraestrutura: todos os dispositivos se comunicam através de um ponto central, que é o responsável por receber e encaminhar as mensagens.

Se você tem um iPhone, conhece um recurso chamado AirDrop; e se você tem um Android, conhece um recurso chamado Nearby Share. Em ambos os casos, é possível estabelecer uma conexão direta entre dois dispositivos para transferência de arquivos (Ex: do seu smartphone para o smartphone de um amigo).

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

Essa conexão é feita sem passar por um roteador, Access Point ou qualquer outro nó central. O funcionamento é descentralizado, pois cada dispositivo se conecta diretamente ao outro. Logo, essa comunicação é um exemplo claro de rede ad-hoc, em que os dispositivos formam uma rede temporária ponto-a-ponto para se comunicar.

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

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

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

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

Quais estão corretas?

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

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

Gerações de Wi-Fi

Assim como ocorreu com a Ethernet, as redes Wi-Fi também passaram por uma série de evoluções tecnológicas para atender às crescentes demandas por velocidade, estabilidade e alcance. Ao longo dos anos, surgiram vários padrões dentro da família IEEE 802.11, cada um trazendo melhorias específicas. Essas tecnologias não são necessariamente a evolução direta uma da outra. Vejamos:

		EVOLUÇÃO DO PADRÃO WI-FI (802.11)[12]

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

PADRÃO	ANO	NOME	FREQUÊNCIA	TAXA MÁXIMA DE TRANSMISSÃO
IEEE 802.11b	1999	-	2.4 Ghz	11 Mbps
IEEE 802.11a	1999	-	5.0 Ghz	54 Mbps
IEEE 802.11g	2003	WI-FI 3	2.4 Ghz	54 Mbps
IEEE 802.11n	2009	WI-FI 4	2.4 / 5.0 Ghz	Até 600 Mbps
IEEE 802.11ac	2014	WI-FI 5	5.0 Ghz	Até 6,9Gbps
IEEE 802.11ax	2019	WI-FI 6	2.4 / 5.0 Ghz	Até 9,6Gbps
IEEE 802.11ax (E)	2021	WI-FI 6E	2.4 / 5.0 / 6.0 Ghz	Até 9,6Gbps
IEEE 802.11be	2025	WI-FI 7	2.4 / 5.0 / 6.0 Ghz	> 40Gbps

O padrão 802.11b entrou no mercado antes do 802.11a e rapidamente se consolidou, pois oferecia um equilíbrio entre alcance e preço acessível, além de operar na banda de 2,4 GHz, que já era amplamente utilizada. Essa faixa de frequência, entretanto, é bastante "poluída", porque outros equipamentos domésticos, como micro-ondas, telefones sem fio, controles de portão eletrônico e dispositivos Bluetooth também operam nela, o que pode gerar interferência nas comunicações Wi-Fi. Apesar disso, o 802.11b permitia uma taxa de transmissão de até 11 Mbps, o que para a época era mais do que suficiente para navegação na web e troca de arquivos simples.

Pouco tempo depois, foi lançado o padrão 802.11g, que surgiu como uma evolução natural do 802.11b. Ele manteve compatibilidade retroativa com o padrão anterior, ou seja, dispositivos 802.11g podiam se comunicar com dispositivos 802.11b. O grande diferencial do 802.11g foi a aumento de velocidade, permitindo taxas de transmissão de até 54 Mbps, ainda operando na banda de 2,4 GHz. Isso atendeu melhor a demandas mais exigentes, como transmissões de vídeos e compartilhamento de arquivos.

Em seguida, veio o padrão 802.11n, que trouxe grandes avanços. Ele utilizada múltiplas antenas para enviar e receber mais dados simultaneamente, melhorando muito a performance. Além disso, o 802.11n introduziu a capacidade de operar tanto em 2,4 GHz quanto em 5 GHz, característica chamada de Dual Band. Essa inovação foi crucial porque, como vimos, a banda de 2,4 GHz sofre muita interferência de outros aparelhos domésticos. O uso da banda de 5 GHz oferece canais mais limpos, menos congestionados, permitindo maiores velocidades e menor latência – ideal para aplicações como videoconferência, jogos online e streaming em alta definição.

Mais recentemente, surgiu o padrão 802.11ac, que opera exclusivamente na banda de 5 GHz. Ele é voltado para tráfego de altíssima velocidade, suportando taxas superiores a 1 Gbps. O 802.11ac também trabalha com tecnologias de múltiplas antenas e múltiplos usuários, que permite que o roteador atenda vários dispositivos simultaneamente com alta eficiência, melhorando ainda mais a performance em ambientes com muitos dispositivos conectados, como casas inteligentes ou escritórios modernos.

O 802.11ax (Wi-Fi 6), lançado em 2019, e sua extensão Wi-Fi 6E em 2021, vieram com foco em eficiência. Usando técnicas como OFDMA e MU-MIMO aprimorado, ele consegue lidar melhor com redes densas, como estádios e escritórios cheios de dispositivos. A introdução da banda de 6 GHz no Wi-Fi 6E abriu espaço para conexões mais estáveis e rápidas, reduzindo interferências.

Por fim, o 802.11be (Wi-Fi 7), previsto para 2025, promete velocidades superiores a 40 Gbps. Ele traz canais ainda mais largos (até 320 MHz), suporte a MLO (Multi-Link Operation, que combina várias bandas ao mesmo tempo) e otimizações para realidade aumentada, streaming em 8K e jogos na nuvem. Esse padrão deve marcar uma nova era de redes sem fio, praticamente equivalentes às conexões cabeadas de alta velocidade.

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

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

Comentários: (a) Errado. O padrão 802.11ac está relacionado ao Wi-Fi 5, oferecendo altas velocidades, mas não é o Wi-Fi 6; (b) Correto. O padrão 802.11ax é o que define a tecnologia Wi-Fi 6, trazendo melhorias de desempenho, eficiência e capacidade, principalmente em ambientes com muitos dispositivos conectados; (c) Errado. O padrão 802.11b é uma versão antiga do Wi-Fi, com velocidades mais baixas (até 11 Mbps); (d) Errado. O padrão 802.11g sucedeu o 802.11b e melhorou a velocidade para 54 Mbps, mas também é anterior ao Wi-Fi 6; (e) Errado. O padrão 802.11n trouxe melhorias como o MIMO para o Wi-Fi 4, mas não é relacionado ao Wi-Fi 6 (Letra B).

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

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

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

Vantagens e Desvantagens

Assim, vemos que os padrões de Wi-Fi evoluíram progressivamente para oferecer mais velocidade, melhor estabilidade, maior alcance e menos interferências. Vejamos as vantagens e desvantagens:

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

Padrão Bluetooth (IEEE 802.15)

INCIDÊNCIA EM PROVA: BAIXA

PADRÃO BLUETOOTH (IEEE 802.15)

O IEEE 802.15 é o padrão que define redes WPAN, permitindo a comunicação sem fio entre dispositivos de curto alcance. Ele foi desenvolvido pelo IEEE para conectar dispositivos sem a necessidade de cabos, geralmente em distâncias inferiores a 10 metros.



O Padrão Bluetooth foi desenvolvido com o objetivo de permitir a integração de equipamentos periféricos de forma prática e sem a necessidade de cabos. Ele é amplamente utilizado em redes WPAN (Wireless Personal Area Network), isto é, redes de área pessoal sem fio, caracterizadas por serem de baixo custo, curto alcance, baixas taxas de transmissão e alta praticidade. Essa tecnologia opera na frequência de 2,4 GHz, a mesma utilizada por muitos outros dispositivos domésticos, e estabelece conexões de forma ad-hoc, ou seja, sem a necessidade de infraestrutura centralizada como roteadores ou access points.

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

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

Comentários: (a) Errado. O padrão 802.3 refere-se às redes Ethernet (com fio), não a redes pessoais sem fio; (b) Errado. O padrão 802.11 é utilizado para redes locais sem fio (Wi-Fi), e não para conexões pessoais via Bluetooth; (c) Correto. O padrão 802.15 é voltado para redes pessoais sem fio (WPANs), como as que utilizam a tecnologia Bluetooth; (d) Errado. O padrão 802.16 é utilizado para redes metropolitanas sem fio (WiMAX), não para redes pessoais (Letra C).

Redes Piconet

O funcionamento do Bluetooth se organiza em torno de uma unidade básica chamada piconet (ou picorrede), que é essencialmente um pequeno grupo de dispositivos Bluetooth que compartilham um canal comum de rádio-frequência. Dentro dela, adota-se uma topologia em estrela, com um único dispositivo mestre no centro da comunicação. Esse dispositivo mestre – também chamado de master ou primário – é o responsável por coordenar todo o tráfego de dados dentro da piconet, controlando a comunicação com até sete dispositivos escravos[13] (ou slave, também chamados de secundários).

(QUADRIX / Prefeitura de Jataí-GO – 2019) Assinale a alternativa que apresenta a unidade básica do sistema bluetooth, a qual consiste em um nó mestre e até em sete nós escravos ativos, situados dentro de uma distância de dez metros.

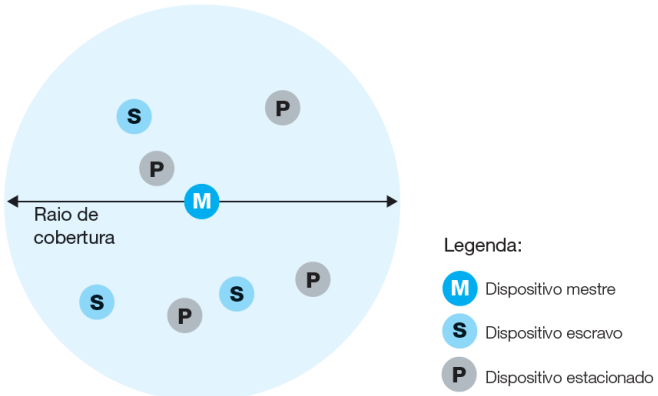
a) scatternet
b) ad-hoc
c) clock interno

[13] 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.

d) piconet
e) page

Comentários: (a) Errado. Scatternet é uma rede formada pela interligação de várias piconets, não a unidade básica individual; (b) Errado. Ad-hoc refere-se a redes formadas sem infraestrutura fixa, conceito diferente da estrutura Bluetooth básica; (c) Errado. Clock interno é relacionado à sincronização de dispositivos Bluetooth, mas não é a unidade estrutural da rede; (d) Correto. A piconet é a unidade básica no sistema Bluetooth, formada por um nó mestre e até sete nós escravos ativos em um raio típico de até dez metros; (e) Errado. Page é uma fase do processo de estabelecimento de conexão Bluetooth, e não a unidade de rede (Letra D).

Embora qualquer dispositivo Bluetooth possa desempenhar o papel de mestre ou escravo, em uma mesma piconet só pode haver um único mestre ativo. Além dos dispositivos escravos, a piconet pode conter até 255 dispositivos estacionados (parked). Um dispositivo estacionado permanece sincronizado com o mestre, mas não participa ativamente da comunicação até ser ativado. Se for necessário ativar um dispositivo estacionado, o mestre deve mover algum escravo ativo para o estado estacionado, respeitando o limite de oito dispositivos ativos ao mesmo tempo na piconet (1 mestre + 7 escravos).



Essa dinâmica é importante para gerenciar melhor os dispositivos conectados, já que os recursos de uma piconet são limitados. Logo, a piconet é composta por dispositivos ativos (transmitindo e recebendo dados) e dispositivos estacionados (em estado de espera, sincronizados, mas inativos). Essa organização permite que uma piconet gerencie dinamicamente quais dispositivos estão ativos conforme a necessidade da comunicação.

Saiba mais:

Imagine que você queira ouvir música no seu smartphone sem usar fios. Para isso, você ativa o Bluetooth e conecta sua caixa de som sem fio. Agora, seu celular se torna o mestre e a caixa de som é o escravo, pois o telefone controla o fluxo de áudio e a caixa de som apenas reproduz o som que recebe.

Agora, pense que você quer adicionar mais dispositivos Bluetooth à rede, como outro smartphone para compartilhar o controle da playlist ou um fone de ouvido para ouvir a mesma música. Assim, uma pequena rede de dispositivos se forma, com o smartphone coordenando a transmissão de áudio e os outros dispositivos recebendo os dados.

Essa pequena rede Bluetooth criada entre dispositivos próximos é chamada de piconet – um grupo temporário de dispositivos conectados, onde um atua como mestre e os outros como escravos, seguindo as instruções para transmissão de dados. Vejamos as principais características de uma piconet:

- Dispositivos conectam-se temporariamente e podem sair da rede quando quiserem;
- Um dispositivo assume o controle (mestre) e os outros seguem suas instruções (escravos);
- Comunicação sem infraestrutura, funcionando sem precisar de roteadores ou Wi-Fi;

Em outras palavras, toda vez que você conecta seu celular a uma caixa de som Bluetooth, um fone de ouvido sem fio ou outro dispositivo móvel, você está – na prática – criando uma piconet.

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

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

Comentários: (a) Correto. Em uma rede Piconet, um dispositivo mestre pode se conectar simultaneamente a até 7 dispositivos escravos ativos, limitando o número de conexões simultâneas; (b) Errado. 15 não é o número máximo de dispositivos escravos ativos em uma Piconet; (c) Errado. 127 refere-se ao número de dispositivos que podem ser reconhecidos em algumas redes, mas não ao número de dispositivos ativos simultâneos em uma Piconet; (d) Errado. 255 não corresponde ao limite de dispositivos ativos na Piconet; trata-se de um valor relacionado a endereçamentos em outros contextos de redes; (e) Errado. 1023 é um valor associado a capacidades de endereçamento em outros padrões, e não ao Bluetooth (Letra A).

Redes Scatternet

Existe ainda uma estrutura mais complexa: a scatternet. Ela se forma quando duas ou mais piconets se interconectam. Isso ocorre quando um mesmo dispositivo atua como escravo em uma piconet e mestre em outra piconet. Por exemplo, imagine duas piconets separadas: a da esquerda com seu mestre e seus escravos, e a da direita com outro mestre e seus escravos. Se houver um dispositivo que participe das duas – sendo escravo em uma e mestre na outra –, temos a formação de uma scatternet. Esse mecanismo permite expandir a cobertura e a capacidade de redes bluetooth, conectando múltiplos grupos de dispositivos de forma flexível e inteligente.

Saiba mais:

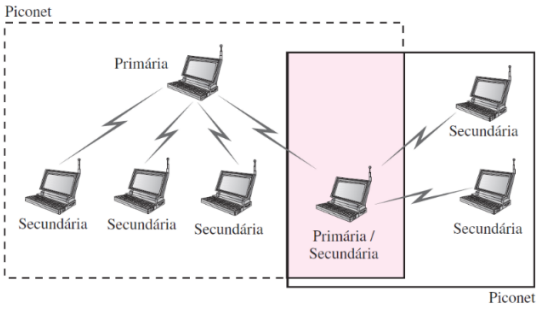
Imagine que cada grupo de amigos na festa tem um líder (mestre), que organiza a conversa e mantém o grupo unido. Mas, diferente de uma piconet, alguns amigos estão conversando com mais de um grupo ao mesmo tempo. Eles atuam como intermediários, conectando diferentes redes, permitindo que as informações fluam entre vários círculos de conversa. Agora, pense em dispositivos Bluetooth como:

- Um smartphone conectado a um fone de ouvido Bluetooth e a uma caixa de som ao mesmo tempo.
- Um notebook conectado a um mouse Bluetooth e também a um celular, permitindo comunicação entre dispositivos diferentes.

Na prática, esses dispositivos formam múltiplas piconets interligadas, criando uma scatternet – uma rede maior e mais flexível, em que alguns dispositivos desempenham o papel de "pontes" entre grupos. Vejamos as principais características de uma scatternet:

- Interconexão entre múltiplas piconets;
- Dispositivos podem pertencer a mais de um grupo ao mesmo tempo;
- Maior capacidade de comunicação entre dispositivos distantes;
- Mais possibilidades de troca de informações;

Se a piconet é uma conversa de um único grupo, a scatternet é uma grande rede de conexões interligadas, onde os dados podem se mover entre diferentes piconets sem a necessidade de uma infraestrutura fixa.



Vamos entender a imagem anterior! À esquerda, temos uma piconet: um dispositivo está atuando como Primária (Mestre) e três outros dispositivos estão atuando como Secundários (Escravos). Esta piconet é uma rede Bluetooth típica com topologia em estrela, onde o mestre coordena a comunicação entre os escravos. À direita, temos outra piconet: o dispositivo central dessa segunda piconet é rotulado como Primária/Secundária. Isso significa que esse dispositivo está simultaneamente participando das duas piconets: ele é escravo na primeira piconet (à esquerda) e ele é mestre na segunda piconet (à direita). Na segunda piconet, ele coordena a comunicação com dois dispositivos Secundários (escravos).

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

Vamos resumir todos 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

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

Comentários: embora o Bluetooth permita a conexão sem fios entre dispositivos, seu alcance é limitado, variando entre cerca de 10 a 100 metros, dependendo da classe do dispositivo (Errado).

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

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

Vantagens e Desvantagens

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

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

Padrão WiMAX (IEEE 802.16)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

PADRÃO WIMAX (IEEE 802.16)

O IEEE 802.16 é o padrão que define a tecnologia WiMAX, voltada para redes de banda larga sem fio de longo alcance. Criado pelo IEEE, ele permite a transmissão de dados em áreas metropolitanas e rurais, funcionando como uma alternativa ao acesso tradicional via cabos.

O Padrão WiMAX (Worldwide Interoperability for Microwave Access) é um conjunto de especificações que define um padrão de comunicação sem fio de alta velocidade para redes de ampla cobertura, especialmente para Redes Metropolitanas sem fio (WMAN). Esse padrão foi desenvolvido sob a responsabilidade do IEEE, no projeto 802.16, e posteriormente impulsionado por um consórcio de empresas, que se dedicou a garantir a interoperabilidade entre equipamentos de diferentes fabricantes, promovendo assim a padronização e a ampla adoção da tecnologia.

Principais Características

Uma das principais características do WiMAX é seu alcance extenso. Em condições ideais, um ponto de acesso WiMAX pode fornecer conectividade para dispositivos situados a até cerca de 40 quilômetros de distância. Na prática, isso torna a tecnologia altamente recomendável para levar internet banda larga a empresas e residências localizadas em áreas rurais, remotas ou suburbanas, onde a implementação de soluções tradicionais como ADSL (linha telefônica) ou HFC (cabo coaxial) se torna inviável ou economicamente desvantajosa devido à dificuldade de infraestrutura.

Saiba mais:

Imagine uma cidade do interior onde não existem cabos de fibra óptica instalados. Em vez de cavar ruas para passar fios, a operadora instala torres WiMAX estrategicamente nas áreas urbanas e rurais. Essas torres enviam o sinal de internet para antenas instaladas nas casas, escolas e empresas – sem a necessidade de cabo. Dessa forma, mesmo quem mora a 30 km da cidade pode ter internet banda larga confiável usando apenas uma antena externa.

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

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

Comentários: (a) Correto. A tecnologia WiMAX (Worldwide Interoperability for Microwave Access) utiliza o padrão IEEE 802.16, voltado para redes metropolitanas sem fio de alta velocidade; (b) Errado. O padrão 802.15 é usado para redes pessoais sem fio, como o Bluetooth; (c) Errado. O padrão 802.11 é usado para redes locais sem fio (Wi-Fi); (d) Errado. O padrão 802.5 é relacionado ao Token Ring, uma tecnologia de rede em anel; (e) Errado. O padrão 802.3 refere-se às redes Ethernet (com fio) (Letra A).

O WiMAX opera em faixas de frequência licenciadas, como 2,5 GHz, 3,5 GHz e 10,5 GHz. Isso significa que, para oferecer serviços baseados nessa tecnologia, as empresas precisam solicitar e obter uma

concessão da ANATEL (Agência Nacional de Telecomunicações), órgão regulador das telecomunicações no Brasil. Essa obrigatoriedade visa organizar o espectro radioelétrico, evitando interferências entre diferentes operadores e assegurando a qualidade dos serviços prestados.

Outro aspecto técnico importante do WiMAX é a questão da modulação do sinal. A potência do sinal percebida na estação-base (o equipamento que emite e gerencia o sinal para os clientes) pode variar bastante de acordo com fatores como distância, obstáculos físicos, condições climáticas e interferências externas. Para adaptar-se a essas variações e garantir uma comunicação confiável, o WiMAX utiliza três esquemas principais de modulação (QPSK, QAM-16 e QAM-64).

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

Comentários: o WiMAX é um padrão de comunicação sem fio baseado no IEEE 802.16, desenvolvido para redes metropolitanas (MAN), oferecendo cobertura de longa distância e altas taxas de transmissão (Correto).

Esses esquemas de modulação permitem que o WiMAX adapte dinamicamente a qualidade e a velocidade da comunicação conforme as condições do ambiente, garantindo uma experiência mais estável e eficiente para os usuários. Assim, o WiMAX surgiu como uma alternativa poderosa e flexível para expandir o acesso à internet em locais onde as tecnologias tradicionais não conseguem chegar facilmente, impulsionando a inclusão digital em áreas anteriormente desassistidas.

Saiba mais:

Imagine o WiMAX como se fosse uma torre de rádio que transmite internet em vez de música. Se o Wi-Fi é como um pequeno rádio caseiro, que cobre sua casa ou seu escritório, o WiMAX é como uma grande estação de rádio, que cobre toda uma cidade ou um bairro inteiro. Enquanto o Wi-Fi alcança poucos metros, o WiMAX consegue espalhar o sinal a dezenas de quilômetros de distância, levando internet para onde seria muito difícil passar cabos.

Vantagens e Desvantagens

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

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

Oferece QoS para garantir que diferentes tipos de tráfego, como voz e vídeo, tenham desempenho adequado na rede.	A gestão eficaz do espectro é necessária para evitar interferências e garantir o desempenho da rede.

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

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

Comentários: (a) Errado. ADSL é uma tecnologia de acesso à Internet via linha telefônica, não uma rede MAN sem fio; (b) Errado. GSM (Global System for Mobile Communications) é um padrão de comunicação móvel para telefonia celular, não específico para MANs sem fio; (c) Errado. LTE (Long Term Evolution) é uma tecnologia de rede móvel para alta velocidade de dados, usada em redes celulares, não diretamente ligada a MANs sem fio; (d) Correto. WiMAX é a implementação prática do padrão IEEE 802.16, utilizado para redes metropolitanas sem fio (WMAN), oferecendo cobertura ampla e alta velocidade; (e) Errado. HSPA (High Speed Packet Access) é uma tecnologia de rede móvel para transmissão de dados, associada a redes celulares 3G (Letra D).

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

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

Comentários: (a) Correto. WiMAX é uma tecnologia de rede sem fio de longa distância, voltada para redes metropolitanas (MAN), com alcance de vários quilômetros; (b) Errado. ZigBee é usado para comunicação de curta distância em aplicações de baixo consumo de energia, como automação residencial; (c) Errado. IEEE 802.11a é uma versão do Wi-Fi para redes locais (LAN), com alcance limitado; (d) Errado. IEEE 802.11g também é uma versão de Wi-Fi para redes locais (LAN), não para longa distância; (e) Errado. Bluetooth é utilizado para comunicação pessoal de curtíssimo alcance, entre dispositivos próximos (Letra A).

INTERNET

Conceitos Básicos

INCIDÊNCIA EM PROVA: MÉDIA

A Internet pode ser definida como um vasto conjunto de redes de computadores distintas que utilizam padrões comuns de comunicação e oferecem determinados serviços integrados aos usuários. Embora o acesso à internet seja amplamente difundido na atualidade, é importante compreender como essa rede mundial teve sua origem. Para isso, é necessário revisitar brevemente a sua história e os motivos que impulsionaram o seu desenvolvimento.

O contexto inicial remonta ao final da década de 1950, durante o auge da Guerra Fria entre Estados Unidos e União Soviética. Um dos grandes temores da época era a possibilidade de uma guerra nuclear, especialmente após o uso de bombas atômicas na Segunda Guerra Mundial. Nesse cenário, o Departamento de Defesa dos Estados Unidos percebeu a necessidade de desenvolver uma rede de controle e comando que fosse resiliente a ataques, incluindo uma eventual guerra nuclear.

Naquele período, a rede pública de telefonia já estava difundida entre a população e era amplamente utilizada para comunicações militares. No entanto, essa infraestrutura era considerada vulnerável, uma vez que se assemelhava a uma arquitetura de cliente/servidor, com centrais telefônicas espalhadas pelo país. Dessa forma, bastaria a destruição de algumas dessas centrais para comprometer toda a comunicação nacional.

O marco de 1957 acelerou as preocupações norte-americanas: a União Soviética lançou o Sputnik, o primeiro satélite artificial do mundo. Em resposta, o presidente Dwight Eisenhower criou a ARPA (Advanced Research Projects Agency), uma agência de pesquisa destinada a impulsionar o avanço tecnológico militar. A ARPA não possuía cientistas ou laboratórios próprios, mas era responsável por financiar projetos de pesquisa em universidades e empresas que apresentassem propostas inovadoras, mantendo os Estados Unidos tecnologicamente à frente dos soviéticos.

Nos primeiros anos, a ARPA investiu em diversos projetos. Contudo, sob a direção de Larry Roberts, a agência voltou sua atenção para a antiga ideia de criação de uma rede de comunicação descentralizada. Em 1969, com a adesão de algumas universidades de ponta, iniciou-se a construção dessa rede, que ficou conhecida como ARPANET – nome derivado de seu financiamento pela ARPA. A ARPANET representaria o embrião do que viria a ser, décadas depois, a Internet moderna.

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

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

Comentários: (a) Errado. Extranet é uma extensão da intranet de uma organização para usuários externos autorizados, sem relação com a origem da Internet; (b) Correto. A Internet surgiu a partir da ARPANET (Advanced Research Projects Agency Network), desenvolvida nos tempos da Guerra Fria para garantir a comunicação militar e acadêmica; (c) Errado. OnlyNet não tem relação histórica com a criação da Internet; (d) Errado. Unix é um sistema operacional criado na mesma época, mas não é o nome da rede que deu origem à Internet (Letra B).

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

Comutação por Circuito

Antigamente havia um emprego que hoje em dia não existe mais: telefonista! 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[14]. Essa comunicação funcionava por meio da comutação por circuito.



Observem na imagem anterior que existem 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.

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.

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

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. Isso que nós acabamos de descrever se chama comutação por circuito. *E 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.

Ainda hoje a telefonia funciona com comutação de circuitos, mas não precisamos mais de operadores porque os circuitos são capazes de se mover automaticamente em vez de manualmente. Ocorre que a comutação por circuito é completamente inviável na internet, porque há muito desperdício de recursos. 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. Vejamos as principais características da comutação por circuitos:

COMUTAÇÃO POR CIRCUITOS	DESCRIÇÃO
CONEXÃO	Estabelecida antes da transmissão de dados.
EXCLUSIVIDADE	Circuito dedicado durante toda a comunicação.
EFICIÊNCIA	Pode ser baixa, pois a linha fica ocupada mesmo em silêncio.
LATÊNCIA	Baixa, ideal para voz em tempo real.
ROBUSTEZ	Menos flexível, difícil de redirecionar em caso de falha.
EXEMPLOS	Ligações telefônicas tradicionais.

A comutação por circuito foi essencial para as comunicações tradicionais, oferecendo conexões contínuas e estáveis. Vejamos alguns exemplos:

- **Telefonia Fixa Tradicional:** ao ligar para alguém, uma linha é reservada apenas para aquela chamada.

- **Centrais Telefônicas Antigas:** telefonistas conectavam manualmente os cabos para estabelecer a comunicação.
- **Sistemas Antigos de Transmissão de Dados:** antes da internet, redes privadas de grandes empresas também usavam comutação por circuito para interligar filiais.

Saiba mais:

Imagine que você quer viajar de uma cidade para outra. Ao invés de usar o transporte público (ônibus ou metrô compartilhado), você aluga uma estrada só para você durante a viagem. Mesmo que você pare para comer ou descansar, a estrada continua reservada exclusivamente para seu uso, sem permitir que outras pessoas a utilizem até você chegar ao seu destino. É assim que a comutação por circuito funciona: uma "estrada" dedicada para sua comunicação, ocupada do início ao fim, mesmo nos momentos de silêncio.

Comutação por Pacotes

A comutação por pacotes surgiu na década de 1960 como uma alternativa mais eficiente à comutação por circuito, muito usada na telefonia da época. O conceito foi desenvolvido como uma forma de comunicação mais resiliente, principalmente diante de preocupações com ataques nucleares no contexto da Guerra Fria. A ideia foi utilizada no projeto da ARPANET, permitindo que dados fossem enviados em pequenas unidades chamadas pacotes, e que pudessem seguir caminhos variados até o destino.

Cada pacote contém parte dos dados originais e informações de controle (como endereço de origem e destino). Os pacotes são enviados individualmente, podendo seguir rotas diferentes pela rede, dependendo da disponibilidade e eficiência dos caminhos no momento. Ao chegar ao destino, eles são reorganizados na ordem correta para reconstruir a mensagem original. Vejamos as principais características da comutação por pacotes:

COMUTAÇÃO POR PACOTES	DESCRIÇÃO
DIVISÃO DE DADOS	Dados são divididos em pacotes menores.
ROTAS	Cada pacote pode seguir um caminho diferente.
EFICIÊNCIA	Uso mais dinâmico dos recursos da rede.
REORGANIZAÇÃO	Pacotes são remontados na ordem correta no destino.
ROBUSTEZ	Se um caminho falhar, os pacotes são redirecionados.
UTILIZAÇÃO	Base das redes modernas (Internet, VPNs, etc).

Essa técnica aumenta a eficiência, resiliência e economia de recursos da rede, pois os caminhos são usados sob demanda e não ficam ocupados durante toda a comunicação. Vejamos alguns exemplos:

- **Internet:** ao enviar um e-mail, fazer uma videochamada ou acessar um site, os dados são enviados em pacotes pela rede.
- **WhatsApp:** uma mensagem de áudio pode ser quebrada em pacotes e enviada por caminhos diferentes até chegar completa no celular do destinatário.
- **Transmissão de Vídeos:** plataformas como YouTube e Netflix utilizam pacotes para transmitir vídeos sob demanda.

Saiba mais:

Imagine que você quer enviar um livro para um amigo. Em vez de enviar o livro inteiro em uma única caixa (como na comutação por circuito), você desmonta o livro página por página e envia cada página por correios diferentes. Cada carta (página) pode seguir rotas distintas: algumas podem passar por aviões, outras por caminhões, e outras por barcos. Quando todas as páginas chegam, seu amigo reorganiza tudo na ordem certa para formar novamente o livro.

Se uma carta se perder ou atrasar, você só precisa reenviar aquela página – e não o livro inteiro. Aliás, pode ser que as dez primeiras páginas cheguem por último e as últimas dez páginas cheguem primeiro. 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).

VANTAGENS DA COMUTAÇÃO POR PACOTES	DESVANTAGENS DA COMUTAÇÃO POR PACOTES
Maior eficiência no uso da rede	Pode haver atraso (latência) na entrega dos pacotes
Melhor tolerância a falhas e congestionamentos	Pacotes podem chegar fora de ordem
Reduz custos de transmissão	Necessita de protocolos de controle para reorganizar pacotes
Suporte para múltiplos tipos de comunicação simultânea	Exige maior capacidade de processamento dos dispositivos

As primeiras redes utilizam tecnologias que funcionavam apenas com equipamentos semelhantes. 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, o que começou a ocasionar 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.

Era preciso criar um conjunto de regras (protocolos) que permitisse que computadores diferentes se entendessem, ou seja, que fossem capazes de se comunicar mesmo sendo de marcas, modelos e sistemas operacionais distintos. Para resolver isso, foi criada uma solução revolucionária: um modelo de comunicação baseado na comutação por pacotes que seria independente do tipo de máquina chamado TCP/IP, que foi oficializado como padrão da ARPANET em 1983.

Arquitetura TCP/IP

O TCP/IP (Transmission Control Protocol/Internet Protocol) é um conjunto de protocolos de comunicação que permite que dispositivos diferentes em uma rede troquem informações entre si, especialmente na Internet. Ele define como os dados devem ser divididos em pacotes, endereçados, transmitidos, roteados e recebidos no destino correto. Podemos dizer basicamente que o IP cuida de "para onde os dados vão" (endereçamento) e o TCP cuida de "como os dados chegam" (controle de erros, reenvio, reordenação).

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 esse conjunto de protocolos e que consiste em milhões de equipamentos, com alcance local ou global, e que está ligada a uma grande

variedade de tecnologias de rede é também conhecida popularmente como: Internet. Veremos mais detalhes sobre o TCP/IP na próxima aula.

Serviços de Internet

A Internet é uma gigantesca rede mundial que interconecta milhões de dispositivos (computadores, smartphones, servidores, sensores, etc) utilizando protocolos de comunicação padronizados. Ela funciona como uma "rede de redes", permitindo que dispositivos de diferentes lugares do mundo se comuniquem entre si para trocar informações, acessar serviços, compartilhar arquivos e utilizar aplicações online. Dentro os principais serviços, os mais conhecidos são:

SERVIÇOS DA INTERNET	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. 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, entre outros).

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

Comentários: o correio eletrônico (e-mail) foi um dos primeiros serviços desenvolvidos na ARPANET, ainda nos anos 1970, e rapidamente se tornou uma das aplicações mais populares da rede (Correto).

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

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

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

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

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

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

Comentários: (a) Errado. "Wide Worring Web" está incorreto – o correto é "World Wide Web" – e "sequenciamento de arquivos" não é um serviço básico da Internet; (b) Correto. World Wide Web, correio eletrônico, transferência de arquivos (FTP), login remoto (Telnet ou SSH) e desktop remoto são serviços amplamente populares e difundidos na Internet; (c) Errado. "Comutação de servidores" e "debugging remoto" não estão entre os serviços mais populares da Internet; (d) Errado. "World Wide Wedge" e "transferência de endereços" são termos incorretos ou inexistentes nesse contexto; (e) Errado. "Wood Wide Weed" e "controle eletrônico" são termos errados ou fora do escopo da Internet (Letra B).

Web (WWW)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Web é uma contração do termo World Wide Web (WWW). Muito cuidado: alguns alunos confundem Internet com Web. A Internet é o conjunto de redes, cabos, satélites, roteadores, protocolos (como TCP/IP) que permitem a conexão e a troca de dados entre dispositivos no mundo inteiro; já a Web é o conjunto de páginas, sites e conteúdos acessados por navegadores (Ex: Google Chrome, Mozilla Firefox e Microsoft Edge) utilizando o protocolo HTTP/HTTPS. Vejamos alguns exemplos:



Saiba mais:

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

Agora, pense na web como lojas, casas, escritórios e pontos de interesse que você encontra ao longo das estradas da Internet. Cada loja ou local representa um site da web, e você pode visitá-los para obter informações, fazer compras, se divertir, entre outros. Os sites da web são destinos ao longo da estrada.

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

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

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

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

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

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

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

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

Comentários: (a) Errado. A internet não é apenas uma coleção de documentos, e a WWW também não é simplesmente um serviço de acesso a um computador; (b) Errado. WWW não é um serviço de acesso exclusivo ao Google; é uma plataforma de acesso a conteúdos em toda a internet; (c) Correto. A internet é uma vasta rede mundial de computadores interconectados, enquanto a World Wide Web (WWW) é apenas um dos muitos serviços que operam sobre essa rede, permitindo acesso a páginas e documentos; (d) Errado. A definição é incompleta e confusa em relação ao que a WWW realmente representa; (e) Errado. A internet não é apenas uma coleção de endereços eletrônicos, e a WWW não é restrita a acesso ao Google (Letra C).

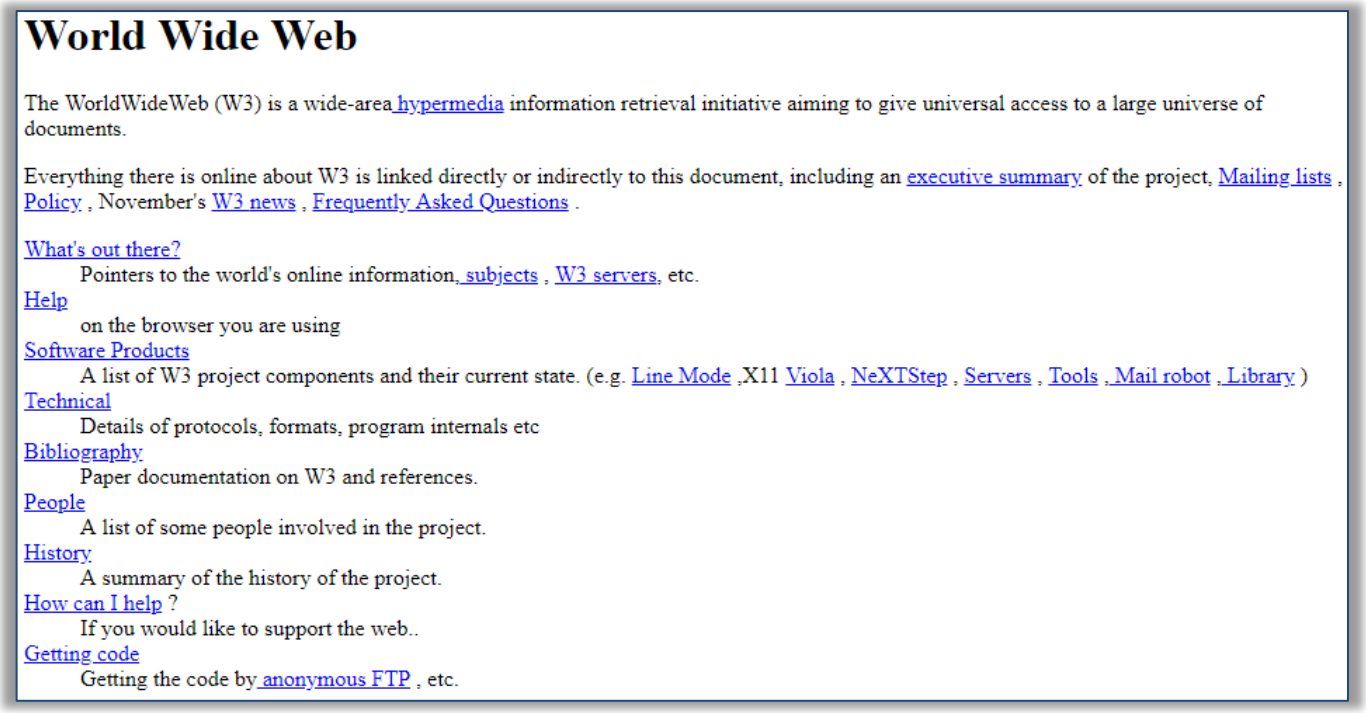
Agora vamos falar um pouco sobre as gerações da web (note que elas não se excluem, elas se sobrepõem). Vamos vê-las em detalhes...

Web 0.0

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

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

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



World Wide Web

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

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

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

Web 1.0

A Web 1.0 é considerada a primeira geração da internet pública, surgida no início dos anos 1990, especialmente após a criação da Web. Essa fase da web era caracterizada por páginas estáticas, ou seja, documentos que eram criados em HTML e exibidos para os usuários de forma fixa, sem interação significativa. Os sites funcionavam basicamente como cartões de visita online: forneciam informações para leitura, mas não havia possibilidade real de interação entre o visitante e o conteúdo. As páginas eram simples, muitas vezes com texto, imagens básicas e poucos recursos gráficos.

Saiba mais:

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

Nesse cenário, as empresas e instituições são como os curadores da biblioteca, selecionando e disponibilizando informações para os visitantes. Os visitantes podem encontrar informações úteis, mas não têm a capacidade de contribuir com seu próprio conteúdo ou interagir com outros

visitantes. A Web 1.0 é semelhante a essa biblioteca digital, onde o conteúdo é fornecido para leitura, mas não há recursos avançados de interatividade, colaboração ou personalização.

Na Web 1.0, os usuários eram meros consumidores de conteúdo, sem participação ativa no processo de criação ou modificação das informações disponíveis. As empresas, universidades e governos eram os principais produtores de conteúdo e a comunicação era unidirecional: do site para o usuário. Ferramentas de busca ainda eram bastante limitadas, e para encontrar informações era comum usar diretórios organizados manualmente. Apesar dessas limitações, essa fase foi fundamental para democratizar o acesso à informação e pavimentar o caminho para as evoluções que viriam a seguir, como a Web 2.0, que introduziu a participação ativa dos usuários.

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

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

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

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

Web 2.0

A Web 2.0 marca uma nova era na internet, surgida no início dos anos 2000, caracterizada principalmente pela interatividade e pela colaboração dos usuários. Diferente da Web 1.0, em que as páginas eram estáticas e o usuário apenas consumia conteúdo, na Web 2.0 os próprios usuários passaram a criar, compartilhar e modificar informações em tempo real. Redes sociais, blogs, fóruns, wikis (como a Wikipédia) e plataformas de vídeos (como o YouTube) são exemplos claros dessa nova fase, onde a comunicação passou a ser bidirecional: usuários não apenas recebem conteúdo, mas também produzem conteúdo para outros usuários.

Saiba mais:

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

Da mesma forma, a Web 2.0 permitiu que os usuários não apenas consumissem informações, mas também as criassem, compartilhassem e colaborassem em um ambiente online, tornando a internet mais interativa e participativa. É uma mudança de uma web estática e informativa para

uma web dinâmica e social, onde os usuários desempenham um papel ativo na criação e compartilhamento de conteúdo.

O conceito de Web 2.0 trouxe também a popularização de aplicações dinâmicas baseadas em tecnologias como JavaScript, AJAX e XML, permitindo a criação de sites muito mais interativos e responsivos. Nesse novo ambiente, surgiram grandes plataformas de redes sociais, comércio eletrônico e serviços baseados em nuvem, transformando a internet em um espaço de intensa colaboração, personalização e interação social. Em resumo, a Web 2.0 transformou a internet em uma plataforma participativa, onde o usuário é tanto consumidor quanto produtor de informação.

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

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

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

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

Comentários: os princípios da Web 2.0, na verdade, têm o efeito oposto: eles incentivam ativamente o público a participar da construção e da customização de serviços e mensagens. A Web 2.0 é caracterizada pela colaboração, interatividade e participação dos usuários na criação e compartilhamento de conteúdo online, o que a torna uma abordagem muito mais aberta e envolvente em comparação com a Web 1.0 (Errado).

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

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

Comentários: (a) Errado. Wiki é uma ferramenta colaborativa específica (como a Wikipédia), mas não representa o conceito geral descrito na questão; (b) Errado. Tags são marcadores usados para classificar conteúdos na internet, não o conceito amplo de inteligência coletiva; (c) Correto. A Web 2.0 descreve a evolução da internet para plataformas que permitem maior interação e colaboração dos usuários, gerando inteligência coletiva com conteúdos criados e compartilhados; (d) Errado. A Web 1.0 refere-se à internet inicial, onde os usuários eram apenas consumidores de conteúdo, sem participação ativa na criação (Letra C).

Web 3.0

A Web 3.0, também chamada de Web Semântica, é considerada a próxima evolução da internet, buscando tornar a interação online mais inteligente, autônoma e personalizada. Diferente da Web 2.0, que enfatizou a colaboração e a criação de conteúdo pelos usuários, a Web 3.0 propõe que as máquinas entendam e processem as informações de maneira mais próxima à interpretação humana. Isso é possível graças ao uso de tecnologias como inteligência artificial (IA), blockchain, big data e machine learning, que permitem que os sistemas sejam capazes de interpretar o contexto e o significado dos dados, e não apenas lê-los de forma literal.

Saiba mais:

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

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

Na prática, a Web 3.0 busca oferecer experiências mais personalizadas, respostas mais relevantes e serviços mais descentralizados. Aplicações como assistentes virtuais (ex: Siri, Alexa), contratos inteligentes baseados em blockchain e o conceito de identidade digital descentralizada são exemplos de iniciativas alinhadas à visão da Web 3.0. Além disso, na Web 3.0, o controle dos dados tende a ser devolvido aos usuários, promovendo mais privacidade, autonomia e segurança em um ambiente mais transparente e descentralizado.

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

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

a) pragmática
b) semântica
c) semiótica
d) ubíqua

Comentários: (a) Errado. Web pragmática não é um termo reconhecido para identificar a evolução da internet; (b) Correto. A Web 3.0 é conhecida como a Web Semântica, pois visa dar significado aos dados, permitindo que as máquinas compreendam e processem as informações de forma mais inteligente; (c) Errado. Semiótica é o estudo dos signos e símbolos, não o conceito usado para definir a Web 3.0; (d) Errado. Embora a Web 3.0 também tenha características de ubiquidade (acesso em qualquer lugar), o termo mais adequado e consagrado é Web Semântica (Letra B).

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

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

Camadas da Web

INCIDÊNCIA EM PROVA: MÉDIA

A web pode ser dividida em camadas que refletem diferentes níveis de acessibilidade, funcionalidade e infraestrutura. Vejamos:

Surface Web

SURFACE WEB

Trata-se da parte da internet que está indexada por mecanismos de busca tradicionais, tais como: Google, Bing e Yahoo. A Surface Web é a parte da web que pode ser acessada livremente por qualquer pessoa usando navegadores comuns. Trata-se da camada visível da web, composta por páginas públicas, que não exigem autenticação especial (como login e senha) para serem acessadas.

A Surface Web (também chamada de Web Navegável) é a parte da internet que é visível, acessível publicamente e indexada por motores de busca tradicionais (Ex: Google, Bing e Yahoo) sem a necessidade de autenticação (Ex: Login e Senha). Esses buscadores possuem rastreadores, isto é, pequenos programas que percorrem a internet e adicionam páginas ao índice de pesquisa, tornando-as acessíveis a qualquer pessoa que faça uma busca.

Saiba mais:

Imagine a internet como um enorme iceberg: a ponta do iceberg, aquela parte visível acima do mar, é a Surface Web. É onde estão os sites que qualquer pessoa pode ver facilmente. Já a parte submersa, escondida debaixo da água, é a Deep Web (e uma parte menor ainda dela é a Dark Web). Assim como a maior parte do iceberg está oculta, a maior parte da internet também não é visível para buscadores comuns.

Por exemplo, se você pesquisar sobre um site como o Estratégia, ele aparecerá nos resultados porque foi indexado pelo buscador. Isso significa que ele está na Surface Web, a parte da web navegável e aberta, que qualquer pessoa pode acessar diretamente por um navegador tradicional sem precisar de login, senha, permissão ou navegador especial – ela é como uma vitrine pública. Apesar de parecer enorme, a Surface Web representa apenas cerca de 4% de toda a internet. A maior parte da informação online (como arquivos protegidos, áreas internas de sites, bases acadêmicas e bancos de dados) está na Deep Web.

SURFACE WEB	DESCRIÇÃO
ACESSIBILIDADE	Facilmente acessível por meio de mecanismos de busca e navegadores padrão de forma direta e sem login obrigatório.
CONTEÚDO PÚBLICO	Compreende sites, páginas e conteúdo que são acessíveis ao público em geral.
INDEXAÇÃO	Os motores de busca, como Google e Bing, indexam e exibem o conteúdo da Surface Web em resultados de pesquisa.
INFORMAÇÕES VISÍVEIS	Notícias, blogs, lojas online, fóruns públicos e outros tipos de sites podem ser encontrados na Surface Web.
SEM RESTRIÇÕES SIGNIFICATIVAS	Os usuários podem navegar e acessar conteúdo sem a necessidade de credenciais ou permissões especiais.
EXEMPLOS	Páginas de notícias, blogs, lojas online e outros sites acessíveis ao público em geral.

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

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

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

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

Deep Web

DEEP WEB

Trata-se da parte da internet que não está indexada pelos mecanismos de busca convencionais, como Google, Bing ou Yahoo. São páginas e conteúdos que não aparecem nas pesquisas e que geralmente exigem alguma forma de autenticação, como login e senha, para serem acessados. Apesar da fama, a Deep Web é composta, em sua maioria, por conteúdos legítimos, como bancos de dados acadêmicos, sistemas internos de empresas, contas bancárias online, e arquivos privados.

A Deep Web é a parte da internet que não é indexada pelos motores de busca comuns como Google, Bing ou Yahoo. Trata-se do conjunto de páginas, bases de dados e conteúdos online que não aparecem em pesquisas tradicionais, mas que ainda são legítimos e utilizados no dia a dia. Ela é invisível para todos aqueles que não tenham autorização para acessá-la. Muito cuidado: é comum vermos manchetes em jornais associando crimes ou atividades ilegais à Deep Web, sendo que o correto seria Dark Web.



"O uso da internet foi muito publicizado. Todo mundo tem acesso. Não adianta o pai proibir o filho de acessar a internet ou de ter um celular, porque ele vai fazer isso com um coleguinha", diz.

O tema da audiência pública surgiu após o massacre ocorrido na escola estadual Professor Raul Brasil, em Suzano (SP). No dia 13 de março deste ano, dois atiradores mataram alunos e funcionários da escola. A polícia afirmou que um dos atiradores havia pesquisado na deep web, durante o planejamento do crime (que levou mais de um ano), sobre atentados semelhantes em escolas dos Estados Unidos.

Saiba mais:

Voltando à analogia do iceberg: se a Surface Web é a ponta visível do iceberg acima da água, a Deep Web é a parte submersa, bem maior e que abriga documentos, registros e informações

protegidas. Assim como a maior parte do iceberg está debaixo d'água e é invisível sem mergulhar, a maior parte da internet real está escondida na Deep Web, longe dos motores de busca.

A maior parte da Deep Web é composta por conteúdos normais, que estão protegidos porque exigem autenticação (login e senha) ou simplesmente porque não foram "rastreados" por buscadores. Você acessa a Deep Web toda vez que acessa seu e-mail pessoal, toda vez que você entra na área de aluno do Estratégia, toda vez que você acessa sua conta corrente no banco, toda vez que você acessa a intranet da empresa em que trabalha – não há nada de ilegal!

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

A Deep Web é, portanto, necessária e legítima para proteger informações privadas e confidenciais. No entanto, não é uma 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.

Dark Web

DARK WEB

Trata-se da parte da Deep Web que só pode ser acessada por meio de softwares e redes específicas, como o Navegador Tor. Ela foi projetada para garantir anonimato completo tanto para quem acessa quanto para quem hospeda os conteúdos. A Dark Web é conhecida por abrigar conteúdos e serviços que não estão disponíveis na internet comum, podendo incluir desde fóruns privados e troca de informações sigilosas até atividades ilegais, como comércio de drogas, armas e dados roubados.

A Dark Web é uma parte da Deep Web que foi deliberadamente oculta e só pode ser acessada usando softwares, configurações ou autorizações específicas, como o navegador Tor. Ela é projetada para oferecer anonimato total tanto para quem hospeda os sites quanto para quem os acessa. Enquanto a Deep Web é simplesmente "não indexada", a Dark Web é propositalmente escondida para proteger identidades e garantir anonimato.

Ela foi criada originalmente para permitir a comunicação segura e privada (por exemplo, para jornalistas em regimes autoritários ou para proteger dissidentes políticos). No entanto, como o anonimato é garantido, a Dark Web também acabou atraindo atividades ilegais, como venda de drogas e armas, hackers oferecendo serviços ilícitos, comércio de documentos falsificados, fóruns criminosos, entre outros.

Saiba mais:

Usando a analogia do iceberg, a Surface Web é a ponta visível; Deep Web é o que está submerso e protegido; e a Dark Web é como cavernas escondidas dentro do iceberg – lugares difíceis de encontrar, que exigem equipamento especial para serem acessados. É como se existisse um mundo subterrâneo secreto, acessível só para quem sabe exatamente como chegar lá.

Apesar disso, nem tudo na Dark Web é criminoso. Existem usos legítimos: ativistas, jornalistas e cidadãos vivendo sob censura utilizam a Dark Web para se comunicar livremente e com segurança. A Dark Web não é indexada por mecanismos de busca comuns e nem possuem um endereço comum[15], 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. A Dark Web não é acessível por meio de navegadores tradicionais 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 web.



Na China, o Google e muitos de seus serviços, como Gmail, Google Maps e YouTube, são bloqueados pelo Grande Firewall do governo. No entanto, algumas pessoas conseguem contornar essa restrição usando VPNs (Redes Privadas Virtuais) e a Deep Web. Na China, existem fóruns e plataformas específicas na Dark Web (Ex: Deepmix e o Chang'na) que são populares entre os usuários chineses. Esses espaços permitem discussões anônimas e até transações, muitas vezes envolvendo criptomoedas

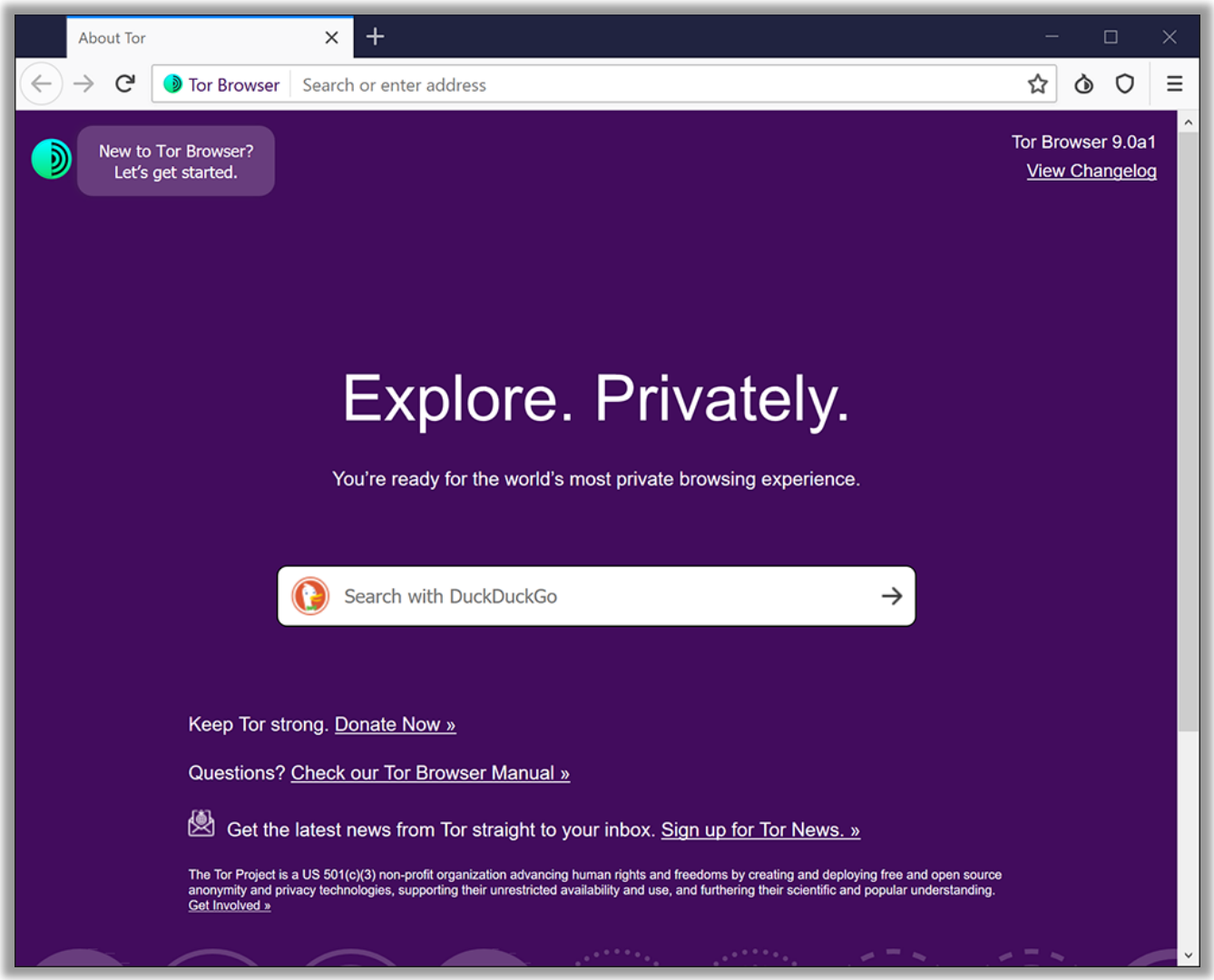
(CEBRASPE / ABIN – 2018) O uso de domínios web de final .on e de roteadores em formato de proxy são características da dark web.

Comentários: na dark web, os domínios geralmente terminam com **.onion**, e o acesso é feito por meio de redes específicas, como a rede Tor, que utiliza roteamento em camadas (e não simplesmente proxies comuns) para garantir o anonimato (Errado).

O Navegador Tor direciona as requisições de uma página através de uma rota que passa por uma série de servidores proxy da Rede Tor operados por milhares de voluntários em todo o mundo, tornando o endereço IP não identificável e não rastreável[16]. 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.

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

[16] 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.



Como exige-se todo esse processo, a Rede Tor é considerada lenta. Não ache que utilizá-la será igual quando você navega em seus sites normais por meio de navegadores tradicionais. Vejam só:

- Cada pacote de dados passa por pelo menos três servidores em diferentes locais do mundo antes de chegar ao destino final e cada salto adiciona atraso (latência);

- Cada vez que seu dado passa por um servidor, ele é descriptografado parcialmente e depois reenviado. Esse processo de criptografar e descriptografar camadas adiciona um tempo de processamento;

- Os servidores da rede são, em sua maioria, mantidos por voluntários, logo nem sempre eles têm banda larga muito rápida ou servidores potentes;

- O número de pessoas querendo usar a rede é muito maior do que a quantidade de nós disponíveis. Por conta de tudo isso, há grande lentidão na rede.

DARK WEB	DESCRIÇÃO
ACESSIBILIDADE	A Dark Web é acessada por meio de redes criptografadas, como o Tor (The Onion Router), que requerem software especial para acesso.
CONTEÚDO ILEGAL E OBSCURO	Inclui sites que hospedam atividades ilegais, como tráfico de drogas, armas, venda de informações roubadas e outros conteúdos obscuros.

ANONIMATO É VALORIZADO	Os usuários da Dark Web muitas vezes valorizam o anonimato, pois os serviços são frequentemente anônimos e transações são criptografadas.
RISCOS À SEGURANÇA	A Dark Web é um ambiente de alto risco, onde os usuários podem ser vítimas de fraudes e ataques cibernéticos.
NÍVEIS DE ANONIMATO	Diferentemente da Deep Web, a Dark Web oferece um nível mais profundo de anonimato e criptografia, tornando difícil rastrear usuários.

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

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

Quando utilizamos o Navegador Tor, é possível acessar tanto páginas da Surface Web quanto páginas exclusivas da Dark Web. Ao acessar uma página da Surface Web, o seu anonimato é preservado, ou seja, ninguém consegue identificar quem está fazendo o acesso (porque não sabem o seu IP verdadeiro), mas é possível identificar qual site você está acessando. Isso acontece porque o endereço do site ainda é público e visível, mesmo que o usuário permaneça oculto por trás da Rede Tor.

Por outro lado, existem sites que só existem dentro da Dark Web, e são acessíveis exclusivamente através da Rede Tor. Esses sites possuem endereços especiais terminados em .onion, que não são encontrados nos navegadores comuns nem nos mecanismos de busca convencionais. Nesses casos, o anonimato é total: não é possível saber quem está acessando; não é possível saber qual site está sendo acessado; não é possível saber quando o acesso ocorreu; e não é possível saber quais dados estão sendo transmitidos.

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

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

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

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

Verifica-se que está(ão) correta(s):

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

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



Em evidência após ataques, dark web é refúgio para quem foge de autoridades

Zona sombria da rede reúne criminosos e fóruns acerca de temas como racismo

Getúlio Vargas especialista em tecnologia e inovação. Ele explica que a *deep web* não é necessariamente ilegal ou "ruim": "Militantes de direitos humanos na China, por exemplo, a utilizam para conseguir se comunicar com o mundo exterior. Os grupos que organizaram a Primavera Árabe também dependiam dela". No entanto, Igreja afirma que existe uma "camada" da *deep web* conhecida como *dark net* (ou rede escura), onde ocorre a venda de armas, drogas, pedofilia e o planejamento de crimes.

Dentro da Dark Web, existem fóruns, marketplaces e comunidades clandestinas onde são encontrados conteúdos extremamente ilícitos e perturbadores, como: tráfico de drogas e armas; contratação de matadores de aluguel; planejamento de atentados terroristas; compartilhamento de fotos/vídeos de pornografia infantil; vazamento de documentos sigilosos; violência extrema; conteúdos de ódio; esquisitices macabras, como canibalismo; falsificação de documentos; dentre vários outros.

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

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

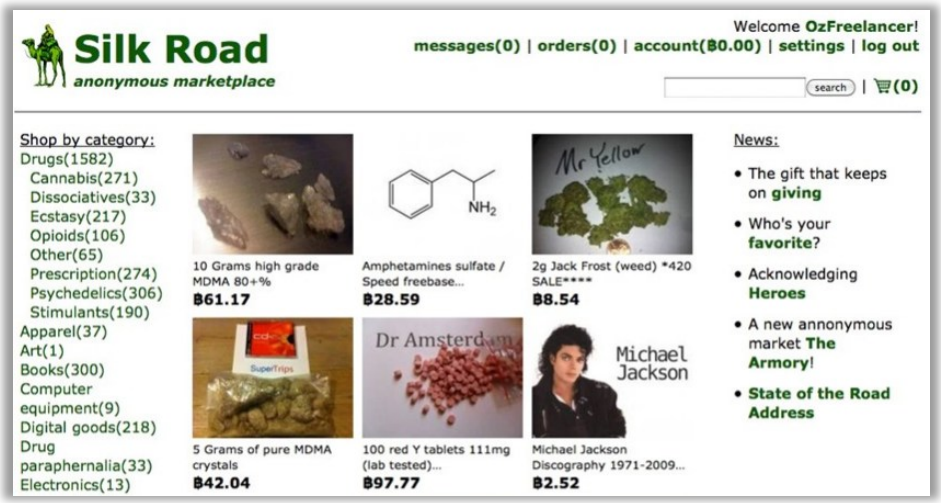
A parte mais obscura da Internet é a Dark Web, onde atividades ilegais podem ocorrer, mas essa é apenas uma pequena fração da Deep Web como um todo. Logo, em minha visão, a questão caberia recurso (Correto).

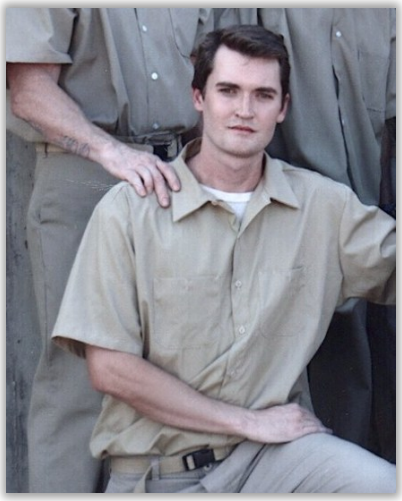
Para terminar, vamos apenas falar um pouco sobre a relação entre a Dark Web e Criptomoedas. Em 2013, existia um site na Rede Tor denominado Silk Road, no qual eram comercializados diversos produtos, desde substâncias ilícitas, como metanfetaminas, até itens comuns, como a discos e vinis. Para garantir o anonimato dos usuários, as transações não eram realizadas com cartões de crédito, mas sim por meio de uma criptomoeda: Bitcoin.

O Bitcoin é uma moeda digital que não transita pelo sistema financeiro tradicional dos países, dificultando o rastreamento das transações. Dentro da Rede Tor, o uso de criptomoedas torna praticamente impossível identificar quem realizou uma compra ou venda, o que favoreceu a popularização de plataformas como o Silk Road para a comercialização de bens e serviços – tanto legais quanto ilegais. Ele se tornou tão popular que virou uma espécie de Amazon do submundo da ilegalidade da internet.

Apesar do alto nível de anonimato, o administrador do Silk Road cometeu um erro que levou à sua captura. Ele utilizou seu nome verdadeiro ao fazer uma pergunta em um fórum público de programadores na Surface Web. O FBI, que já conduzia investigações sobre suas atividades ilícitas, conseguiu cruzar as informações, identificar o responsável e efetuar sua prisão. Como resultado, ele foi condenado a duas penas de prisão perpétua, acrescidas de 40 anos, sem possibilidade de liberdade condicional.

Esse episódio ilustra que, mesmo em ambientes projetados para preservar o anonimato, uma falha mínima pode comprometer toda a segurança.





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

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

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

Saiba mais:

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



Fóruns na dark web incitam violência e mortes e desafiam polícia

Massacre em Suzano foi comemorado em comunidades virtuais de criminosos

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

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

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

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

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

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

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

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

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

Internet das Coisas (IoT)

INCIDÊNCIA EM PROVA: BAIXA

INTERNET DAS COISAS

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

A ideia de conectar objetos à internet surgiu nos anos 1980, com experiências iniciais como uma máquina de refrigerantes capaz de informar se as bebidas estavam geladas. O termo Internet of Things (IoT) só foi formalmente criado em 1999. Ele propôs o conceito ao trabalhar com identificação por radiofrequência (RFID) para rastreamento de produtos. A partir da popularização da internet e da miniaturização de sensores e processadores, a IoT começou a ganhar força em larga escala, principalmente a partir de 2010.

A IoT é o conceito que descreve a capacidade de objetos físicos estarem conectados à internet, trocando informações entre si ou com servidores, de maneira automática, sem a necessidade constante de intervenção humana. Ela transforma itens do cotidiano em dispositivos inteligentes, capazes de coletar dados, processá-los e agir com base em informações recebidas. Esses dispositivos estão ficando cada vez mais comuns em nosso dia a dia.

Atualmente nós temos lâmpadas inteligentes, câmeras de segurança controladas por smartphone, carros configurados por aplicativo, agricultura inteligente, semáforos adaptativos, televisões acessadas via celular, relógios que monitoram batimentos cardíacos, entre outros. Isso porque estamos no Brasil! Em outros países mais desenvolvidos, já existem outras coisas: geladeiras, máquina de lavar roupa, forno de micro-ondas, termostato, alarme de incêndio, sistema de som e iluminação, entre outros.

Dispositivos IoT usam sensores, software e outras tecnologias embarcadas para se comunicar e interagir tanto com outros dispositivos quanto com sistemas de gerenciamento. Essa conexão cria redes de dispositivos inteligentes que melhoram a eficiência, otimizam processos e tornam a vida mais prática – seja em casas, cidades ou indústrias. Esses dispositivos podem funcionar de maneira local (apenas em uma rede interna) ou conectados a servidores remotos, usando computação em nuvem para processar dados e enviar comandos.

Saiba mais:

Imagine que a Internet das Coisas é como criar uma grande "rede social" não de pessoas, mas de coisas. Você chega em casa e vai abrir a porta da frente – já existem fechaduras inteligentes que podem abrir portas por meio do smartphone, senha ou impressão digital. Caso outra pessoa chegue na porta da sua casa, uma campainha com câmera pode avisar no seu celular quando alguém se aproximou - você pode ver quem é, falar com a pessoa e até abrir a porta remotamente.

Você entra em casa e vai para a sala de estar: luzes se acendem e mudam de cor e intensidade por meio de comandos de voz (Ex: Alexa). Aliás, você pode utilizar a voz para pedir para tocar ligar a televisão e colocar vídeo musical específico para tocar. Estamos no verão e quando a temperatura ultrapassa os 30°C, as cortinas são fechadas e o ar-condicionado é ligado automaticamente em 15°C. Aqui mencionei apenas uma casa, mas isso tem aplicabilidades na agricultura, pecuária, hospitais, escolas, fábricas, transporte público, logística, entre outros.

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

Comentários: na Internet das Coisas (IoT), o termo "coisas" refere-se a qualquer dispositivo ou objeto que pode ser equipado com eletrônicos, software e sensores para coletar, processar e compartilhar dados com outros dispositivos, sistemas ou a nuvem. Esses dispositivos podem variar desde eletrodomésticos inteligentes, veículos, sensores ambientais, máquinas industriais até wearables e muitos outros. O objetivo é permitir que essas "coisas" se comuniquem, coletem dados e tomem ações com base nessas informações, criando um ambiente conectado e inteligente (Correto).

IoT no Serviço Público

No contexto do serviço público, a IoT oferece ao setor público inúmeras possibilidades para aumentar eficiência, reduzir custos, melhorar serviços prestados e ampliar a transparência.

EXEMPLOS NO SERVIÇO PÚBLICO	DESCRIÇÃO
MONITORAMENTO INTELIGENTE	Sensores em iluminação pública, trânsito, estacionamentos água e esgoto podem reduzir custos, melhorar a manutenção preventiva e aumentar a qualidade de vida.
TRANSPORTE PÚBLICO	Integração de ônibus com sensores para acompanhamento em tempo real, reduzindo atrasos e melhorando a eficiência da mobilidade urbana.
MONITORAMENTO AMBIENTAL	Sensores instalados em rios, florestas e áreas urbanas identificam poluição, alertam sobre riscos ambientais (enchentes, incêndios) e ajudam no planejamento sustentável.
EFICIÊNCIA ENERGÉTICA	Prédios públicos inteligentes que otimizam automaticamente iluminação, climatização e consumo de energia elétrica.
HOSPITAIS CONECTADOS	Dispositivos de saúde conectados para monitoramento remoto de pacientes, gestão automatizada de medicamentos e equipamentos médicos.
MONITORAMENTO EPIDEMIOLÓGICO	Sensores para coleta e análise rápida de dados sobre epidemias, permitindo ações mais rápidas e assertivas.
MONITORAMENTO INTELIGENTE	Câmeras conectadas com reconhecimento facial e análise em tempo real para prevenção e combate ao crime.
SEGURANÇA COMUNITÁRIA	Alarmes comunitários conectados à polícia, sensores de ruídos de tiros, identificação automática de acidentes de trânsito.
AMBIENTES ESCOLARES	Salas conectadas para gestão eficiente de energia, segurança e acessibilidade.
MONITORAMENTO DE FREQUÊNCIA	Sensores para controle automatizado da presença escolar e alertas em casos de evasão.

Principais Componentes

A IoT não é uma tecnologia monolítica: seus componentes principais podem variar bastante. No entanto, em regra, incluem:

COMPONENTES DE IOT	DESCRIÇÃO
DISPOSITIVOS	São os elementos físicos que compõem a IoT, como sensores, atuadores e outros dispositivos conectados, como câmeras, medidores inteligentes, veículos e eletrodomésticos. Eles coletam dados do mundo real e podem executar ações com base nesses dados.
TECNOLOGIAS DE COMUNICAÇÃO	São os meios pelos quais os dispositivos IoT se comunicam entre si e com a nuvem. Isso pode incluir Wi-Fi, Bluetooth, 3G/4G/5G, Zigbee, LoRa, entre outros. As redes de

	comunicação são responsáveis pela transferência de dados dos dispositivos para a nuvem e vice-versa.
SENSORES E ATUADORES	Os sensores coletam informações do ambiente, como temperatura, umidade, localização, movimento e muito mais. Os atuadores são responsáveis por tomar ações, como ligar ou desligar um dispositivo. Eles são os olhos e as mãos da IoT.
NUVEM (CLOUD)	A nuvem é onde os dados coletados pelos dispositivos IoT são processados, armazenados e disponibilizados para acesso. Plataformas de nuvem fornecem recursos de computação, armazenamento e análise de dados em grande escala, tornando possível o processamento de grandes volumes de informações.

Interação com Nuvem

Os dispositivos IoT geram uma quantidade gigantesca de dados constantemente. Esses dispositivos muitas vezes têm capacidade limitada de processamento e armazenamento local. Como esses dispositivos sozinhos não conseguem armazenar ou processar todos os dados que geram, eles enviam essas informações para servidores de nuvem. A nuvem oferece capacidade virtualmente ilimitada para armazenar, analisar, processar e distribuir esses dados de forma eficiente.

Ao integrar IoT com a nuvem, é possível acessar e controlar dispositivos de qualquer lugar do mundo. Por exemplo, você pode verificar as câmeras de segurança da sua casa ou ajustar o ar-condicionado pelo celular, mesmo estando em outra cidade. A nuvem também permite aplicar análises avançadas e inteligência artificial sobre os dados coletados. Assim, sistemas conseguem identificar padrões, prever problemas, automatizar decisões ou alertar o usuário sobre algo importante.

Um ponto importante para essa realidade ser possível é o surgimento do IPv6: a nova versão do protocolo de endereçamento da internet. Diferente da versão anterior (IPv4), que já enfrenta escassez de endereços, o IPv6 oferece uma quantidade quase ilimitada de endereços IP. Isso significa que, mesmo com a conexão de bilhões de dispositivos e sensores no mundo, ainda teremos endereços suficientes por muito tempo.

Tecnologias de Comunicação

Além disso, para que todos esses equipamentos possam "conversar" entre si e com o sistema central, a comunicação é fundamental. Existem diversas tecnologias e protocolos criados especialmente para a Internet das Coisas (IoT), cada um adequado a diferentes necessidades, como consumo de energia, velocidade de transmissão ou alcance de sinal. A seguir, vamos conhecer algumas dessas principais tecnologias de comunicação utilizadas em projetos de IoT.

TECNOLOGIAS DE IOT	DESCRIÇÃO
WI-FI (802.11)	Trata-se de uma das tecnologias de comunicação sem fio mais amplamente utilizadas e oferece alta largura de banda. É adequado para dispositivos que têm acesso a redes locais de alta velocidade e energia suficiente.
BLUETOOTH (802.15)	Trata-se de uma tecnologia de comunicação sem fio de curto alcance, adequada para dispositivos pessoais, como fones de ouvido sem fio e dispositivos vestíveis. O Bluetooth Low Energy (BLE) é uma variante de baixo consumo de energia.
ZIGBEE	Trata-se de um padrão de comunicação sem fio de baixa potência projetado para redes de sensores e dispositivos IoT em ambientes domésticos e industriais.

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

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

Vantagens e Desvantagens

Por fim, vejamos agora as vantagens e desvantagens dessa tecnologia:

VANTAGENS DO IOT	DESVANTAGENS DO IOT
Varejistas podem fornecer bônus de fidelidade para clientes preferenciais.	A dependência de compras online pode custar empregos.
As cidades podem avaliar as necessidades futuras de transporte.	Os varejistas podem saber tudo o que você está comprando.
Indivíduos podem reduzir os custos de energia e dos sistemas de aquecimento residenciais.	Os indivíduos podem receber mais e-mails de spam.
Fabricantes podem reduzir a inatividade prevendo as necessidades de manutenção dos equipamentos.	Uma falha da rede pode ser catastrófica.
Os governos podem monitorar o ambiente.	As empresas que criam dispositivos vestíveis têm muitas informações pessoais sobre os usuários.

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

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

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

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

Tecnologias de Acesso

TECNOLOGIAS DE ACESSO À INTERNET

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

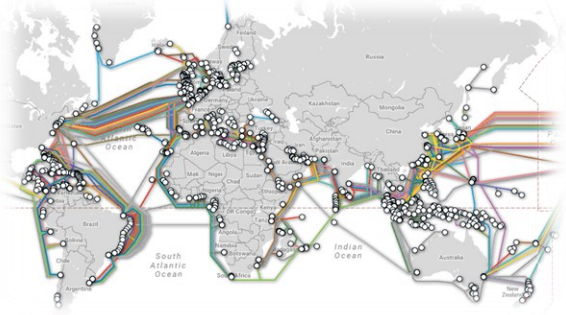
Até o início da década de 1990, o uso da internet era restrito a um grupo seleto de pessoas: pesquisadores de universidades, instituições governamentais e grandes corporações industriais. Era uma rede com fins eminentemente acadêmicos, científicos e militares, sem qualquer propósito comercial ou de entretenimento para o grande público. No entanto, essa realidade começou a mudar radicalmente quando foi criada a World Wide Web (WWW).

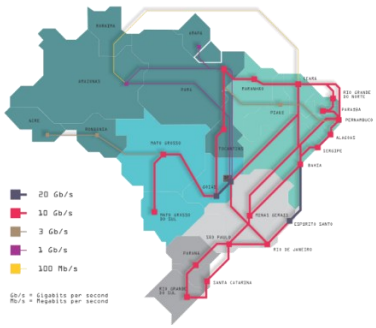
A criação da Web possibilitou a popularização da internet como conhecemos hoje, tornando seu acesso e utilização muito mais intuitivos e acessíveis para o cidadão comum. Ela introduziu uma nova forma de organização da informação: páginas interligadas por hiperlinks, possibilitando que, com apenas um clique, o usuário fosse direcionado de uma página para outra.

Ao lado da Web, surgiu também o primeiro navegador da história, chamado WorldWideWeb (posteriormente renomeado para Nexus), que permitia a visualização de documentos contendo textos, imagens, áudio e, futuramente, vídeos. Essa combinação de navegação fácil e conteúdo multimídia impulsionou o rápido crescimento do número de páginas e, consequentemente, de usuários conectados.

Esse crescimento exponencial da internet foi impulsionado, em grande parte, por empresas denominadas ISPs (Internet Service Providers) – Provedores de Serviço de Internet. Essas empresas passaram a oferecer ao público em geral a possibilidade de se conectar à internet de forma prática, segura e acessível. Com isso, milhões de novos usuários ingressaram na rede, alterando o perfil típico de utilização – que deixou de ser estritamente acadêmico para se tornar cada vez mais popular, comercial e voltado para a comunicação e o entretenimento. A internet transformou-se, então, em um serviço essencial, comparável a outros serviços públicos como a telefonia e a energia elétrica.

Para disponibilizar o acesso à internet em escala mundial, é necessária uma vasta infraestrutura de comunicação. Essa infraestrutura é composta por satélites, antenas de rádio e, principalmente, por uma imensa rede de cabos de fibra óptica terrestres e submarinos que conectam diferentes países e continentes. Estima-se que cerca de 80% da comunicação global de dados trafegue por meio dessas redes de fibra óptica. Essa estrutura crítica é chamada de Backbone – a "espinha dorsal" da internet. O backbone interliga grandes redes de dados em alta velocidade, garantindo o fluxo de informações através de vastas distâncias geográficas.



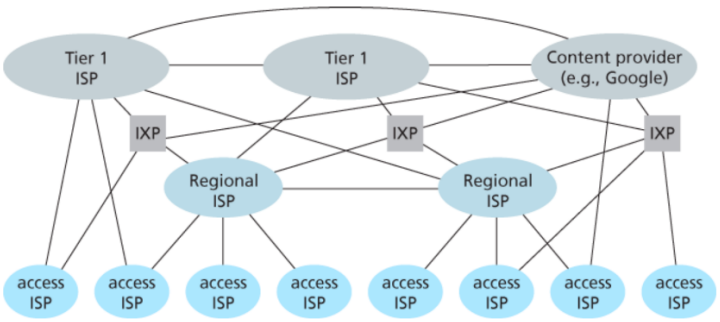


A construção e manutenção dos backbones são tarefas realizadas por grandes corporações ou entidades governamentais. No Brasil, por exemplo, temos backbones construídos por empresas como a Embratel (operadora de longa distância) e pela Rede Nacional de Ensino e Pesquisa (RNP), que conecta universidades, institutos de pesquisa e outras entidades públicas. Esses backbones formam a base sobre a qual os ISPs se conectam para oferecer acesso aos usuários finais. De forma prática: os grandes backbones fornecem acesso aos grandes provedores de internet (Ex: NET/CLARO, GVT/VIVO e SKY), que por sua vez oferecem o serviço diretamente aos clientes domésticos ou a pequenos provedores regionais.



A interligação global dos backbones pode ser visualizada em mapas que mostram verdadeiras redes de cabos submarinos e terrestres espalhados pelos oceanos e continentes. Esses cabos são responsáveis por manter a comunicação fluída entre países e possibilitar, por exemplo, que um usuário no Brasil possa acessar um servidor nos Estados Unidos ou na Europa em questão de milissegundos. É essa complexa e robusta infraestrutura que sustenta a internet como a conhecemos hoje – um sistema descentralizado, resiliente e capaz de conectar bilhões de dispositivos em todo o planeta.

Nem todos os ISPs têm o mesmo papel ou alcance: existem diferentes níveis de provedores, classificados conforme sua capacidade de infraestrutura, cobertura e dependência de outras redes[17]. Vejamos:



NÍVEIS DE ISP	DESCRIÇÃO
ISP NÍVEL 1	São os provedores de backbone mundial. Não precisam comprar trânsito IP de ninguém. Se conectam diretamente entre si (acordos de peering). Apresentam características como: cobertura global; alta capacidade de infraestrutura própria; e conectam redes sem custo de trânsito (peering). ISP Nível 1 são como aviões de grande porte que fazem voos internacionais e controlam as principais rotas aéreas globais (Exemplos: AT&T, CenturyLink (Lumen), NTT, Telia)
ISP NÍVEL 2	Compram acesso de ISPs Nível 1 e fazem peering com outros ISPs Nível 2. Atendem a grandes regiões, países ou continentes. Apresentam características como: têm alguma infraestrutura; dependem parcialmente de Nível 1; buscam acordos de peering para reduzir custos. ISP Nível 2 são como companhias nacionais que compram o direito de usar parte dessas rotas para conectar cidades e países (Exemplos: Embratel, Vivo, TIM, Claro)
ISP NÍVEL 3	São provedores locais ou regionais. Compram completamente o acesso à Internet de ISPs Nível 2 ou Nível 1. Apresentam características como: pouco ou nenhuma infraestrutura própria; conexão limitada a clientes locais; dependem totalmente de ISPs superiores. ISP Nível 3 são como empresas de transporte local, que compram serviços das grandes

[17] A classificação em Níveis 1, 2 e 3 é suficiente para entender como a internet se organiza mundialmente. Alguns autores chegam a detalhar ainda mais e mencionam subdivisões (como Nível 2,5 para provedores regionais maiores), mas oficialmente só existem três níveis reconhecidos.

	companhias para levar passageiros até bairros e pequenas localidades (Exemplos: provedores de bairro, pequenos provedores locais).

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

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

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

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

Dial-Up

INCIDÊNCIA EM PROVA: MÉDIA

O Dial-Up foi uma das primeiras formas de acesso residencial à Internet e funcionava por meio da linha telefônica convencional. Para se conectar, o computador utilizava um modem que discava (literalmente fazia uma chamada telefônica) para o número de um provedor de Internet (ISP). Uma vez estabelecida a conexão, os dados eram transmitidos em formato analógico através da rede telefônica. A taxa de transmissão era bastante limitada, com velocidades máximas de 56 Kbps, o que tornava atividades como carregar páginas pesadas, baixar arquivos ou assistir vídeos bastante lentas e demoradas.

Essa tecnologia tinha diversas limitações: enquanto o usuário estava conectado à Internet, a linha telefônica ficava ocupada, impedindo a realização de chamadas comuns. Além disso, a conexão podia ser instável e facilmente interrompida. Apesar disso, o Dial-Up foi essencial nos primeiros anos da popularização da Internet, principalmente entre usuários domésticos, por ser relativamente barato e aproveitar uma infraestrutura de telefonia que já existia. Com o tempo, foi substituído por tecnologias mais rápidas, como ADSL e fibra óptica.

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

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

Comentários: dial-up é uma forma de acesso à Internet usando linhas telefônicas e modems, sendo caracterizada por baixa velocidade de conexão, e não por alta velocidade; além disso, não é considerada uma rede de computadores, mas sim um meio de acesso à rede (Errado).

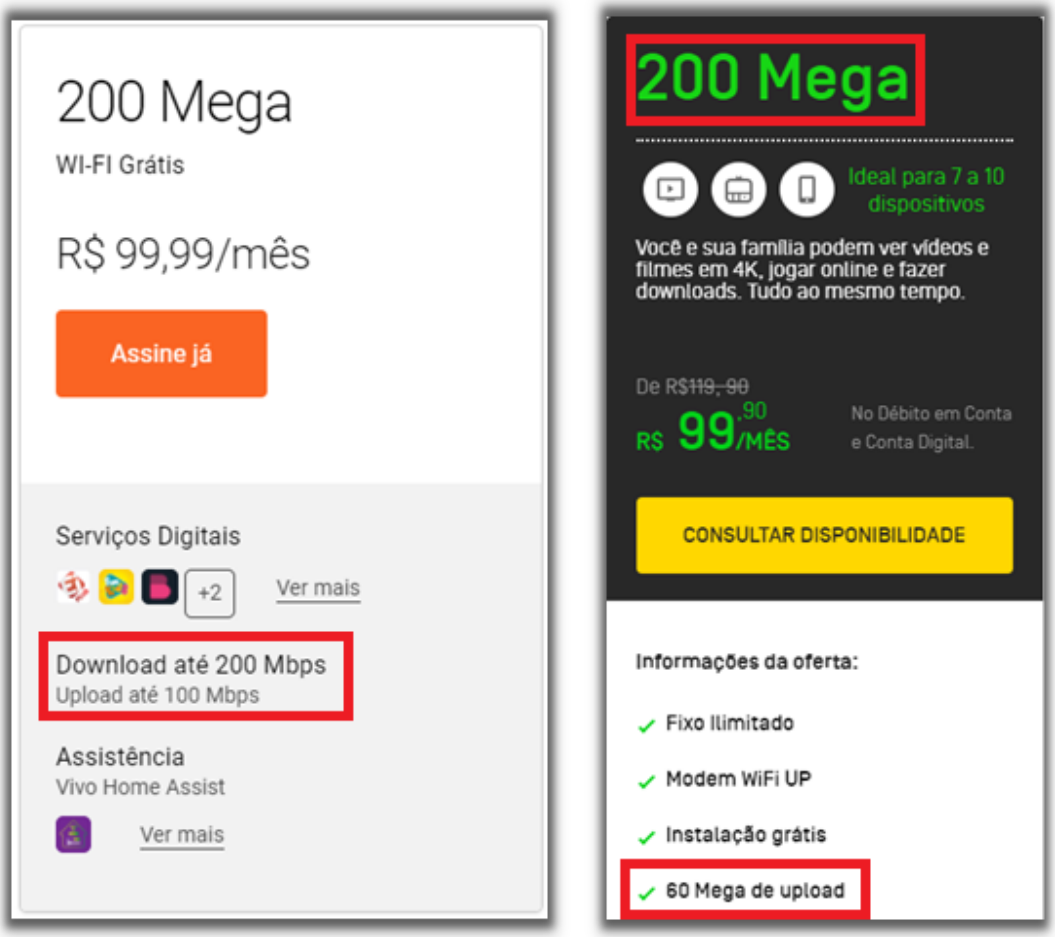
ADSL

INCIDÊNCIA EM PROVA: MÉDIA

O ADSL (Asymmetric Digital Subscriber Line) é uma tecnologia de acesso à Internet que utiliza a linha telefônica comum, mas de forma diferente do antigo Dial-Up. Em vez de ocupar toda a linha para transmissão de dados, o ADSL divide a linha em três faixas de frequência: uma para voz (ligações telefônicas) e duas para dados (upload e download), permitindo que o usuário navegue na Internet e faça ligações telefônicas simultaneamente. Como o próprio nome diz, a conexão é assimétrica, ou seja, a velocidade de download é maior que a de upload – o que atende à maioria dos usuários, que geralmente baixam mais dados do que enviam.

O ADSL trouxe um grande avanço para o acesso residencial e comercial à Internet, oferecendo velocidades muito superiores ao Dial-Up, variando de 256 Kbps a vários Mbps dependendo da qualidade da linha e da distância até a central telefônica. Além de permitir conexão contínua (sem necessidade de discagem), o ADSL foi fundamental para a popularização de novos serviços como streaming de vídeos, jogos online e VoIP. Com o tempo, no entanto, foi sendo substituído por tecnologias ainda mais rápidas, como VDSL e fibra óptica.

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



ADSL	DESCRIÇÃO
ASSIMÉTRICA	O "A" em ADSL significa assimétrico, o que indica que a taxa de upload (envio de dados) é diferente da taxa de download (recebimento de dados). Geralmente, a taxa de download é significativamente mais rápida do que a de upload.
UTILIZAÇÃO DAS LINHAS TELEFÔNICAS	O ADSL utiliza as linhas telefônicas convencionais para transmitir dados. Ele é compatível com a infraestrutura de telefone existente, permitindo que os usuários acessem a Internet e façam chamadas telefônicas simultaneamente.
FREQUÊNCIAS DIFERENTES	Linhas telefônicas transmitem dados em diferentes frequências. As frequências mais baixas são reservadas para voz, enquanto as frequências mais altas são usadas para transmitir dados. Isso permite que a Internet e as chamadas coexistam na mesma linha.

VELOCIDADE VARIÁVEL	A velocidade da conexão ADSL pode variar de acordo com a distância entre o usuário e a central telefônica. Quanto mais longa a linha telefônica, mais lenta é a conexão. Isso ocorre porque o sinal ADSL enfraquece à medida que viaja por distâncias maiores.
TAXA DE UPLOAD LIMITADA	A taxa de upload no ADSL é geralmente menor do que a de download. Isso significa que o envio de dados, como o carregamento de arquivos ou o envio de e-mails com anexos grandes, é mais lento do que o download.
LARGURA DE BANDA COMPARTILHADA	A largura de banda em uma linha ADSL é compartilhada entre todos os usuários conectados a essa linha. Isso significa que, em horários de pico, a velocidade da conexão pode diminuir devido à concorrência por largura de banda.
ADEQUADA PARA APLICAÇÕES RESIDENCIAIS	O ADSL é frequentemente usado em ambientes residenciais. É adequado para atividades como navegação na web, streaming de vídeos em qualidade padrão e jogos online.
AMPLA DISPONIBILIDADE	Devido à utilização das linhas telefônicas existentes, o ADSL é amplamente disponível em muitas áreas urbanas e rurais. No entanto, a velocidade da conexão pode variar dependendo da localização geográfica.
REQUER UM MODEM ADSL	Os usuários precisam de um modem ADSL para estabelecer a conexão. Esse modem é fornecido pelo provedor de serviços de Internet ou pode ser adquirido separadamente.
SUPERADO POR TECNOLOGIAS MAIS RÁPIDAS	Embora ainda seja utilizado, o ADSL foi superado por tecnologias de banda larga mais rápidas, como a fibra óptica e o cabo, que oferecem velocidades mais altas e uma experiência de Internet mais fluida.

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

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

Comentários: (a) Correto. ADSL é uma tecnologia que permite a transmissão digital de dados em alta velocidade por meio de linhas telefônicas comuns, sem interferir nas chamadas telefônicas; (b) Errado. AUP (Acceptable Use Policy) refere-se a políticas de uso aceitável, não a uma tecnologia de transmissão; (c) Errado. IP (Internet Protocol) é um protocolo de comunicação para identificação e localização de dispositivos na rede, não uma tecnologia de transmissão telefônica; (d) Errado. FTP (File Transfer Protocol) é um protocolo para transferência de arquivos, também não relacionado ao uso de linha telefônica para transmissão de dados (Letra A).

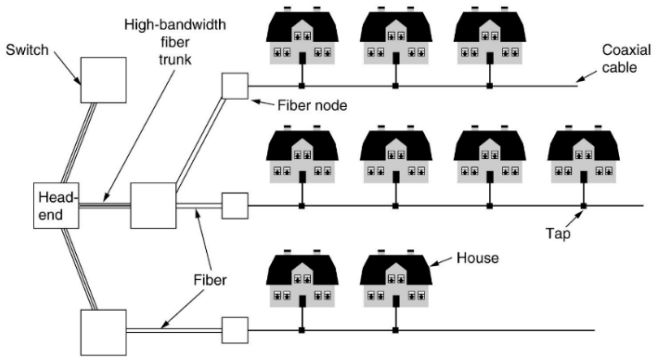
HFC

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

O HFC (Hybrid Fiber-Coaxial) é uma tecnologia de acesso à Internet que combina dois tipos de cabos: fibra óptica e cabo coaxial. A fibra óptica é usada da central do provedor até um ponto próximo à residência ou empresa do usuário (chamado de nó óptico). A partir desse nó, o sinal é convertido e transmitido por cabo coaxial até o modem do usuário final. Essa combinação aproveita a alta capacidade de transmissão da fibra para grandes distâncias e o custo mais baixo do coaxial nas últimas conexões. É comum que empresas de TV a cabo também ofereçam acesso à Internet usando a infraestrutura HFC.

Essa tecnologia trouxe velocidades muito superiores às do ADSL, atingindo facilmente centenas de megabits por segundo, além de possibilitar a oferta simultânea de televisão por assinatura, Internet e telefone na mesma infraestrutura, o chamado serviço "triple-play". Uma limitação do HFC, porém, é que o cabo coaxial é compartilhado entre vários usuários em uma mesma região, o que pode gerar quedas

de desempenho nos horários de pico. Ainda assim, o HFC foi (e continua sendo) fundamental para a expansão do acesso rápido à Internet em áreas urbanas.



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

(PROF. DIEGO / INÉDITA – 2025) HFC é uma tecnologia que utiliza tanto fibra óptica quanto cabos coaxiais para fornecer serviços de internet e TV a cabo.

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

FTTH

INCIDÊNCIA EM PROVA: BAIXÍSSIMA





O FTTH (Fiber To The Home) é basicamente uma fibra óptica vai diretamente da central do provedor até a casa do usuário, sem utilizar nenhum outro meio intermediário, como cabos metálicos (coaxiais ou de cobre). Essa abordagem permite oferecer altíssimas velocidades de transmissão (podendo chegar a vários gigabits por segundo), além de garantir maior estabilidade, baixa latência e resistência a interferências eletromagnéticas.

Como o meio óptico é mantido integralmente até o usuário final, o FTTH é hoje considerado a tecnologia mais moderna e eficiente para acesso à Internet residencial e corporativo. Uma das grandes vantagens do FTTH é que, ao contrário do ADSL ou do HFC, o sinal não é compartilhado no último trecho da rede. Cada usuário possui sua própria conexão direta em fibra, o que mantém a velocidade contratada mesmo em horários de pico.

Além disso, a fibra óptica é altamente durável e tem capacidade de expansão para suportar novas demandas futuras sem necessidade de substituição da infraestrutura básica. No entanto, o FTTH exige investimento mais alto em sua implantação inicial, o que explica por que ele é mais comum em grandes centros urbanos e ainda está em expansão em áreas mais afastadas.

FTTH	DESCRIÇÃO
FIBRA DIRETA À RESIDÊNCIA	Diferente do HFC, a fibra óptica vai diretamente até a residência do usuário, sem transição para cabos coaxiais.
CANAL DEDICADO	No FTTH, cada usuário pode ter um canal dedicado, o que elimina o compartilhamento do meio de transmissão e reduz a concorrência de banda com vizinhos.
VELOCIDADES MUITO ALTAS	O FTTH proporciona velocidades extremamente altas de download e upload, com planos que podem ultrapassar 1 Gbps, ideal para grandes transferências, jogos, vídeos 4K/8K e aplicações profissionais.
BAIXÍSSIMA LATÊNCIA	A tecnologia de fibra direta oferece latência muito baixa, fundamental para aplicações em tempo real, como videoconferências, cirurgias remotas, e jogos online competitivos.

APENAS INTERNET (OU COM TV/IPTV)	Embora o FTTH seja focado principalmente na Internet de alta velocidade, também é possível adicionar serviços de IPTV (TV pela Internet) e VoIP, dependendo do provedor.
ONT E ROTEADORES ESPECÍFICOS	No FTTH, utiliza-se um ONT (Optical Network Terminal) para converter o sinal óptico em dados de rede. É necessário equipamento específico, fornecido ou indicado pelo provedor.
MAIOR DISPONIBILIDADE EM ÁREAS NOVAS	O FTTH está crescendo principalmente em novos bairros urbanos, condomínios e cidades inteligentes, em que a instalação de fibra é mais fácil e econômica.
PACOTES DE ULTRA-VELOCIDADE	Provedores de FTTH oferecem planos premium, como internet simétrica (velocidades iguais de download e upload) e serviços para usuários de alta demanda.
CUSTO DE IMPLANTAÇÃO E MANUTENÇÃO	O investimento inicial para instalação é mais alto que o HFC, mas, em compensação, a manutenção é mais barata e a rede é mais escalável para o futuro.

(FUNCERN / Prefeitura de Carnaúba dos Dantas-RN – 2024) Um aluno de graduação de rede de computadores foi convidado para assistir uma palestra sobre tecnologia FTTH. Essa tecnologia está relacionada com:

a) CAT6.
b) WiMax.
c) Fibra óptica.
d) Cabo Coaxial.

Comentários: (a) Errado. CAT6 é um tipo de cabo de par trançado utilizado em redes Ethernet, não relacionado diretamente à tecnologia FTTH; (b) Errado. WiMax é uma tecnologia de comunicação sem fio de longa distância, não ligada diretamente ao conceito de FTTH; (c) Correto. FTTH (Fiber To The Home) refere-se à tecnologia de entrega de conexões de fibra óptica diretamente até as residências dos usuários, proporcionando alta velocidade de acesso à Internet; (d) Errado. Cabo coaxial é utilizado em redes antigas de TV a cabo e internet, mas não caracteriza a tecnologia FTTH (Letra C).

PLC

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

O PLC (Power Line Communication) é uma técnica que permite a transmissão de dados digitais utilizando a própria fiação elétrica já existente nos edifícios e residências. Em vez de instalar cabos de rede separados, os dados são "injetados" nas tomadas elétricas através de adaptadores especiais (Modems PLC), permitindo que qualquer ponto da casa com uma tomada elétrica se torne um ponto de acesso à rede. Essa tecnologia surgiu como uma solução prática e econômica para melhorar a cobertura da internet em locais onde o Wi-Fi apresenta dificuldades de alcance ou onde a instalação de cabos estruturados seria inviável ou muito onerosa.

O PLC é bastante utilizado em ambientes domésticos para estender redes de internet de forma simples, mas também possui aplicações industriais e comerciais. Apesar da facilidade de uso, a qualidade da conexão pode ser afetada por interferências elétricas, como motores de geladeiras ou furadeiras, e pela qualidade da rede elétrica interna. Ainda assim, para muitos usuários, o PLC representa uma solução eficiente para garantir acesso à internet em todos os cômodos, utilizando simplesmente as tomadas elétricas já disponíveis.

PLC	DESCRIÇÃO
USO DE INFRAESTRUTURA ELÉTRICA	O PLC utiliza a rede elétrica preexistente para transmitir dados. Isso significa que não são necessários cabos de rede adicionais, como os usados em conexões Ethernet tradicionais.

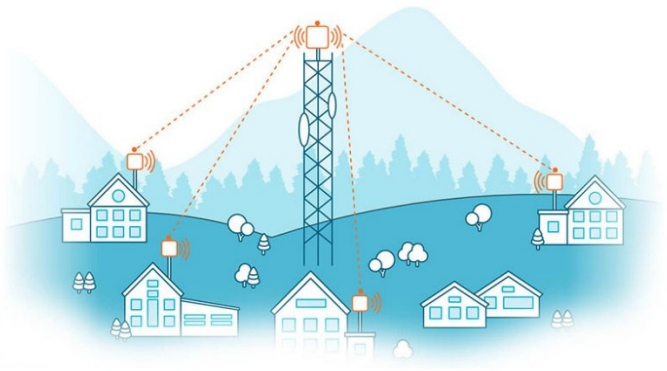
FACILIDADE DE INSTALAÇÃO	A instalação é relativamente simples. Em geral, usuários precisam de um adaptador PLC que é conectado a uma tomada elétrica e ao roteador. Outros adaptadores podem ser conectados a tomadas em diferentes partes da residência para estender a cobertura.
VELOCIDADE VARIÁVEL	A velocidade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

(CEBRASPE / FUB – 2011) A tecnologia Power Line Communication (PLC) possibilita a transmissão de dados através das redes de energia elétrica, utilizando-se uma faixa de frequência diferente da normalmente utilizada na rede elétrica para a distribuição de energia.

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

Rádio

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



A tecnologia de acesso via rádio é uma forma de conexão sem fio que utiliza ondas de rádio para transmitir dados entre um ponto de acesso (geralmente uma torre ou antena) e os usuários finais. Essa tecnologia é bastante utilizada em áreas onde o cabeamento de redes (como fibra óptica ou HFC) é inviável, seja por custo elevado ou pela dificuldade de infraestrutura, como em zonas rurais ou regiões afastadas. As conexões por rádio podem oferecer velocidades variadas, dependendo da tecnologia

empregada (como WiMAX ou rádio ponto-a-ponto) e da qualidade da linha de visada entre a antena do provedor e a antena do cliente.

Apesar de ser uma solução prática e relativamente rápida de implementar, o acesso via rádio pode sofrer com limitações como interferências climáticas (chuvas fortes, por exemplo), barreiras físicas (montanhas, prédios) e limitações de alcance. Para um bom desempenho, é importante que exista uma linha de visada clara (sem obstáculos) entre o transmissor e o receptor. Ainda assim, a tecnologia é uma alternativa importante para levar internet a locais onde outras formas de acesso não chegaram ou são muito custosas. Vejamos as principais características de redes de rádio:

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

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

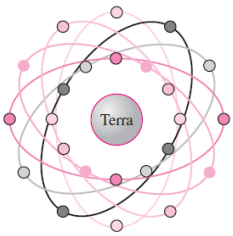
a) Fibra óptica
b) Cabo de par trançado
c) Enlace de rádio

d) Cabo coaxial
e) Rede elétrica

Comentários: (a) Errado. A fibra óptica é bastante resistente a interferências externas, incluindo variações climáticas, pois transmite sinais de luz internamente; (b) Errado. O cabo de par trançado é suscetível a interferências eletromagnéticas, mas não diretamente a variações climáticas como nuvens e chuva; (c) Correto. Enlaces de rádio, especialmente em comunicações via satélite ou ponto a ponto, são bastante afetados por condições climáticas, como acúmulo de nuvens, chuvas e tempestades, prejudicando a qualidade do sinal; (d) Errado. O cabo coaxial é relativamente protegido contra interferências externas e menos impactado por mudanças climáticas; (e) Errado. A rede elétrica é mais sensível a variações de carga e interferências elétricas internas, não diretamente a variações de clima como nuvens e precipitação (Letra C).

Satélite

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



A tecnologia de acesso via satélite permite que usuários se conectem à Internet utilizando sinais enviados e recebidos por satélites orbitando a Terra. Esse tipo de acesso é especialmente útil para regiões muito remotas, como zonas rurais isoladas, áreas montanhosas ou locais sem infraestrutura terrestre de telecomunicações (fibra óptica, cabos, rádio). O funcionamento básico envolve uma antena parabólica instalada na casa ou empresa do usuário, que se comunica diretamente com o satélite, que, por sua vez, se conecta aos pontos da rede global de Internet.

Embora o acesso por satélite tenha a grande vantagem de cobertura praticamente global, ele também apresenta algumas limitações importantes. A latência (atraso de resposta) é geralmente mais alta do que em outras tecnologias, devido à distância que os sinais precisam percorrer até o satélite e voltar. Isso pode prejudicar aplicações que exigem resposta rápida, como jogos online e chamadas de vídeo em tempo real. Ademais, o serviço pode ser afetado por condições climáticas adversas (Ex: chuvas fortes) e, tradicionalmente, o custo de instalação e manutenção tende a ser mais elevado do que outras alternativas.

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

APLICAÇÕES DIVERSAS

Além do acesso à internet, a tecnologia de satélite é usada em comunicações globais, TV via satélite e comunicações por satélite em locais sem infraestrutura de telecomunicações.

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

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

Comentários: (a) Errado. O cabo coaxial é usado para transmissões locais (como TV a cabo) e não oferece cobertura global; (b) Errado. O canal de HF (alta frequência) é usado para comunicações de longa distância em rádio, mas com baixa largura de banda, inadequada para transmissões intensivas como ensino à distância; (c) Errado. A fibra óptica oferece alta largura de banda, mas depende de cabeamento físico, não proporcionando cobertura global; (d) Errado. O par trançado é usado em redes locais (LANs) e possui alcance e largura de banda limitados, sem cobertura global; (e) Correto. O satélite é ideal para o ensino à distância, pois proporciona cobertura global, alta largura de banda e capacidade de transmissões de difusão (broadcast), alcançando regiões remotas (Letra E).

Telefonia Móvel

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

A tecnologia de acesso à Internet via telefonia móvel utiliza as redes celulares para conectar dispositivos como smartphones, tablets e até computadores à Internet. Essa conexão é realizada por meio de torres de transmissão (antenas) que se comunicam com dispositivos móveis utilizando padrões de comunicação como 3G, 4G e, mais recentemente, 5G. À medida que a tecnologia evoluiu, as velocidades de conexão aumentaram drasticamente, permitindo hoje acesso a vídeos em alta definição, videoconferências e jogos online diretamente pelo celular, com alta mobilidade e em qualquer lugar que tenha cobertura de sinal.

Apesar da praticidade e da ampla cobertura urbana, o acesso móvel apresenta algumas limitações. A qualidade da conexão pode variar bastante dependendo da densidade de usuários (como em grandes eventos), da distância até a torre e de obstáculos físicos (prédios, montanhas). Além disso, muitos planos de telefonia impõem limites de dados ou reduzem a velocidade após certo consumo mensal. Mesmo com essas limitações, o acesso à Internet pela rede móvel é hoje uma das principais formas de conexão no mundo, especialmente em países em desenvolvimento. Vejamos as principais gerações de telefonia:

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

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

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

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

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

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

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

GLOSSÁRIO

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



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

CONEXÃO PONTO-MULTIPONTO	Tipo de conexão em que um único dispositivo central se conecta a múltiplos dispositivos, formando uma rede de comunicação de uma para muitas conexões.
ARQUITETURA PONTO-A-PONTO	Modelo de rede em que cada dispositivo pode funcionar tanto como cliente quanto como servidor, permitindo compartilhamento direto de arquivos e recursos.
ARQUITETURA CLIENTE/SERVIDOR	Modelo de rede em que um servidor central fornece recursos ou serviços, e os clientes acessam esses serviços.
MEIO GUIADO	Tipo de meio de transmissão em que os sinais são direcionados ao longo de um caminho físico, como cabos e fios.
MEIO NÃO GUIADO	Meio de transmissão que utiliza ondas de rádio, micro-ondas ou infravermelho para transmitir dados pelo ar ou espaço, sem a necessidade de um caminho físico.
CABO COAXIAL	Tipo de cabo usado para transmitir sinais elétricos, caracterizado por um núcleo interno de metal rodeado por um isolante, um condutor externo de metal e uma capa externa.
CABO DE PAR TRANÇADO	Cabo composto por pares de fios entrelaçados que são usados para reduzir a interferência eletromagnética e aumentar a confiabilidade na transmissão de dados.
FIBRA ÓPTICA	Meio de transmissão de dados que utiliza luz para transmitir informações através de fibras de vidro ou plástico.
CONECTOR BNC	Tipo de conector usado principalmente com cabos coaxiais, caracterizado por sua conexão de baioneta que oferece uma conexão rápida e segura.
CONECTOR RJ-45	Tipo de conector usado principalmente em cabos de par trançado para redes Ethernet, comumente utilizado para conectar computadores a redes locais.
ARQUITETURA TCP/IP	Conjunto de protocolos usados para interligar dispositivos em redes. Baseia-se em camadas de protocolos que abrangem funções desde a comunicação básica até aplicações avançadas.
MODELO OSI	Modelo conceitual criado para padronizar as funções de um sistema de telecomunicações ou computação em sete camadas abstratas, desde a camada física até a camada de aplicação.
INTERNET	Rede global de computadores interconectados que utilizam o padrão TCP/IP para servir bilhões de usuários em todo o mundo, facilitando a troca de informações e comunicação.
WWW	Sistema de documentos e recursos interligados por links de hipertexto, acessíveis pela Internet e visualizados por navegadores web.
SURFACE WEB	Parte da Web que é indexada por motores de busca convencionais e acessível ao público em geral.
DEEP WEB	Parte da Internet que não é indexada por motores de busca convencionais, incluindo páginas protegidas por senha, bancos de dados privados, entre outros.
DARK WEB	Parte da Deep Web intencionalmente escondida e inacessível através de navegadores web convencionais, frequentemente associada com atividades ilegais.
FERRAMENTAS DE BUSCA	Programas ou serviços online que permitem aos usuários pesquisar conteúdo na Internet, geralmente através de palavras-chave ou consultas (Ex: Google, Bing, etc).
REDE TOR	Rede de servidores voluntários que permite o anonimato na Internet através do encaminhamento de tráfego através de múltiplas camadas de servidores.
INTELIGÊNCIA ARTIFICIAL	Área computacional que envolve a criação de máquinas capazes de realizar tarefas que normalmente requerem inteligência humana, como aprendizado, raciocínio e adaptação.
NAVEGADOR WEB	Software utilizado para acessar e visualizar páginas da Web na Internet, interpretando e exibindo conteúdos HTML e outros.
BITTORRENT	Protocolo para compartilhamento de arquivos Peer-To-Peer (P2P), permitindo a distribuição de dados e arquivos eletrônicos pela Internet de maneira descentralizada.
REDES CELULARES	Sistemas que usam uma rede distribuída de estações base (antenas de celular) para fornecer conectividade móvel e comunicação sem fio em uma área geográfica ampla.
ISP	Empresa que fornece serviços de acesso à Internet para clientes, oferecendo diferentes tipos de conexões, como banda larga, fibra óptica, entre outras.
DIAL-UP	Tipo de acesso à Internet de baixa velocidade que utiliza linhas telefônicas convencionais e um modem para conectar-se à Internet.

ADSL	Tipo de conexão de banda larga que utiliza as linhas telefônicas existentes para transmitir dados, oferecendo maior velocidade de download em relação ao upload.
HFC	Tecnologia de rede que combina fibra óptica e cabos coaxiais para entrega de serviços de Internet e TV a Cabo.
FIBRA ÓPTICA	Tecnologia de transmissão de dados de alta velocidades que utiliza fibras de vidro ou plástico para conduzir luz.
PLC	Tecnologia que permite a transmissão de dados por meio das linhas de energia elétrica existentes, utilizando-as simultaneamente para transmissão de energia e dados.
RÁDIO	Método de transmissão de sinais de áudio e vídeo (rádio e TV) através de ondas eletromagnéticas no espaço livre, sem a necessidade de uma conexão física.
SATÉLITE	Tecnologia de comunicação que utiliza satélites artificiais em órbita terrestre para transmitir e receber sinais.
INTERNET DAS COISAS (IOT)	Conexão de dispositivos do cotidiano à internet, permitindo que eles enviem e recebam dados, como eletrodomésticos, carros e sistemas de segurança.
NUVEM (CLOUD)	Armazenamento e processamento de dados em servidores remotos acessíveis pela internet, possibilitando acesso a informações e aplicativos de qualquer lugar.
IPV6	Versão mais recente do Protocolo de Internet, desenvolvida para substituir o IPv4.
AIRDROP	Tecnologia que permite o compartilhamento de arquivos entre dispositivos Apple (como iPhones e Macs) usando Wi-Fi e Bluetooth.
PICONET	Tipo de rede sem fio formada pela conexão entre dispositivos Bluetooth, geralmente consistindo em um dispositivo principal e até sete dispositivos secundários.
SCATTERNET	Rede que interliga várias piconets bluetooth, permitindo que dispositivos comuniquem entre diferentes piconets.
WIMAX	Tecnologia de comunicação sem fio de alta velocidade, destinada a oferecer acesso à internet de banda larga a longas distâncias.
WEP, WPA, WPA2, WPA3	Protocolos de segurança para redes Wi-Fi. WEP é o mais antigo e menos seguro, enquanto WPA, WPA2 e WPA3 são evoluções com segurança aprimorada.
BITCOIN	Primeira e mais conhecida criptomoeda, um tipo de moeda digital que utiliza criptografia para controlar sua criação e gestão, sem a necessidade de uma autoridade central.
CRIPTOMOEDAS	Moedas digitais que usam criptografia para segurança. São descentralizadas e baseadas em tecnologia blockchain, permitindo transações seguras e anônimas.

RESUMO

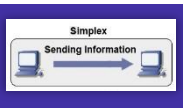
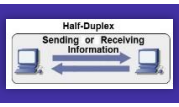
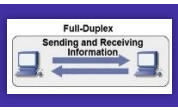
REDES DE COMPUTADORES

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

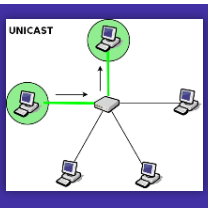
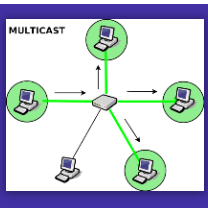
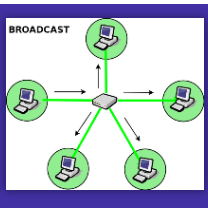
TIPOS DE CONEXÃO/ENLACE

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

DIREÇÕES DE TRANSMISSÃO

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

MODOS DE TRANSMISSÃO

TIPO	REPRESENTAÇÃO	DESCRIÇÃO
UNICAST		Uma mensagem só pode ser enviada para um destino. Grosso modo, quando você envia uma mensagem no Whatsapp para uma pessoa específica, você está enviando uma mensagem unicast.
MULTICAST		Uma mensagem é enviada para um grupo de destino. Grosso modo, quando você cria uma lista de transmissão no Whatsapp com um grupo de pessoas e os envia uma mensagem, você está enviando uma mensagem multicast.
BROADCAST		Uma mensagem é enviada para todos os destinos. Grosso modo, quando você cria uma lista de transmissão no Whatsapp com todos os seus contatos e os envia uma mensagem, você está enviando uma mensagem broadcast.

CLASSIFICAÇÃO DE REDES: QUANTO À DIMENSÃO

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

CLASSIFICAÇÃO DE REDES: QUANTO À ARQUITETURA

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

CLASSIFICAÇÃO DE REDES: QUANTO À TOPOLOGIA

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

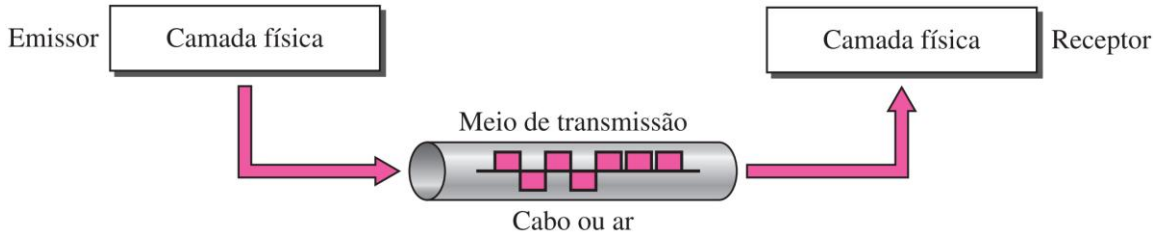
TIPO	REPRESENTAÇÃO	DESCRIÇÃO
BARRAMENTO (BUS)		Todas as estações ficam ligadas ao mesmo meio de transmissão, isto é, um único cabo (chamado backbone) em que os nós se ligam através de conectores. Há maior facilidade na instalação e economia de cabeamento, mas não há isolamento de falhas – uma ruptura no cabo implica a interrupção da comunicação.
ANEL (RING)		Cada dispositivo possui uma conexão ponto-a-ponto com outros dois dispositivos conectados lado a lado, e fazendo uso de uma comunicação com transmissão unidirecional (simplex). Nesse caso, a mensagem circula o anel, sendo regenerada e retransmitida a cada nó, passando pelo dispositivo de destino que copia a informação enviada, até retornar ao emissor original. Nesse momento, o link é liberado para que possa ser utilizado pelo nó seguinte.

ESTRELA (STAR)		As estações estão ligadas a um nó central controlador, pelo qual passam todas as mensagens, não havendo tráfego direto entre os dispositivos. O enlace entre estações e o nó central é Ponto-a-Ponto. É a topologia mais usada atualmente por facilitar a adição de novas estações e a identificação ou isolamento de falhas, em que – se uma conexão se romper – não afetará a comunicação de outras estações.
MALHA (MESH)		Cada estação possui um link ponto a ponto dedicado geralmente com transmissão bidirecional (full duplex) entre cada uma das demais estações. Em outras palavras, todos os computadores estão interligados entre si, de modo que caso haja uma ruptura em algum cabo, não cai a rede inteira, somente o nó conectado a esse cabo.

TOPOLOGIA FÍSICA	DIREÇÃO DE TRANSMISSÃO	TIPO DE ENLACE	MODOS DE TRANSMISSÃO
BARRAMENTO	Half-Duplex	Multiponto	Broadcast
ANEL	Simplex	Ponto-a-Ponto	Broadcast
ESTRELA	Half-Duplex, se usar Hub; caso contrário Full-Duplex	Ponto-a-Ponto	Broadcast, se usar Hub; caso contrário, Unicast, Multicast ou Broadcast
MALHA	Depende	Ponto-a-Ponto	Unicast, Multicast ou Broadcast

MEIOS DE TRANSMISSÃO

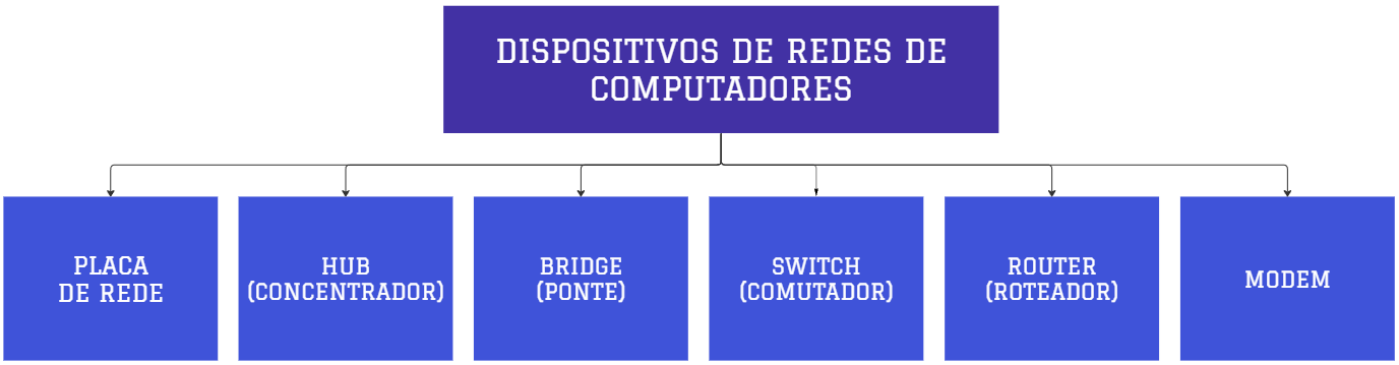
TIPO DE MEIO	DESCRIÇÃO
GUIADO	Trata-se da transmissão por cabos ou fios de cobre, onde os dados transmitidos são convertidos em sinais elétricos que propagam pelo material condutor. Exemplo: cabos coaxiais, cabos de par traçado, fibra óptica, entre outros.
NÃO-GUIADO	Trata-se da transmissão por irradiação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

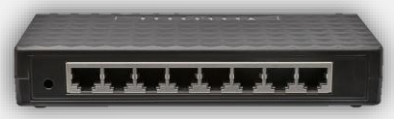


TIPO	REPRESENTAÇÃO	DESCRIÇÃO
CABO COAXIAL		Consiste em um fio central de cobre, envolvido por uma blindagem metálica. Isolantes de plástico flexível separam os condutores internos e externos e outras camadas do revestimento que cobrem a malha externa. Esse meio de transmissão é mais barato, relativamente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

CABO DE PAR TRANÇADO		Consiste de quatro pares de fios trançados blindados ou não, e envolto de um revestimento externo flexível. Eles são trançados para diminuir a interferência eletromagnética externa e interna – quanto mais giros, maior a atenuação. Este é o cabo mais utilizado atualmente por ser o mais barato de todos e ser bastante flexível. Esse cabo cobre distâncias menores que o cabo coaxial e utiliza um conector chamado RJ-45 (Memorizem!).
CABO DE FIBRA ÓPTICA		Consiste em uma Casca e um Núcleo (de vidro) para transmissão de luz. Possui capacidade de transmissão virtualmente infinita, é imune a interferências eletromagnéticas e consegue ligar distâncias maiores sem a necessidade de repetidores. Como desvantagens, podemos dizer que é incapaz de fazer curvas acentuadas, além de ter um custo de instalação e manutenção muito alto em relação ao par trançado. Há dois tipos de fibra: Monomodo e Multimodo.

EQUIPAMENTOS DE REDES



PLACA DE REDE	HUB (CONCENTRADOR)	BRIDGE (PONTE)
		
Equipamento de rede de comunicação bidirecional (entrada e saída de dados) conectado à placa-mãe do computador. Toda placa de rede possui um número identificador chamado Endereço MAC (48 Bits).	Dispositivo de rede capaz de aumentar o alcance de uma rede local por meio da regeneração de sinais. É capaz de trabalhar apenas com broadcast, isto é, ao receber um pacote de dados, distribui para todas as máquinas da rede.	Equipamento capaz de separar uma rede em segmentos menores, reduzindo as chances de colisões quando várias máquinas desejam transmitir dados ao mesmo tempo. São dispositivos capazes de enviar dados para máquinas específicas.
SWITCH (COMUTADOR)	**ROUTER (ROTEADOR)**	**MODEM**

		
Equipamento semelhante às Bridges, no entanto possuem mais portas. Em contraste com hubs, são capazes de transmitir dados para máquinas específicas (unicast ou multicast). Por segmentarem a rede, reduzem as colisões e diminuem o fluxo de informações.	Equipamento que permite interligar redes distintas e são capazes de escolher as melhores rotas para transmissão de pacotes de dados. É responsável por interligar dispositivos de uma rede local (Ex: Computador, Notebook, Smartphone, Impressora, etc) à internet.	Equipamento capaz de converter sinais digitais em sinais analógicos e vice-versa, em geral por meio de uma linha telefônica. Os três modelos principais são: Acesso Discado; Modem ADSL; e Cable Modem.

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

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

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

SWITCHES	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede projetado para encaminhar pacotes de dados com base nos Endereços MAC (Media Access Control).
CAMADA OSI	Camada 2 (Enlace).
VANTAGENS	Rápido encaminhamento de pacotes; reduz colisões na rede; segmenta o tráfego da rede em diferentes portas; suporta redes com fio e sem fio; melhora o desempenho da rede.
DESVANTAGENS	Mais caro do que um hub; requer configuração e gerenciamento adequados; pode ter uma curva de aprendizado para administradores de rede.

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

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

PADRÕES DE REDES

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

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

PADRÕES DE REDES: 802.3

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

EVOLUÇÃO DOS PADRÕES ETHERNET

PADRÃO (CABO DE PAR TRANÇADO)	PADRÃO – TAXA MÁXIMA DE TRANSMISSÃO
Ethernet	10BASE-T / 10 Mbps
Fast Ethernet	100BASE-T / 100 Mbps
Gigabit Ethernet	1000BASE-T / 1000 Mbps
10G Ethernet	10GBASE-T / 10000 Mbps

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

PADRÕES DE REDES: 802.5

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

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

CARACTERÍSTICA	PADRÃO TOKEN RING	PADRÃO ETHERNET
TOPOLOGIA	Usa uma topologia em anel, onde os dispositivos são conectados em círculo e os dados são transmitidos em sequência – um dispositivo após o outro.	Usa uma topologia em estrela ou em barramento. Os dispositivos são conectados a um hub ou switch central.
DESEMPENHO	Oferece um desempenho consistente devido à ausência de colisões de dados. A largura de banda é dividida igualmente entre os dispositivos no anel.	Pode ter colisões de dados, especialmente em redes ocupadas. A largura de banda é compartilhada entre todos os dispositivos na rede.
CUSTO	Geralmente é mais caro devido ao hardware específico necessário, como conectores de cabo MAU (*Media Access Unit*).	Geralmente é mais econômico, pois o hardware é amplamente disponível e menos caro.

IMPLEMENTAÇÃO	Requer configuração mais complexa, como a definição de endereços de estação e prioridades de token.	É mais fácil de implementar, com menos requisitos de configuração.
ESCALABILIDADE	Pode ser menos flexível para adicionar ou remover dispositivos sem interromper a rede.	É escalável e permite adicionar dispositivos com facilidade, especialmente em redes comutadas.
POPULARIDADE	Foi popular nas décadas de 1980 e 1990, mas agora é menos comum, pois a Ethernet se tornou dominante.	É a tecnologia de rede mais amplamente usada e suportada, com constante evolução.

PADRÕES DE REDES: 802.11

PADRÃO WIRELESS (IEEE 802.11)

Arquitetura de conexão de redes locais sem fio que define um conjunto de padrões de transmissão e codificação para comunicações não cabeadas.

CARACTERÍSTICA	MODO DE OPERAÇÃO AD-HOC	MODO DE OPERAÇÃO INFRAESTRUTURA
DESCRIÇÃO	Comunicação direta entre equipamentos e válida somente naquele momento, conexão temporária, apresentando alcance reduzido (Ex: 5m).	Comunicação que faz uso de equipamento para centralizar fluxo da informação na WLAN (Ex: Access Point ou Hotspot) e permite um alcance maior (Ex: 500m).
TOPOLOGIA DE REDE	Tipo de topologia de malha, onde cada dispositivo se conecta diretamente a outros dispositivos na rede.	Os dispositivos se conectam a um ponto de acesso central, como um roteador, que age como intermediário para encaminhar o tráfego.
CONFIGURAÇÃO DE REDE	Configurada sem a necessidade de um ponto de acesso central. Os dispositivos podem se comunicar diretamente uns com os outros.	Requer um ponto de acesso central (como um roteador) para gerenciar e encaminhar o tráfego na rede.
FLEXIBILIDADE	Mais flexível e útil em cenários onde não há acesso a uma infraestrutura de rede. Pode ser configurada rapidamente para conexões ponto a ponto.	Menos flexível em termos de implantação, pois depende de um ponto de acesso central. Ideal para redes com vários dispositivos em um único local.
ESCALABILIDADE	Menos escalável para grandes redes devido à complexidade de gerenciar muitas conexões ponto a ponto.	Mais escalável para redes maiores, pois o ponto de acesso central gerencia eficientemente as conexões.
SEGURANÇA	Geralmente menos segura, pois não existe um ponto de controle central. As comunicações podem ser vulneráveis a ataques.	Mais segura, pois o ponto de acesso central pode implementar medidas de segurança, como criptografia e autenticação, em nome de todos os dispositivos.
EXEMPLOS DE UTILIZAÇÃO	Redes temporárias de curto prazo, comunicação direta entre dispositivos móveis (por exemplo, compartilhamento de arquivos entre smartphones).	Redes domésticas, redes empresariais, hotspots públicos e ambientes onde múltiplos dispositivos precisam se conectar a uma rede comum.

EVOLUÇÃO DO PADRÃO WI-FI (802.11)

PADRÃO	ANO	NOME	FREQUÊNCIA	TAXA MÁXIMA DE TRANSMISSÃO
IEEE 802.11b	1999	-	2.4 Ghz	11 Mbps
IEEE 802.11a	1999	-	5.0 Ghz	54 Mbps
IEEE 802.11g	2003	WI-FI 3	2.4 Ghz	54 Mbps
IEEE 802.11n	2009	WI-FI 4	2.4 / 5.0 Ghz	Até 600 Mbps
IEEE 802.11ac	2014	WI-FI 5	5.0 Ghz	Até 6,9Gbps
IEEE 802.11ax	2019	WI-FI 6	2.4 / 5.0 Ghz	Até 9,6Gbps
IEEE 802.11ax (E)	2021	WI-FI 6E	2.4 / 5.0 / 6.0 Ghz	Até 9,6Gbps
IEEE 802.11be	2025	WI-FI 7	2.4 / 5.0 / 6.0 Ghz	> 40Gbps

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

PADRÕES DE REDES: 802.15

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

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

VANTAGENS DO PADRÃO BLUETOOTH	DESVANTAGENS DO PADRÃO BLUETOOTH
O padrão IEEE 802.15 é projetado para dispositivos de baixo consumo de energia, adequados para baterias.	As redes IEEE 802.15 têm alcance limitado, geralmente cobrindo apenas algumas dezenas de metros.
O padrão é ideal para comunicações de curto alcance, como sensores e dispositivos IoT em uma área próxima.	A largura de banda é limitada, o que a torna inadequada para aplicações que requerem alta taxa de transferência.
Permite a criação de redes de malha, onde dispositivos podem rotear dados entre si, aumentando a cobertura.	Pode ser afetada por interferências de outras redes sem fio e dispositivos, especialmente em ambientes lotados.

Usado em aplicações como IoT, sensores sem fio, automação residencial, dispositivos médicos e muito mais.	Não é a melhor opção para redes de grande escala, devido ao seu alcance limitado e limitações de largura de banda.
Substitui a necessidade de cabos em ambientes onde a conectividade com fio não é prática ou possível.	A segurança é uma preocupação, pois dispositivos dentro do alcance de uma rede IEEE 802.15 podem acessá-la.

PADRÕES DE REDES: 802.16

PADRÃO WIMAX (IEEE 802.16)
O Padrão WiMAX especifica um padrão sem fio de alta velocidade para Redes Metropolitanas (WMAN), criado por um consórcio de empresas para promover interoperabilidade entre equipamentos. Seu raio de comunicação com o ponto de acesso pode alcançar até cerca de 40 km, sendo recomendável para prover acesso à internet banda larga a empresas e residências em que o acesso ADSL ou HFC se torna inviável por questões geográficas.

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

INTERNET

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

COMUTAÇÃO POR CIRCUITOS	DESCRIÇÃO
CONEXÃO	Estabelecida antes da transmissão de dados.
EXCLUSIVIDADE	Circuito dedicado durante toda a comunicação.
EFICIÊNCIA	Pode ser baixa, pois a linha fica ocupada mesmo em silêncio.
LATÊNCIA	Baixa, ideal para voz em tempo real.
ROBUSTEZ	Menos flexível, difícil de redirecionar em caso de falha.
EXEMPLOS	Ligações telefônicas tradicionais.

COMUTAÇÃO POR PACOTES	DESCRIÇÃO
DIVISÃO DE DADOS	Dados são divididos em pacotes menores.

ROTAS	Cada pacote pode seguir um caminho diferente.
EFICIÊNCIA	Uso mais dinâmico dos recursos da rede.
REORGANIZAÇÃO	Pacotes são remontados na ordem correta no destino.
ROBUSTEZ	Se um caminho falhar, os pacotes são redirecionados.
UTILIZAÇÃO	Base das redes modernas (Internet, VPNs, etc).

VANTAGENS DA COMUTAÇÃO POR PACOTES	DESVANTAGENS DA COMUTAÇÃO POR PACOTES
Maior eficiência no uso da rede	Pode haver atraso (latência) na entrega dos pacotes
Melhor tolerância a falhas e congestionamentos	Pacotes podem chegar fora de ordem
Reduz custos de transmissão	Necessita de protocolos de controle para reorganizar pacotes
Suporte para múltiplos tipos de comunicação simultânea	Exige maior capacidade de processamento dos dispositivos

SERVIÇOS DA INTERNET	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. 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.

COMPONENTES DA WEB	DESCRIÇÃO
HIPERTEXTO	A Web é baseada em documentos que contêm links (hiperlinks) para outros documentos relacionados. Isso permite que os usuários naveguem de uma página para outra, seguindo os links.
URL	Cada documento ou recurso na Web é identificado por um URL exclusivo, que é um endereço usado para acessar o recurso em um navegador.
NAVEGADORES DA WEB	São aplicativos que permitem aos usuários visualizar e interagir com documentos da Web. Exemplos populares de navegadores incluem o Google Chrome, Mozilla Firefox, Microsoft Edge e Safari.
PROTOCOLOS DE COMUNICAÇÃO	A Web utiliza protocolos de comunicação, como HTTP (Hypertext Transfer Protocol) e HTTPS (HTTP Secure), para transferir dados entre navegadores e servidores web.
SERVIDORES WEB	São computadores que hospedam documentos e recursos da Web. Eles respondem às solicitações dos navegadores e fornecem os conteúdos solicitados.

PÁGINAS DA WEB	São documentos criados usando linguagens de marcação, como HTML (Hypertext Markup Language). As páginas da web podem conter texto, imagens, links e outros elementos interativos.
MOTORES DE BUSCA	São ferramentas que ajudam os usuários a encontrar informações na Web, indexando e classificando páginas da web com base em palavras-chave.

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

DEEP WEB E DARK WEB

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

INTERNET DAS COISAS

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

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

TECNOLOGIAS DE IOT	DESCRIÇÃO
WI-FI (802.11)	Trata-se de uma das tecnologias de comunicação sem fio mais amplamente utilizadas e oferece alta largura de banda. É adequado para dispositivos que têm acesso a redes locais de alta velocidade e energia suficiente.
BLUETOOTH (802.15)	Trata-se de uma tecnologia de comunicação sem fio de curto alcance, adequada para dispositivos pessoais, como fones de ouvido sem fio e dispositivos vestíveis. O Bluetooth Low Energy (BLE) é uma variante de baixo consumo de energia.
ZIGBEE	Trata-se de um padrão de comunicação sem fio de baixa potência projetado para redes de sensores e dispositivos IoT em ambientes domésticos e industriais.

VANTAGENS DO IOT	DESVANTAGENS DO IOT
Varejistas podem fornecer bônus de fidelidade para clientes preferenciais.	A dependência de compras online pode custar empregos.
As cidades podem avaliar as necessidades futuras de transporte.	Os varejistas podem saber tudo o que você está comprando.
Indivíduos podem reduzir os custos de energia e dos sistemas de aquecimento residenciais.	Os indivíduos podem receber mais e-mails de spam.
Fabricantes podem reduzir a inatividade prevendo as necessidades de manutenção dos equipamentos.	Uma falha da rede pode ser catastrófica.
Os governos podem monitorar o ambiente.	As empresas que criam dispositivos vestíveis têm muitas informações pessoais sobre os usuários.

TECNOLOGIAS DE ACESSO

TECNOLOGIAS DE ACESSO À INTERNET
Referem-se aos métodos e infraestruturas utilizados para conectar dispositivos, como computadores, smartphones e outros equipamentos, à Internet. Essas tecnologias permitem que os dispositivos acessem os

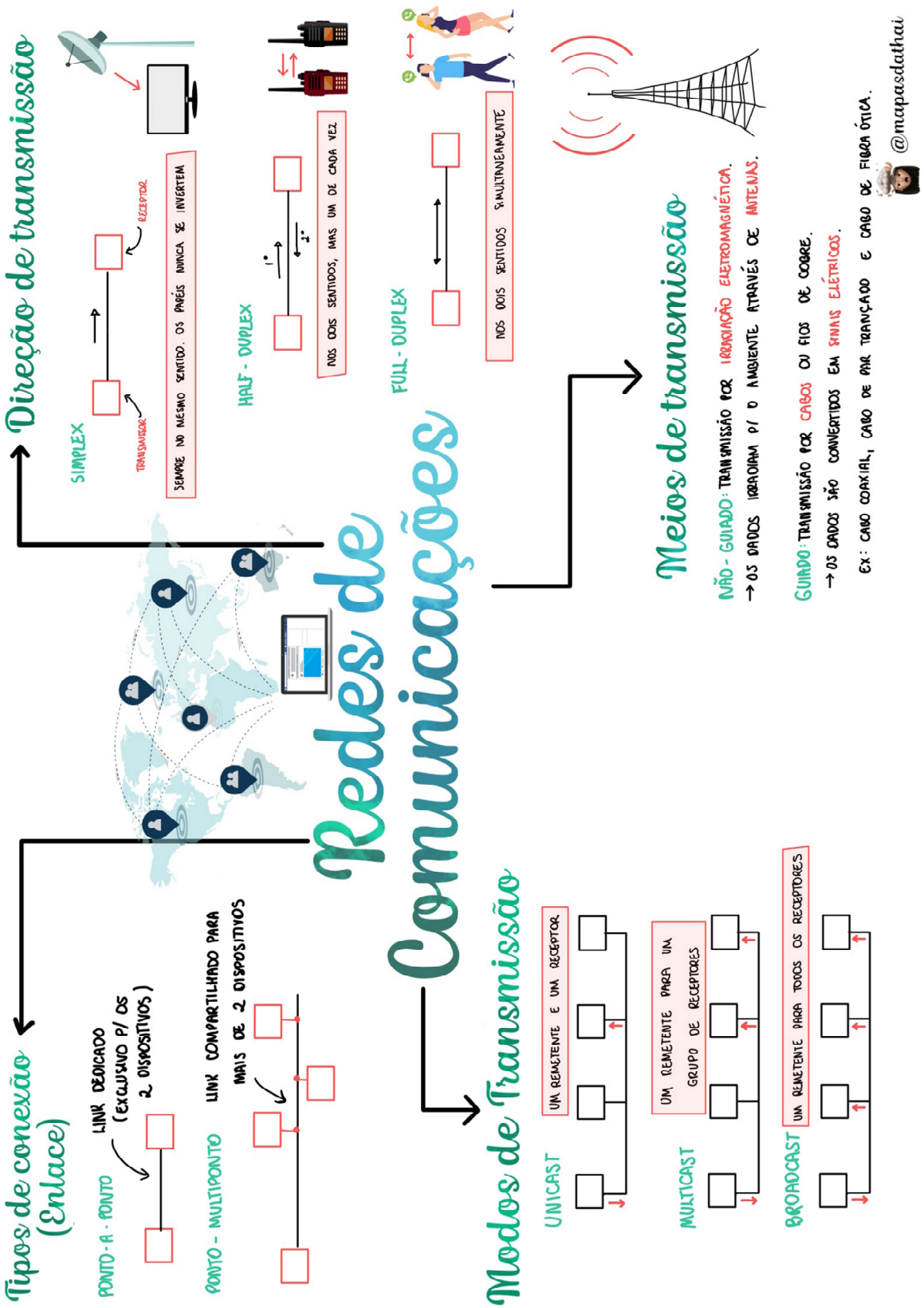
serviços e recursos disponíveis na World Wide Web e em outros serviços online. Existem várias tecnologias de acesso à Internet (Ex: Dial-Up, ADSL, HFC, Fibra Óptica, PLC, Rádio, Satélite e Telefonia Móvel), e a escolha depende das necessidades e da disponibilidade em uma determinada região.

NÍVEIS DE ISP	DESCRIÇÃO
ISP NÍVEL 1	São os provedores de backbone mundial. Não precisam comprar trânsito IP de ninguém. Se conectam diretamente entre si (acordos de peering). Apresentam características como: cobertura global; alta capacidade de infraestrutura própria; e conectam redes sem custo de trânsito (peering). ISP Nível 1 são como aviões de grande porte que fazem voos internacionais e controlam as principais rotas aéreas globais (Exemplos: AT&T, CenturyLink (Lumen), NTT, Telia)
ISP NÍVEL 2	Compram acesso de ISPs Nível 1 e fazem peering com outros ISPs Nível 2. Atendem a grandes regiões, países ou continentes. Apresentam características como: têm alguma infraestrutura; dependem parcialmente de Nível 1; buscam acordos de peering para reduzir custos. ISP Nível 2 são como companhias nacionais que compram o direito de usar parte dessas rotas para conectar cidades e países (Exemplos: Embratel, Vivo, TIM, Claro)
ISP NÍVEL 3	São provedores locais ou regionais. Compram completamente o acesso à Internet de ISPs Nível 2 ou Nível 1. Apresentam características como: pouco ou nenhuma infraestrutura própria; conexão limitada a clientes locais; dependem totalmente de ISPs superiores. ISP Nível 3 são como empresas de transporte local, que compram serviços das grandes companhias para levar passageiros até bairros e pequenas localidades (Exemplos: provedores de bairro, pequenos provedores locais).

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

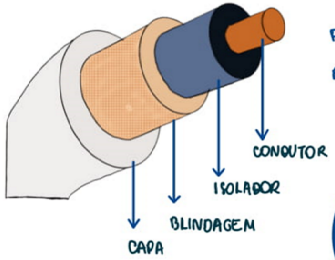
PARA MAIS DICAS: WWW.INSTAGRAM.COM/PROFESSORDIEGOCARVALHO

MAPA MENTAL

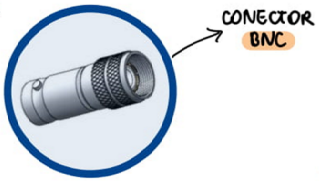

Redes de Comunicações
Direção de transmissão
SIMPLEX
TRANSMISSOR
RECEPTOR
SEMPRE NO MESMO SENTIDO. OS PAPÉIS NUNCA SE INVERTEM
HALF - DUPLEX
NOS DOIS SENTIDOS, MAS UM DE CADA VEZ
FULL - DUPLEX
NOS DOIS SENTIDOS SIMULTANEAMENTE
Meios de transmissão
NÃO - GUIADO: TRANSMISSÃO POR IRRADIAÇÃO ELETROMAGNÉTICA.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

Meios de Transmissão Guiados

Cabo coaxial



FIO METAL DE COBRE, ENVOLVIDO POR UMA BLINDAGEM METÁLICA.

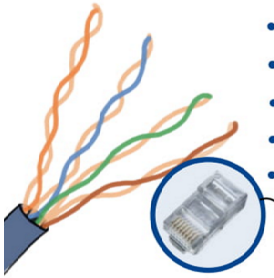


- MAIS BARATO
- RELATIVAMENTE FLEXÍVEL
- MUITO RESISTENTE (NÃO IMUNE) À INTERFERÊNCIA ELETROMAGNÉTICA
  - GRAÇAS À MALHA/CAPA DE PROTEÇÃO
- COBRE DISTÂNCIAS MAIORES
- TAXA DE TRANSMISSÃO MENOR
- LARGURA DE BANDA MAIOR

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

Cabo de par trançado

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



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

CONECTOR RJ-45

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

Cabo de Fibra Ótica

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

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

FIBRA MULTIMODO



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

FIBRA MONOMODO



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



@mapasdathai

Tipos de Rede



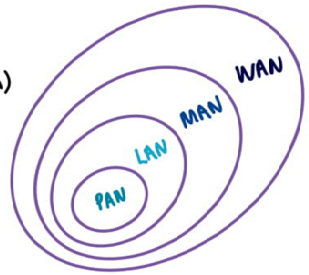
Por Dimensão

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

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

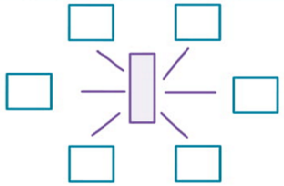
MAN: REDE ENTRE UMA MATRIZ E FILIAIS EM UMA MESMA CIDADE

WAN: REDE ENTRE CIDADES, PAÍSES OU CONTINENTES



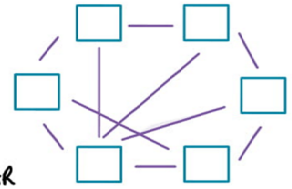
Por Arquitetuta/Forma de Interação

REDE CLIENTE-SERVIDOR



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

REDE PONTO-A-PONTO



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

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

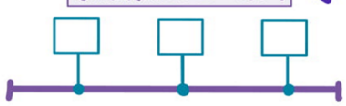


@mapasdathai

Tipos de Rede

Por Topologia/Layout

BARRAMENTO (BUS)

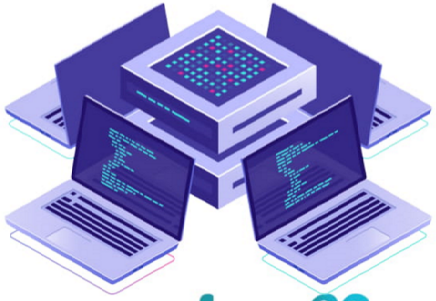


- TODAS AS ESTAÇÕES SÃO LIGADAS A UM MESMO MEIO DE TRANSMISSÃO (BACKBONES)
- CONEXÃO PONTO-MULTIPONTO
- HALF-DUPLEX (SINAL EM AMBAS AS DIREÇÕES)
- BROADCAST (SINAL RECEBIDO POR TODOS OS NÓS)

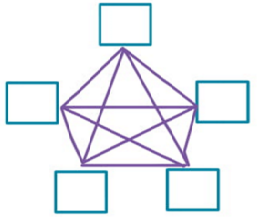
→ VANTAGENS:
- FÁCIL E BARATO

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





MALHA (MESH)

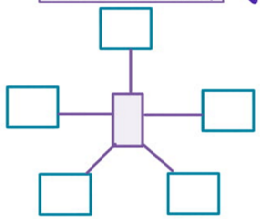


- TODAS AS ESTAÇÕES ESTÃO LIGADAS ENTRE SI
- LINKS PONTO-A-PONTO, DEDICADOS E COM TRANSMISSÃO FULL-DUPLEX

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

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

ESTRELA (STAR)

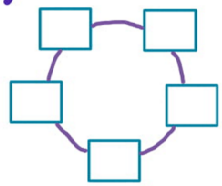


- AS ESTAÇÕES ESTÃO LIGADAS POR UMA CONEXÃO PONTO-A-PONTO A UM NÓ CENTRAL CONTROLADOR, PELO QUAL PASSAM TODAS AS INFORMAÇÕES
- NÃO HÁ TRAFEGO DIRETO ENTRE ESTAÇÕES

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

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

ANEL (RING)



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

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

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



@mapasdathai

Equipamentos de Redes

NIC (PLACA DE REDE)



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

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

SWITCH (COMUTADOR)



BRIDGE MULTIPORTAS

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



BRIDGE (PONTE)

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

HUB (CONCENTRADOR)



CONCENTRA O TRÁFEGO DE REDE QUE PROVÉM DE VÁRIOS DISPOSITIVOS

REGENERA O SINAL E DEPOIS ENVIA PARA TODAS AS PORTAS

BROADCAST (FOFOQUEIRO)

HALF - DUPLEX

TOPOLOGIA FÍSICA: ESTRELA

TOPOLOGIA LÓGICA: BARRAMENTO



MODEM (MODULADOR/DEMODULADOR)

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

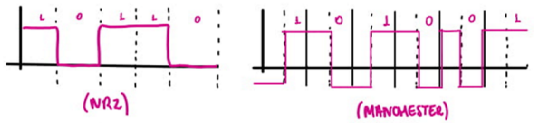
MODEM DIAL-UP - ACESSO DISCADO

MODEM ADSL - ACESSO A BANDA LARGA POR CABO OU WIRELESS

CABLE MODEM - CABOS COAXIAIS / NÃO USA A LINHA TELEFÔNICA

TIPOS DE SINAIS

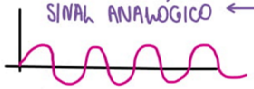
SINAL DIGITAL



(NRZ) (MANCHESTER)

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

SINAL ANALÓGICO



- NÚMERO INFINITO DE VALORES
- MAIS NÍVEIS DE INTENSIDADE

ROUTER (ROTEADOR)



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

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

ACCESS POINT (PONTO DE ACESSO)



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

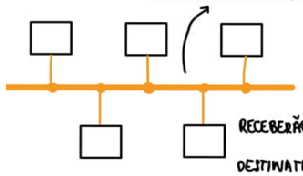


@mapasdathai

Padrões de Redes

Ethernet

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

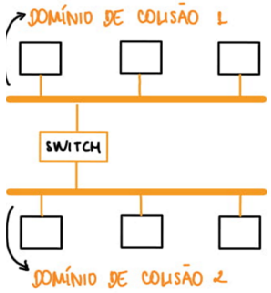


CSMA - CARRIER SYSTEM MULTIPLE ACCESS: TODOS OS COMPUTADORES RECEBERÃO A MENSAGEM, MAS SÓ O DESTINATÁRIO IRÁ PROCESSÁ-LA.

DESVANTAGEM: TRÁFEGO ALTO PODE GERAR COLISÃO = MENSAGENS ININTELIGÍVEIS

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

QUANDO A REDE É MUITO GRANDE:



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

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

Wireless

- SUA CONEXÃO UTILIZA ONDAS DE RÁDIO

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

OBSERVAÇÕES:

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



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

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

Bluetooth

OBJETIVO: INTEGRAR EQUIPAMENTOS PERIFÉRICOS NA WPAN

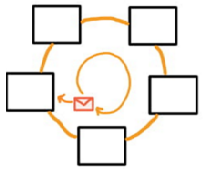
- REDE DE BAIXO CUSTO
- CURTO ALCANCE
- BAIXAS TAXAS DE TRANSMISSÃO
- FAIXA DE 2.4 GHz
- CONECTA ATÉ 7 DISPOSITIVOS
- ARQUITETURA MASTER / SLAVE
  - MESTRE: PODE SE CONECTAR A VÁRIOS ESCRAVOS
  - ESCRAVO: SE CONECTA A APENAS UM MESTRE



WiMAX

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

Token Ring



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



@mapasdathai

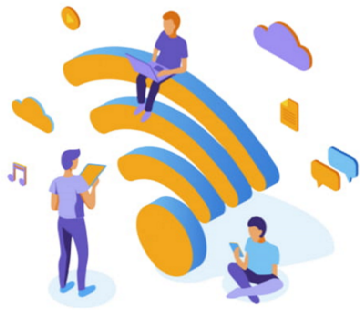
Internet

Arpanet

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

World Wide Web (WWW)

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



Correio Eletrônico

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

Acesso Remoto

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

Comutação por circuito

- UTILIZADA NA TELEFONIA
- A INFORMAÇÃO DE VOZ SEMPRE PERCORRE A MESMA ROTA E SEMPRE CHEGA NA MESMA ORDEM
- FASES:
  1. ESTABELECIMENTO DA CONEXÃO
  2. TRANSFERÊNCIA DE DADOS
  3. ENCERRAMENTO DA CONEXÃO

- É INVIÁVEL P/ A INTERNET PORQUE DESPERDIÇARIA RECURSOS POR FECHAR UMA CONEXÃO DEDICADA AINDA QUE NÃO ESTEJA HAVENDO COMUNICAÇÃO E PORQUE SÓ SERIA POSSÍVEL ACESSAR UM SITE POR VEZ.

Comutação por pacotes

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

Protocolos TCP/IP

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

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

Transferência de Arquivos

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

PROTOCOLOS: EM GERAL: FTP E P2P



@mapasdathai

QUESTÕES COMENTADAS – CESPE

1. **(CESPE / ANTT – 2024)** N, hacker mundialmente conhecido por sua atuação na Deep Web e na Dark Web e por cometer, sem deixar vestígios, crimes virtuais e atentar contra a cibersegurança de diversos órgãos públicos em todo o mundo, acessou um programa computacional de determinado ente federativo brasileiro que tem por objeto o estudo jurimétrico de infrações e acidentes trânsito e obteve os dados de inúmeros condutores. De posse desses dados, acessou os softwares dos veículos identificados em tal programa como detentores de tecnologia de condução semiautônoma e os fraudou, com o intuito de gerar acidentes de trânsito. N também instalou, no programa computacional, uma ferramenta de inteligência artificial que se vale de algoritmos para automaticamente gerar uma série de notificações de infração de trânsito a inúmeros condutores.

   Deep Web e Dark Web são expressões sinônimas utilizadas para descrever uma parte da Internet que, em contraposição à chamada Surface Web, é acessada para a realização de atividades ilegais.

Comentários:

Deep Web e Dark Web não são expressões sinônimas. A Deep Web inclui conteúdos não indexados por motores de busca, como e-mails e bancos de dados, a maioria legítimos. Já a Dark Web é um subconjunto da Deep Web, acessado por navegadores específicos, que pode abrigar atividades ilegais, mas não exclusivamente.

Gabarito: Errado

---

2. **(CESPE / CNPQ – 2024)** Para que um computador possa se conectar à Internet, é essencial que ele esteja equipado com um hardware de comunicação, denominado placa de rede, que pode ser um chipset integrado à placa mãe do computador.

Comentários:

A placa de rede é essencial para a conexão de um computador à Internet, pois permite a comunicação com outros dispositivos por meio de redes cabeadas (Ethernet) ou sem fio (Wi-Fi). Essa placa pode ser um dispositivo dedicado ou um chipset integrado à placa-mãe.

Gabarito: Correto

---

3. **(CESPE / TJ-ES – 2023)** Com base nas propriedades de rede exibidas na imagem a seguir, extraídas de um computador com Windows 10 conectado à rede por meio de apenas um adaptador de rede, é correto afirmar que esse computador poderá conectar-se a uma rede com velocidade de até 1.000 Mbps.



Comentários:

A imagem mostra as propriedades da conexão Ethernet do computador, destacando que a "Velocidade da conexão (Recepção/Transmissão)" é de 1000/1000 Mbps. Isso indica que a interface de rede suporta velocidades de até 1 Gbps (1000 Mbps), desde que a infraestrutura da rede (como switch e cabos) também suporte essa velocidade.

Gabarito: Correto

---

4. **(CESPE / CBM-TO – 2023)** Determinado usuário verificou que seu roteador wi-fi transmite dados nas faixas de frequência de 2,4 GHz e 5 GHz, respectivamente.

   A partir dessa situação hipotética, assinale a opção correta.

   a) O roteador wi-fi permite que as redes sejam utilizadas, exclusivamente, de maneira não concorrente.

   b) A frequência de rede de 5 GHz, por padrão, é mais veloz que a frequência de rede de 2,4 GHz, porém o alcance da primeira é menor que o da segunda.

   c) A rede com frequência nominal de 2,4 GHz é imune a interferência de sinal de rádio, pois a imunidade ao ruído é diretamente proporcional à velocidade de transferência de dados.

   d) O roteador wi-fi permite que a velocidade de transmissão das duas frequências sejam somadas, o que resulta em uma rede com frequência nominal de 7,4 GHz e com alcance ainda menor que o da rede com frequência nominal de 5 GHz.

Comentários:

(a) Errado. Roteadores Wi-Fi que operam nas faixas de 2,4 GHz e 5 GHz geralmente permitem que dispositivos se conectem a ambas as redes simultaneamente, não exigindo o uso exclusivo e não concorrente de uma ou outra.

(b) Correto. A frequência de 5 GHz é geralmente mais rápida e tem menos interferência que a de 2,4 GHz, mas seu alcance é menor, o que significa que o sinal não viaja tão longe ou não penetra tão bem em obstáculos como paredes.

(c) Errado. A rede de 2,4 GHz não é imune a interferências de sinal de rádio. Na verdade, essa banda é mais suscetível a interferências de outros dispositivos, como micro-ondas e telefones sem fio, do que a banda de 5 GHz.

(d) Errado. O roteador não soma as velocidades de transmissão das duas faixas de frequência. Cada banda opera independentemente, e a velocidade combinada não se traduz em uma frequência nominal de 7,4 GHz.

No entanto, a questão foi anulada pela banca com a seguinte justificativa: "*A questão apresenta mais de uma opção correta, fato que prejudicou seu julgamento objetivo*".

Gabarito: Anulada

---

5. **(CESPE / TCE-RJ – 2022)** Diferentemente das bridges, os repetidores são dispositivos capazes de reconhecer e examinar os quadros da camada de enlace.

Comentários:

Na verdade, o correto seria:

"Diferentemente dos repetidores, as bridges são dispositivos capazes de reconhecer e examinar os quadros da camada de enlace".

Gabarito: Errado

---

6. **(CESPE / TCE-RJ – 2022)** No padrão Gigabit Ethernet, tanto no modo de operação half-duplex quanto no modo full-duplex, o uso do protocolo CSMA/CD para evitar colisões é dispensável, em razão da extensão de portadora, uma característica voltada à prevenção de colisões incluída originalmente nas definições do padrão.

Comentários:

No modo full-duplex, é realmente dispensável já que não existe possibilidade de colisão. No modo half-duplex, não é dispensável justamente porque existe a possibilidade de colisão.

Gabarito: Errado

---

7. **(CESPE / SECONT-ES – 2022)** As mensagens enviadas na Internet denominam-se pacotes, e os comutadores de pacotes são denominados roteadores ou switches.

Comentários:

As mensagens realmente podem ser chamadas de pacotes no contexto de internet e, de fato, roteadores e switches (de camada 3) são considerados comutadores de pacotes. De toda forma, questão com uma redação bem esquisita...

Gabarito: Correto

---

8. **(CESPE / PG-DF – 2021)** Uma rede formada por dispositivos bluetooth é exemplo de PAN (Personal Area Network).

Comentários:

Uma rede formada por dispositivos Bluetooth é, de fato, um exemplo de PAN. Essas são redes de curto alcance projetadas para conectar dispositivos pessoais, como smartphones, tablets, laptops, fones de ouvido Bluetooth e outros dispositivos portáteis em um alcance próximo.

Gabarito: Correto

---

9. **(CESPE / TELEBRÁS - 2021)** O único requisito obrigatório ao se projetar uma rede de computadores é realizar um levantamento da quantidade de computadores a serem conectados à rede.

Comentários:

Para se projetar uma rede, há muitos parâmetros a serem observados, entre eles: a quantidade de computadores, o cabeamento, os equipamentos de rede que serão utilizados, a extensão da rede, entre vários outros requisitos.

Gabarito: Errado

---

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

Comentários:

A rede metropolitana abrange a área de uma metrópole, logo não é da proporção de um país ou continente – essa seria uma WAN (Wide Area Network).

Gabarito: Errado

---

11. (CESPE / PC-AL – 2021) Denomina-se cabo coaxial, em uma rede de comunicação, o tipo de mídia de comunicação que realiza a conexão entre pontos, é imune a ruídos elétricos e é responsável pela transmissão de dados com capacidade de largura de banda muito maior do que os pares trançados.

Comentários:

Está tudo perfeito, com uma exceção: ele é muito resistente, mas não é imune a ruídos elétricos.

Gabarito: Errado

---

12. (CESPE / SEFAZ-CE – 2021) Em uma rede em topologia de barramento, as comunicações de mensagens do tipo difusão são facilitadas porque todos os nós conectados ao barramento são capazes de ouvir todas as transmissões realizadas.

Comentários:

Perfeito... em uma topologia em barramento, comunicações do tipo difusão (broadcast) realmente são ouvidas por todos os nós.

Gabarito: Correto

---

13. (CESPE / Polícia Federal – 2021) Uma LAN (*local área network*) fornece conectividade em tempo integral para os serviços de conexão da Internet.

Comentários:

Uma LAN (Local Area Network) é uma rede de computadores que permite a comunicação entre dispositivos dentro de uma área geográfica limitada, como uma casa, escola, laboratório ou edifício de escritórios. Embora uma LAN possa fornecer conectividade para acessar serviços de internet, não é correto afirmar que sua função é fornecer conectividade em tempo integral para os serviços de conexão da Internet. Uma LAN é projetada para redes locais e não depende de conectividade com a Internet para operar, embora muitas LANs estejam conectadas à Internet para proporcionar acesso aos seus usuários.

Gabarito: Errado

---

14. (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

---

15. (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

---

16. (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

---

17. (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

---

18. (CESPE / Polícia Federal – 2018) As redes de computadores podem ser classificadas, pela sua abrangência, em LAN (Local Area Network), MAN (Metropolitan Area Network), e WAN (Wide Area Network).

Comentários:

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.

As redes de computadores realmente podem ser classificadas em LAN, MAN e WAN. Essa é a classificação tradicional, apesar de nos últimos anos PAN ter ficado cada vez mais comum! Cuidado: não é porque a questão não menciona PAN que a questão está errada!

Gabarito: Correto

---

19. (CESPE / Polícia Federal – 2018) PAN (*Personal Area Network*) são redes de computadores destinadas a ambientes com acesso restrito, seja por limitações físicas ou por definições de segurança.

Comentários:

Definições de Segurança? Não, apenas por limitações físicas – assim como todas as outras classificações quanto à dimensão, tamanho ou área geográfica. *Professor, é uma rede de computadores?* Sim, em sentido genérico, dispositivos são computadores capazes de processar dados.

Gabarito: Errado

---

20. (CESPE / Polícia Federal – 2018) Uma empresa tem unidades físicas localizadas em diferentes capitais do Brasil, cada uma delas com uma rede local, além de uma rede que integra a comunicação entre as unidades. Essa rede de integração facilita a centralização do serviço de email, que é compartilhado para todas as unidades da empresa e outros sistemas de informação.

Se as redes locais das unidades da empresa estiverem interligadas por redes de operadoras de telecomunicação, então elas formarão a WAN (Wide Area Network) da empresa.

Comentários:

Se a empresa possui unidades físicas localizadas em diferentes capitais do Brasil, trata-se de uma Wide Area Network (WAN).

Gabarito: Correto

---

21. (CESPE / Polícia Federal – 2018) A conexão de sistemas como TVs, laptops e telefones celulares à Internet, e também entre si, pode ser realizada com o uso de comutadores (switches) de pacotes, os quais têm como função encaminhar a um de seus enlaces de saída o pacote que está chegando a um de seus enlaces de entrada.

Comentários:

A banca considerou a questão como correta, mas eu discordo! Essa questão foi bastante polêmica! Para mim, a questão erra em afirmar que é possível realizar a conexão de equipamentos à Internet por meio de switches - essa é uma função dos roteadores. Switches, por si só, são incapazes de realizar a conexão de computadores à internet. Existem alguns tipos de switches – chamados Switch Level 3 – que conseguem realizar funções semelhantes às dos roteadores, mas nem mesmo eles são capazes de fazer a conexão com a Internet.

Switches L3 são projetados principalmente para comutação de tráfego dentro de uma LAN, mas têm recursos de roteamento limitados – não sendo ideais para conectar diretamente uma rede local à internet. Embora possam possuir recursos básicos de roteamento, eles geralmente não oferecem funcionalidades avançadas de roteamento exigidas para o encaminhamento de tráfego entre redes, incluindo a Internet (Ex: em geral, não possuem NAT).

Gabarito: Correto

---

22. (CESPE / Polícia Federal – 2018) Uma empresa tem unidades físicas localizadas em diferentes capitais do Brasil, cada uma delas com uma rede local, além de uma rede que integra a comunicação entre as unidades. Essa rede de integração facilita a centralização do serviço de

email, que é compartilhado para todas as unidades da empresa e outros sistemas de informação. Tendo como referência inicial as informações apresentadas, julgue o item subsecutivo.

Em uma rede local que possui a topologia estrela, podem ser utilizados switches para integrar a comunicação entre os computadores.

Comentários:

Perfeito! Na topologia em estrela, os equipamentos são conectados a um nó central concentrador para integrar a comunicação entre os computadores. Em geral, o nó concentrador pode ser um hub ou um switch.

Gabarito: Correto

---

23. (CESPE / Polícia Federal – 2018) Uma das vantagens da rede de computadores com tipologia mesh é a varredura de diversas possibilidades de roteamento para identificar a mais eficiente.

Comentários:

Para mim, essa é mais uma questão que poderia ser anulada. Não existe *tipologia* mesh, mas *topologia* mesh. Ignorando o erro do termo utilizado, a topologia mesh (malha) realmente possui a vantagem de poder varrer diversas possibilidades de roteamento para identificar a mais eficiente. A internet funciona como uma malha, logo pacotes transmitidos entre duas máquinas podem percorrer caminhos distintos até chegar ao destinatário final. Lembrando que – nessa topologia – um nó está conectado a diversos outros, mas isso não significa que todos os nós estarão conectados diretamente a todos os outros.

Gabarito: Correto

---

24. (CESPE / Polícia Federal – 2018) Em redes de comunicação de dados, existem três modos de transmissão: o simplex, em que os dados circulam em apenas um sentido; o half-duplex, em que os dados circulam nos dois sentidos ao mesmo tempo; e o full-duplex, também conhecido por ligação de alternância.

Comentários:

A questão inverteu half-duplex e full-duplex. No primeiro, os dados circulam nos dois sentidos, mas de forma alternada: ambos podem transmitir e receber dados, porém nunca simultaneamente. No segundo, os dados circulam nos dois sentidos ao mesmo tempo.

Gabarito: Errado

---

25. **(CESPE / Polícia Federal – 2018)** Por se tratar de arquitetura ultrapassada e possuir pouco compartilhamento de recursos, redes do tipo cliente/servidor não podem ter mais que 100 clientes conectados ao respectivo servidor.

Comentários:

Pelo contrário, redes do tipo cliente/servidor são as mais utilizadas atualmente no mundo inteiro. Um exemplo clássico desse tipo de rede é a Internet, logo é óbvio que pode haver muito mais que cem clientes conectados ao respectivo servidor.

Gabarito: Errado

---

26. **(CESPE / Polícia Federal – 2018)** Uma empresa tem unidades físicas localizadas em diferentes capitais do Brasil, cada uma delas com uma rede local, além de uma rede que integra a comunicação entre as unidades. Essa rede de integração facilita a centralização do serviço de email, que é compartilhado para todas as unidades da empresa e outros sistemas de informação. Tendo como referência inicial as informações apresentadas, julgue o item subsecutivo.

Para viabilizar a comunicação de dados entre as unidades da empresa, podem ser utilizados serviços de interconexão com roteadores providos por operadoras de telecomunicação.

Comentários:

Perfeito! Podem, sim, ser utilizados roteadores fornecidos por operadoras de telecomunicação para interconectar as redes. Essa é – inclusive – a função principal de um roteador!

Gabarito: Correto

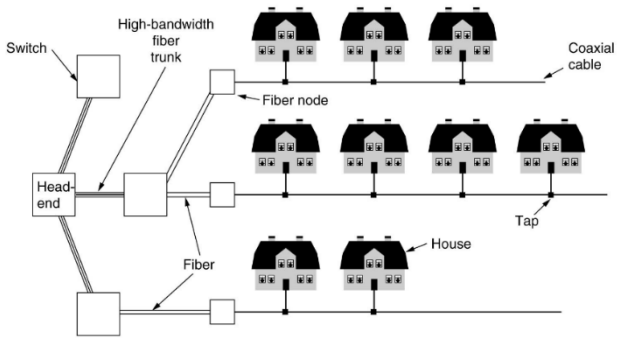
---

27. **(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 sabemos 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

28.(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

29.(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

---

30. **(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

---

31. **(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 MÁXIMA DE TRANSMISSÃO

IEEE 802.11B	2.4 Ghz	11 Mbps
IEEE 802.11A	5.0 Ghz	54 Mbps
IEEE 802.11G	2.4 Ghz	54 Mbps
IEEE 802.11N	2.4 ou 5.0 Ghz	150, 300 até 600 Mbps
IEEE 802.11AC	5.0 Ghz	500 Mbps, 1 Gbps ou +

Gabarito: Letra A

---

32. **(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

---

33. **(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

---

34. **(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

---

35. **(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

---

36. **(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

---

37. **(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

---

38. **(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

39.(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

40.(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: Correto

41.(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

---

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

Gabarito: Errado

---

43. (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

---

44. (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

---

45. (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

---

46. (CESPE / Polícia Federal – 2018) O padrão IEEE 802.11g permite que as redes locais das unidades da empresa operem sem cabeamento estruturado nos ambientes físicos e com velocidade mínima de 200 Mbps.

Comentários:

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

O Padrão IEEE 802.11g é um Padrão Wi-Fi, logo realmente permite que as redes locais das unidades da empresa operem sem cabeamento estruturado nos ambientes físicos, mas a velocidade máxima – conforme podemos ver na tabela – é de 54 Mbps, o que já extrapola a velocidade mínima apresentada pelo enunciado da questão.

Gabarito: Errado

---

47. (CESPE / ABIN – 2018) Redes wi-fi e Bluetooth podem ser utilizadas para IoT, já NFC (Near Field Communication) não atende a demandas de IoT.

Comentários:

Na verdade, podem ser utilizados Wi-fi, Bluetooth e também NFC.

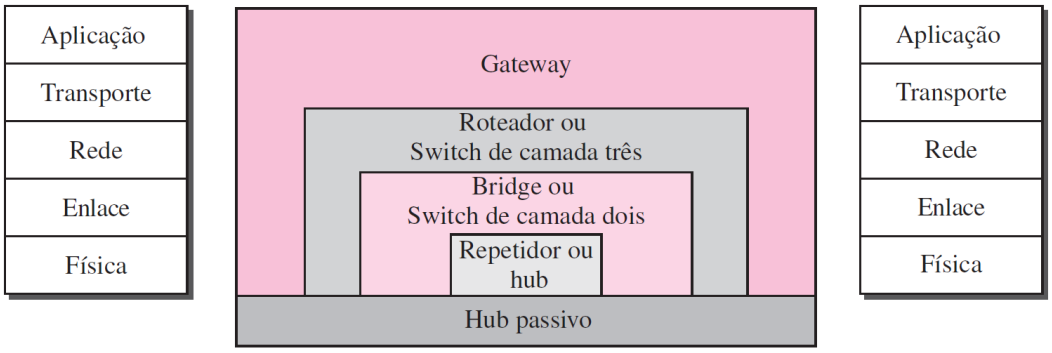
Gabarito: Errado

---

48. (CESPE / TRE-BA – 2017) O dispositivo de rede que opera nas camadas física, de enlace e de rede e que altera os endereços físicos em um pacote é denominado:

a) amplificador.
b) repetidor.
c) bridge.
d) hub.
e) roteador.

Comentários:



O único dispositivo apresentado que opera nas camadas física, de enlace e de rede é o roteador (conforme imagem anterior) – lembrando que ele atua primariamente na camada de rede. Agora a parte interessante: ele realmente altera os endereços físicos em um pacote. *Sério, professor?* Sim! Quando você envia pacotes de um computador para outro, os endereços de rede de origem e destino permanecem fixados e imutáveis.

Em outras palavras, o Endereço IP de origem e o Endereço IP de destino jamais se modificam. No entanto, nós também sabemos que para que um pacote de dados seja transmitido de um dispositivo de origem para um dispositivo de destino, ele geralmente passa por diversos outros roteadores intermediários no meio do caminho para percorrer a melhor rota. Quando ele passa de um roteador para outro, o endereço físico é realmente modificado.

Nós já sabemos que endereço físico é o Endereço MAC! Quando um pacote chega a um roteador, ele verificar o endereço de rede de destino para ver se ele é o destinatário. Caso não seja, ele verifica a tabela de roteamento e manda para o próximo roteador. *Ele faz isso modificando o endereço de rede?* Não, ele faz isso modificando o endereço físico. Dessa forma, a cada hop (pulo) entre roteadores em uma rota, o endereço físico é realmente modificado.

Gabarito: Letra E

49.(CESPE / DPU – 2016) Switchs e roteadores são equipamentos utilizados para definir a origem e o destino de pacotes de dados que trafegam entre máquinas de usuários ou de servidores e podem ser utilizados para interligar várias redes de computadores entre si.

Comentários:

Essa questão também foi bastante polêmica, então vamos por partes. *Switches e Roteadores são equipamentos?* Sim, eles são equipamentos de rede. *Utilizados para definir a origem e o destino de pacotes de dados que trafegam entre máquinas de usuários ou de servidores?* "Definir" não ficou legal! O Endereço MAC, por exemplo, é definido pelo fabricante do dispositivo de rede. *Podem ser utilizados para interligar várias redes de computadores entre si?* Galera, roteadores realmente conectam várias redes; switches conectam computadores à rede. No máximo, a questão poderia dizer que Switches conectam segmentos de uma mesma rede. Dessa forma, na minha opinião, a questão possui vários deslizes, no entanto o gabarito se manteve como correto.

Gabarito: Correto

---

50. (CESPE / FUB – 2016) Para conectar-se a uma rede wireless, um computador do tipo notebook deve estar conectado a algum tipo de receptor para o recebimento do sinal, como, por exemplo, um receptor integrado.

Comentários:

Essa questão é bem simples, mas a redação faz parecer que é difícil. Em uma rede wireless, não existe um meio físico de transmissão de dados porque os dados são transmitidos em ondas eletromagnéticas. Logo, para haver comunicação, é necessário ter algo que envia o sinal e algo que receba o sinal de internet. Quem geralmente envia esse sinal é o Roteador ou Access Point e quem geralmente recebe esse sinal é um computador, notebook, celular, etc. Esses dispositivos que recebem o sinal da internet realmente devem possuir algum tipo de receptor de sinal. Por exemplo: um computador precisa de uma placa de rede wireless que geralmente precisa ser adquirida separadamente; já um notebook já possui essa placa de rede wireless integrada, não é necessário adquiri-la separadamente. É isso que a questão quis dizer com receptor integrado.

Gabarito: Correto

---

51. (CESPE / TELEBRAS – 2016) Redes de computadores do tipo ponto a ponto apresentam a vantagem de fornecer elevado nível de segurança.

Comentários:

Como não há um dispositivo central capaz de oferecer serviços de autenticação, criptografia, entre outros, o nível de segurança é reduzido nesse tipo de rede em comparação a redes de computadores do tipo cliente/servidor.

Gabarito: Errado

---

52. (CESPE / Prefeitura de São Paulo – 2016) Com relação a redes de computadores, assinale a opção correta.

a) Computadores que utilizam o Linux não acessam computadores que usam o Windows, pois, em uma rede de computadores, não é possível a conexão entre sistemas operacionais diferentes.

b) Para a implantação de uma rede de computadores, são necessários, no mínimo, um computador servidor e quatro computadores clientes.

c) Access point é um dispositivo usado para a conexão de computadores em uma rede sem fio.

d) Para garantir o acesso de um computador a uma rede local, é suficiente conectar a placa de rede, dispensando-se qualquer tipo de configuração do usuário e do administrador de rede.

e) LAN (Local Area Network) é uma rede que conecta computadores localizados a, no máximo, dez metros de distância do servidor e fisicamente próximos uns aos outros.

Comentários:

(a) Errado, é claro que é possível a conexão entre computadores com sistemas operacionais diferentes dentro de uma mesma rede; (b) Errado, não existe uma quantidade mínima estabelecida de computadores para implantação de uma rede – a única restrição é que seja mais de um; (c) Correto, ele é realmente utilizado para conectar computadores a uma rede sem fio; (d) Errado, é necessário cadastrar usuários, definir suas permissões e seus perfis como usuários comuns ou administradores, dentre outras configurações; (e) Errado, trata-se de uma área pequena limitada a algumas centenas de metros.

Gabarito: Letra C

---

53. **(CESPE / PC-AL – 2016)** Os conectores padrão do tipo RJ-45 são utilizados para conectar as placas de redes dos computadores aos cabos de redes locais.

Comentários:

Os conectores RJ-45 realmente são utilizados para conectar placas de rede dos computadores aos cabos de redes locais (cabo de par trançado).

Gabarito: Correto

---

54. **(CESPE / FUNPRESP-JUD – 2016)** O sucesso de aplicativos de mensagens instantâneas deve-se à comunicação assíncrona entre os usuários e à presença de recursos como compartilhamento peer-to-peer.

Comentários:

Vamos pensar em aplicativos de mensagem instantânea, como Whatsapp e Telegram! *O sucesso desses aplicativos se deve à comunicação assíncrona entre os usuários?* Sim, lembrando que a comunicação assíncrona é aquela em que emissor e receptor não precisam estar sincronizados – prontos para enviar e receber dados. Em outras palavras, o emissor pode enviar dados e o receptor pode responder em outro momento. *Além disso, o sucesso desses aplicativos se deve à presença de recursos como compartilhamento peer-to-peer?* Não, esses aplicativos geralmente possuem um servidor intermediário entre emissor e receptor. *Lembra que eventualmente o Whatsapp sai do ar?* Em geral, é por conta de algum problema com o servidor! *Sabe quando você envia uma mensagem para outra pessoa e ela está com celular desligado?* A mensagem fica armazenada no servidor até que a pessoa fique online novamente para poder entregá-la. *Sabe aquela foto que você envia foto que você envia?* Ela passa por um servidor antes de ser entregue ao recipiente final. Dessa forma, podemos concluir que aplicativos de mensagem instantânea não tem sucesso graças aos recursos de compartilhamento peer-to-peer.

Gabarito: Errado

---

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

Comentários:

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

Gabarito: Errado

---

56. (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

---

57. (CESPE / STJ – 2015) A topologia física de uma rede representa a forma como os computadores estão nela interligados, levando em consideração os tipos de computadores envolvidos. Quanto a essa topologia, as redes são classificadas em homogêneas e heterogêneas.

Comentários:

Na verdade, não leva em consideração os tipos de computadores envolvidos, mas o layout físico dos links e nós da rede, isto é, como os cabos estão dispostos. Ademais, quanto a essa topologia, as redes são classificadas em: Barramento, Anel, Estrela, Malha, etc.

Gabarito: Errado

---

58. (CESPE / TELEBRÁS – 2015) O acesso à Internet com o uso de cabo (Cable Modem) é, atualmente, uma das principais formas de acesso à rede por meio de TVs por assinatura, pois um cabo (geralmente coaxial) de transmissão de dados de TV é compartilhado para trafegar dados de usuário.

Comentários:

O cabo coaxial é utilizado para transmitir sinais e informações a determinados aparelhos. Os pacotes de TV/Internet utilizam cabos coaxiais também para transmitir dados de usuário. À época da questão, era a principal forma de acesso – atualmente tem perdido espaço para a fibra óptica.

Gabarito: Correto

---

59. (CESPE / TELEBRÁS – 2015) As fibras ópticas do tipo monômodo apresentam, atualmente, taxas de transmissão máxima de 100 Gbps, que é um limite estabelecido pelo fabricante com base na demanda do mercado, e não um limite prático decorrente da incapacidade de se converterem sinais elétricos em ópticos a velocidades superiores a tal limite.

Comentários:

A fibra ótica possui capacidade de transmissão virtualmente infinita – nenhuma tecnologia existente atualmente chegou ao limite máximo de velocidade de transmissão, logo nenhuma fabricante estabeleceu limite algum! Dessa forma, a questão estaria errada! *Não está errada, Diego?* Não, porque questão foi anulada por conta do termo *monômodo*, quando o correto seria *monomodo*.

Gabarito: Anulada

---

60. (CESPE / MEC – 2015) Nas redes em estrela, se houver rompimento de um cabo, consequentemente toda a rede parará de funcionar.

Comentários:

O rompimento de um cabo não afetará a comunicação de outras estações. Por outro lado, se o nó central falhar, todas as estações serão prejudicadas.

Gabarito: Errado

---

61. (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

---

62. (CESPE / CADE – 2014) Tamanho físico, tecnologia de transmissão e topologia são critérios utilizados para classificar as redes de computadores.

Comentários:

Perfeito! É possível classificar redes de computadores de diversas formas, dentre elas: tamanho físico, tecnologia de transmissão ou topologia.

Gabarito: Correto

---

63. (CESPE / CADE – 2014) Para que uma rede de computadores seja classificada de acordo com o modelo cliente/servidor, faz-se necessário que tanto o cliente quanto o servidor estejam fisicamente no mesmo local.

Comentários:

Não, senhor! Pelo contrário, eles podem estar em qualquer lugar do planeta, respondendo a requisições remotamente. Para que uma rede de computadores seja classificada de acordo com o modelo cliente/servidor é que tenhamos máquinas diferentes que exercem o papel de consumir serviços e máquinas que fazem o papel de oferecer serviços.

Gabarito: Errado

---

64. (CESPE / ICMBio – 2014) Uma rede de dados, assim como os softwares, tem a função de transmitir informações e processá-las.

Comentários:

Redes de dados têm a função de transmitir informações e, não, de processá-las; e softwares têm a função de processar informações e, não, de transmiti-las.

Gabarito: Errado

---

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

Comentários:

Redes de abrangência ampla são WAN (**Wide** Area Network) e, não, MAN (Metropolitan Area Network). Além disso, a rede apresentada no enunciado conecta regiões de uma mesma cidade ou metrópole e, não, cidades distantes. Por fim, é possível ter redes MAN com transmissão sem fio.

Gabarito: Errado

---

66. (CESPE / CBM-CE – 2014) Em uma rede que utiliza o modelo cliente/servidor, um computador com atributos de servidor pode atender a diversos clientes em uma mesma empresa.

Comentários:

Perfeito! Essa é a ideia por traz do modelo cliente/servidor, isto é, um servidor atende a requisições de diversos clientes.

Gabarito: Correto

---

67. 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

---

68. (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

---

69. (CESPE / MJ – 2013) Uma rede local (LAN) permite conectar um número reduzido de computadores entre si, uma vez que ela é usada para comunicação em uma área geograficamente pequena. A recomendação técnica é de que esse número não ultrapasse cem computadores.

Comentários:

Esse item não faz o menor sentido! Primeiro, a classificação da rede como Rede Local trata de sua abrangência geográfica e, não, quantidade de computadores. Além disso, não existe recomendação técnica que limite a quantidade de computadores conectados em uma Rede Local.

Gabarito: Errado

---

70. (CESPE / TELEBRAS – 2013) A arquitetura de rede Ethernet, definida pelo padrão IEEE 802.3, é geralmente montada em barramento ou em estrela, com cabos de par trançado e switches.

Comentários:

Essa arquitetura é realmente definida pelo Padrão 802.3, geralmente montada com a Topologia em Barramento ou Topologia em Estrela, e geralmente se utiliza cabos de par trançado (como enlace físico) e switches (como dispositivos para segmentação de redes).

Gabarito: Correto

---

71. (CESPE / Câmara dos Deputados – 2012) Uma rede local (LAN — Local Area Network) é caracterizada por abranger uma área geográfica, em teoria, ilimitada. O alcance físico dessa rede permite que os dados trafeguem com taxas acima de 100 Mbps.

Comentários:

A LAN é caracterizada por abranger uma área geográfica bastante limitada. A WAN (*Wide Area Network*) seria uma rede que não possui uma abrangência geográfica muito definida. Ademais, o alcance físico de uma rede local não tem relação com sua taxa de transmissão de dados. É possível ter, sim, redes locais com taxas acima de 100 Mbps.

Gabarito: Errado

---

72. (CESPE / TRE/RJ – 2012) Redes LAN (Local Area Network) podem ser providas por mecanismos que estabeleçam a comunicação com fios, sem fios ou com ambos os meios de transmissão.

Comentários:

Perfeito! Redes LAN podem ser providas por diversos meios (com fio, sem fio ou ambos). Claro que, quando providas por mecanismos sem fio, ela passa a se chamar WLAN.

Gabarito: Correto

---

73. (CESPE / Câmara dos Deputados – 2012) AccessPoint ou hotspot é a denominação do ponto de acesso a uma rede bluetooth operada por meio de um hub.

Comentários:

Access Point é um dispositivo de rede utilizado para fornecer acesso sem fio aos recursos de uma rede de computadores; Hotspot é um dispositivo utilizado para fornecer acesso sem fio à internet; Por fim, não é operada por meio de um hub, é operador por meio do próprio dispositivo Access Point.

Gabarito: Errado

---

74. (CESPE / Polícia Federal – 2012) Para proferir uma palestra acerca de crime organizado, um agente conectou dispositivo USB do tipo bluetooth no computador que lhe estava disponível. A respeito desse cenário, julgue o item abaixo.

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:

Esse item causou tanta polêmica que a banca indeferiu os recursos e deu uma justificativa:

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 drives 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. Item sem alteração de gabarito.

Nada melhor do que a justificativa da própria banca, mas eu ainda acrescentaria que ela é mais semelhante à tecnologia WPAN do que WLAN.

Gabarito: Errado

---

75. (CESPE / TRT-RN – 2011) Um hub é um equipamento que permite a integração de uma ou mais máquinas em uma rede de computadores, além de integrar redes entre si, com a característica principal de escolher qual é a principal rota que um pacote de dados deve percorrer para chegar ao destinatário da rede.

Comentários:

O Hub recebe dados e os distribui para todas as outras máquinas em *broadcast*. Quem escolhe a principal rota é o roteador – ele é o responsável por encaminhar os pacotes de dados entre origem e destino.

Gabarito: Errado

---

76. (CESPE / PREVIC – 2011) WAN é uma rede geográfica que surgiu da necessidade de se compartilhar recursos especializados para uma maior comunidade de usuários geograficamente dispersos. Por terem um custo de comunicação elevado, essas redes são, em geral, públicas, ou seja, o sistema de comunicação é mantido, gerenciado e de propriedade de grandes operadoras (públicas ou privadas) e seu acesso é público.

Comentários:

Vamos por partes! *WAN compartilha recursos para uma comunidade maior de usuários geograficamente dispersos?* Sim! *WAN possui alto custo de comunicação?* Sim! *Redes WAN são geralmente são públicas?* Sim, mas isso não significa que sejam gratuitas! É pública no sentido de que qualquer pessoa que deseje acessá-la, pode pagar para tê-la. *Elas são geralmente de propriedade de grandes operadoras?* Sim, apenas elas possuem capacidade de investimento de fazer instalações intercontinentais, por exemplo.

Gabarito: Correto

---

77. (CESPE / PREVIC – 2011) A topologia em anel proporciona uma economia considerável relativamente ao número de conexões, ao se considerar os sistemas geograficamente distribuídos. Esse tipo de topologia apresenta fatores limitantes que inviabilizam a sua utilização, como, por exemplo, o aumento de pontos intermediários entre os pontos finais do canal de comunicação.

Comentários:

Questão retirada do renomado autor Behrouz Forouzan. Ele afirma que: "*Acrescentar ou eliminar um dispositivo exige apenas a mudança de duas conexões. **Os únicos fatores limitantes** são as questões relacionadas ao meio de transmissão e ao tráfego (comprimento máximo do anel e o **número máximo de dispositivos**)*". Logo, essa topologia realmente apresenta fatores limitantes com relação à quantidade de dispositivos ou pontos intermediários.

Gabarito: Correto

---

78. (CESPE / PREVIC – 2011) Na topologia em estrela, cada nó é interligado a um nó central (mestre), através do qual todas as mensagens devem passar. Este nó age, assim, como centro de controle da rede, interligando os demais nós (escravos). Nada impede que haja comunicações simultâneas entre os nós, desde que as estações envolvidas sejam diferentes.

Comentários:

Vocês sabem melhor do que eu que "desde que" é uma locução subordinativa condicional, logo tem o sentido de uma condição, podendo ser substituída por "contanto que". Todavia, não existe essa condição! Nada impede que haja comunicações simultâneas entre os nós, visto que essa topologia trabalha em full duplex.

Imaginem uma topologia em estrela com quatro máquinas: A, B, C e D. A e B podem se comunicar enquanto C e D também estão se comunicando simultaneamente. A questão afirma que nada impede que haja comunicações simultâneas desde que as estações sejam diferentes. Ora, se uma das estações participar de ambas as comunicações, ainda haverá comunicação simultânea.

É possível que A se comunique com B enquanto B se comunica com C, porque a comunicação é full-duplex. Logo, acho que a questão vacilou e discordo do gabarito. Observação: a topologia em estrela pode funcionar tanto em uma configuração cliente/servidor quanto em uma configuração mestre/escravo.

Gabarito: Correto

---

79. (CESPE / PREVIC – 2011) A fibra óptica é imune a interferências eletromagnéticas e, portanto, a fenômenos de indução eletromagnética, sendo apropriada para transmitir sinais luminosos e não elétricos.

Comentários:

Perfeito! Ela realmente é imune a interferências eletromagnéticas e fenômenos de indução eletromagnética. Além disso, ela realmente é apropriada para transmissão de sinais de luz em vez de sinais elétricos.

Gabarito: Correto

---

80. (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

81.(CESPE / MEC – 2011) Na arquitetura peer-to-peer (P2P) pura, as aplicações podem assumir simultaneamente os papéis de cliente e de servidor, o que lhes confere grande escalabilidade e facilidade de gerenciamento.

Comentários:

Na Arquitetura P2P Pura, a arquitetura é completamente descentralizada e não há um elemento central, sendo o completo oposto do modelo cliente-servidor – isso realmente confere grande escalabilidade, mas dificulta o gerenciamento. É por essa razão, inclusive, que existe a Arquitetura P2P Híbrida.

Gabarito: Errado

82.(CESPE / Banco da Amazônia – 2010) A Internet funciona a partir do modelo cliente/servidor, no qual os computadores dos usuários operam como clientes conectados aos servidores que funcionam como provedores de acesso e de serviços de correio eletrônico, transferência de arquivos e acesso a páginas web.

Comentários:

A Internet realmente funciona a partir do Modelo Cliente/Servidor. Nesse modelo, os computadores realmente operam como clientes conectados aos servidores e esses funcionam como provedores de diversos serviços. Acho que há uma imprecisão em dizer que os servidores funcionam como provedores de acesso.

Gabarito: Correto

83.(CESPE / Ministério da Saúde – 2010) A Internet funciona a partir de um modelo cliente/servidor, em que servidores são os usuários que produzem informações (documentos, imagens, programas) e os clientes são os provedores de acesso que contratam as empresas de telecomunicação para oferecerem serviços de conexão à rede.

Comentários:

A internet realmente funciona a partir de um modelo cliente/servidor, mas servidores não são usuários que produzem informações, eles são máquinas que fornecem informações; e clientes não são provedores de acesso, clientes consomem informações. Provedores de acesso são contratados por usuários para ter acesso à internet.

Gabarito: Errado

84.(CESPE / SEFAZ/ES – 2010) Para a conexão de um computador à Internet, é necessário ter, entre outros componentes de hardware, uma placa de rede ou um modem. A placa é usada no caso de o computador pertencer a uma rede de comunicação, enquanto que o modem é necessário quando a conexão é realizada via linha telefônica.

Comentários:

Para conectar um computador à internet, é realmente necessário ter – entre outros equipamentos de hardware – uma placa de rede e/ou um modem. Antigamente, para acessar a internet era comum ter um modem instalado no computador conectado diretamente via cabo à linha telefônica. Hoje em dia, para acessar a internet, um notebook pode fazê-lo sem possuir um modem, desde que ele pertença a uma rede de computadores (Ex: ele pode estar conectado à rede doméstica de uma casa). Além disso, é possível também acessar a internet por meio de um computador com placa de rede conectada via cabo a um modem. A questão é polêmica porque você pode interpretar o **ou** de uma forma inclusive ou exclusiva.

Gabarito: Correto

85.(CESPE / MPU – 2010) Um modem ADSL permite que, em um mesmo canal de comunicação, trafeguem sinais simultâneos de dados e de voz. Por isso, com apenas uma linha telefônica, um usuário pode acessar a Internet e telefonar ao mesmo tempo.

Comentários:

O Modem ADSL realmente permite o tráfego de sinais de dados e voz em um mesmo canal de comunicação. Lembrem-se de que é possível utilizar a internet e o telefone sem que este último esteja com a linha ocupada. Enfim... ele modula o sinal de forma que possam trafegar em conjunto dados e voz sem que um interfira no outro.

Gabarito: Correto

---

86. (CESPE / MPU – 2010) Determinada empresa pretende adquirir computadores para alguns dos seus funcionários e recebeu oferta de notebooks com as seguintes especificações: processador Intel® Celeron 900 (2.2 GHz, 1 MB L2 cache, 800 MHz FSB); memória RAM de 2 GB DDR2 800 MHz (2 × 1 GB); gravador de DVD/CD dual layer; rede sem fio padrão 802.11g, de 2,4 GHz; placa de rede integrada 10/100 Ethernet; sistema operacional Linux de 64 bits. Considerando as informações acima, julgue o item que se segue.

Os notebooks terão problemas com acesso às redes sem fio mais modernas, uma vez que o padrão 802.11g é incompatível com o padrão 802.11n de 2,4 GHz utilizado por essas redes.

Comentários:

EVOLUÇÃO DO PADRÃO WIRELESS (802.11)		
PADRÃO	**FREQUÊNCIA**	**TAXA MÁXIMA DE TRANSMISSÃO**
IEEE 802.11G	2.4 Ghz	54 Mbps
IEEE 802.11N	2.4 ou 5.0 Ghz	150, 300 até 600 Mbps

Notem que ambos são compatíveis e podem funcionar na mesma frequência (2.4Ghz) sem nenhum problema de compatilidade.

Gabarito: Errado

---

87. (CESPE / ANEEL – 2010) A fibra óptica é um filamento de vidro, constituído de material dielétrico, formado de duas partes principais: o núcleo, por onde se propaga a luz, e a casca, que serve para manter a luz confinada no núcleo.

Comentários:

Perfeito! É realmente um filamento de vidro, constituído de material dielétrico (que permite o isolamento), formado por duas partes principais: núcleo e casca.

Gabarito: Correto

---

88. (CESPE / TRE-PR – 2009) A Internet se caracteriza por ser uma rede do tipo cliente/servidor, na qual cada computador independe um do outro e compartilha os dados sem uma centralização, e qualquer computador do tipo cliente é um servidor independente de informações ou serviços.

Comentários:

A questão descreve o Modelo Ponto-a-Ponto. A Internet se caracteriza realmente por ser uma rede do tipo cliente/servidor, mas existe uma centralização e qualquer computador do tipo cliente é apenas do tipo cliente, ele não exerce o papel de servidor.

Gabarito: Errado

---

89. (CESPE / MIN – 2009) O termo Wi-Fi é entendido como uma tecnologia de interconexão entre dispositivos sem fios na qual é usado o protocolo IEEE 802.11.

Comentários:

O termo wi-fi é realmente entendido como uma tecnologia de interconexão entre dispositivos sem fio e utiliza o Padrão IEEE 802.11. A questão utilizou o termo *protocolo* em vez de *padrão*. Não se trata do termo mais adequado, mas não está errado se considerarmos protocolo em um sentido mais amplo de um conjunto de normas, procedimentos, entre outros.

Gabarito: Correto

90.(CESPE / Polícia Federal – 2009) Um computador permitiu acesso à Internet por meio de uma rede wi-fi, padrão IEEE 802.11b, em que uma portadora de 2,4 GHz de freqüência foi utilizada para a transmissão de dados a taxas de até 11 Mbps. Nessa situação, apesar de se poder transmitir a taxas de até 11 Mbps, essa taxa é compartilhada com os diversos usuários que estão na mesma rede wi-fi e, na medida em que um usuário se distancia do access point dessa rede, a sua taxa de transmissão tende a diminuir.

Comentários:

EVOLUÇÃO DO PADRÃO WIRELESS (802.11)		
PADRÃO	FREQUÊNCIA	TAXA MÁXIMA DE TRANSMISSÃO
IEEE 802.11B	2.4 Ghz	11 Mbps

Vamos por partes! Padrão IEEE 802.11b é realmente um padrão Wi-Fi! Ele – de fato – apresenta uma portadora de frequência de 2.4Ghz e taxas de transmissão de até 11Mbps. É claro que essa é uma taxa máxima que, quando compartilhada com outros usuários na mesma rede sem fio, essa taxa de transmissão tende a diminuir – assim como com o aumento da distância do Access Point.

Gabarito: Correto

91.(CESPE / MIN – 2009) A terceira geração de padrões e de tecnologias de telefonia móvel, denominada 3G, permite conexão com a Internet.

Comentários:

GERAÇÃO	DESCRIÇÃO
3ª GERAÇÃO (3G)	Utilizando tecnologia digital UMTS, oferece banda larga através da telefonia celular. Sucessor natural do GSM, o UMTS foi o resultado da padronização de várias tecnologias 3G, permitindo a transmissão de dados e totalmente compatível com GSM para transmissão de voz. Atualmente oferece taxas de até 14,4 Mbps.

Perfeito! Ela realmente permite a conexão com a internet banda larga.

Gabarito: Correto

---

92. **(CESPE / ANATEL – 2009)** Uma rede residencial de computadores, que atende aos moradores de uma residência e está conectada à Internet, por meio de acesso ADSL, denomina-se PAN (Personal Area Network).

Comentários:

Na verdade, trata-se de uma LAN (Local Area Network). A PAN (Personal Area Network) atende a uma única pessoa e geralmente está conectada via Bluetooth.

Gabarito: Errado

---

93. **(CESPE / CLDF – 2006)** Internet banda larga, downloads mais rápidos, conexão limpa, alta velocidade... as promessas são as mais variadas, porém, a realidade é bem diferente das propagandas. Quando o usuário resolve, finalmente, abolir o telefone para contratar um serviço de banda larga, vem a frustração: não há cobertura da operadora para instalar a conexão rápida. Pior, às vezes não há sequer a presença de um bom provedor de serviços na sua área, como é o caso de quem mora em cidades menores.

Em 2006, tudo pode mudar. Operadoras telefônicas e provedores de acesso estão esperando o início do ano para, aos poucos, divulgarem novidades em planos de acesso mais baratos e mais rápidos. E, nessa reviravolta, um dos grandes destaques é o WiMAX, uma tecnologia que permite conexões em alta velocidade sem o uso de fios e, conseqüentemente, sem aquela parafernália de cabos e ligações comuns à infra-estrutura das conexões ADSL e a cabo.

Internet: <http://tecnologia.uol.com.br>. Acesso em jan./2006.

Tendo o texto anterior como referência inicial, julgue o item seguinte, relacionado a conceitos de Internet.

É correto inferir-se que, ao permitir uma conexão "em alta velocidade sem o uso de fios", o acesso à Internet em banda larga por meio da tecnologia WiMAX dispensa o uso de modem, necessário em conexões ADSL e a cabo.

Comentários:

WiMAX é uma tecnologia que disponibiliza acesso a banda larga sem fio a distâncias maiores, no entanto essa tecnologia ainda necessitará do uso de um modem para conversão de dados.

Gabarito: Errado

---

94. **(CESPE / DATAPREV – 2006)** Redes locais — Local Area Networks (LANs) — normalmente cobrem pequenas áreas geográficas, operam a baixas taxas de transmissão e com pequena ocorrência de erros.

Comentários:

As Redes Locais – em geral – realmente operam com pequena ocorrência de erros, mas com altas taxas de transmissão. Em relação a taxas de transmissão, temos que LAN > MAN > WAN!

Gabarito: Errado

LISTA DE QUESTÕES – CESPE

1. **(CESPE / ANTT – 2024)** N, hacker mundialmente conhecido por sua atuação na Deep Web e na Dark Web e por cometer, sem deixar vestígios, crimes virtuais e atentar contra a cibersegurança de diversos órgãos públicos em todo o mundo, acessou um programa computacional de determinado ente federativo brasileiro que tem por objeto o estudo jurimétrico de infrações e acidentes trânsito e obteve os dados de inúmeros condutores. De posse desses dados, acessou os softwares dos veículos identificados em tal programa como detentores de tecnologia de condução semiautônoma e os fraudou, com o intuito de gerar acidentes de trânsito. N também instalou, no programa computacional, uma ferramenta de inteligência artificial que se vale de algoritmos para automaticamente gerar uma série de notificações de infração de trânsito a inúmeros condutores.

   Deep Web e Dark Web são expressões sinônimas utilizadas para descrever uma parte da Internet que, em contraposição à chamada Surface Web, é acessada para a realização de atividades ilegais.

2. **(CESPE / CNPQ – 2024)** Para que um computador possa se conectar à Internet, é essencial que ele esteja equipado com um hardware de comunicação, denominado placa de rede, que pode ser um chipset integrado à placa mãe do computador.

3. **(CESPE / TJ-ES – 2023)** Com base nas propriedades de rede exibidas na imagem a seguir, extraídas de um computador com Windows 10 conectado à rede por meio de apenas um adaptador de rede, é correto afirmar que esse computador poderá conectar-se a uma rede com velocidade de até 1.000 Mbps.



4. **(CESPE / CBM-TO – 2023)** Determinado usuário verificou que seu roteador wi-fi transmite dados nas faixas de frequência de 2,4 GHz e 5 GHz, respectivamente.

   A partir dessa situação hipotética, assinale a opção correta.

   a) O roteador wi-fi permite que as redes sejam utilizadas, exclusivamente, de maneira não concorrente.

   b) A frequência de rede de 5 GHz, por padrão, é mais veloz que a frequência de rede de 2,4 GHz, porém o alcance da primeira é menor que o da segunda.

   c) A rede com frequência nominal de 2,4 GHz é imune a interferência de sinal de rádio, pois a imunidade ao ruído é diretamente proporcional à velocidade de transferência de dados.

   d) O roteador wi-fi permite que a velocidade de transmissão das duas frequências sejam somadas, o que resulta em uma rede com frequência nominal de 7,4 GHz e com alcance ainda menor que o da rede com frequência nominal de 5 GHz.

5. **(CESPE / TCE-RJ – 2022)** Diferentemente das bridges, os repetidores são dispositivos capazes de reconhecer e examinar os quadros da camada de enlace.

6. **(CESPE / TCE-RJ – 2022)** No padrão Gigabit Ethernet, tanto no modo de operação half-duplex quanto no modo full-duplex, o uso do protocolo CSMA/CD para evitar colisões é dispensável, em razão da extensão de portadora, uma característica voltada à prevenção de colisões incluída originalmente nas definições do padrão.

7. **(CESPE / SECONT-ES – 2022)** As mensagens enviadas na Internet denominam-se pacotes, e os comutadores de pacotes são denominados roteadores ou switches.

8. **(CESPE / PG-DF – 2021)** Uma rede formada por dispositivos bluetooth é exemplo de PAN (Personal Area Network).

9. **(CESPE / TELEBRÁS - 2021)** O único requisito obrigatório ao se projetar uma rede de computadores é realizar um levantamento da quantidade de computadores a serem conectados à rede.

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

11. **(CESPE / PC-AL – 2021)** Denomina-se cabo coaxial, em uma rede de comunicação, o tipo de mídia de comunicação que realiza a conexão entre pontos, é imune a ruídos elétricos e é responsável pela transmissão de dados com capacidade de largura de banda muito maior do que os pares trançados.

12. **(CESPE / SEFAZ-CE – 2021)** Em uma rede em topologia de barramento, as comunicações de mensagens do tipo difusão são facilitadas porque todos os nós conectados ao barramento são capazes de ouvir todas as transmissões realizadas.

13. **(CESPE / Polícia Federal – 2021)** Uma LAN (*local área network*) fornece conectividade em tempo integral para os serviços de conexão da Internet.

14. **(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.

15. **(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.

16. **(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).

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

18. **(CESPE / Polícia Federal – 2018)** As redes de computadores podem ser classificadas, pela sua abrangência, em LAN (Local Area Network), MAN (Metropolitan Area Network), e WAN (Wide Area Network).

19. **(CESPE / Polícia Federal – 2018)** PAN (*Personal Area Network*) são redes de computadores destinadas a ambientes com acesso restrito, seja por limitações físicas ou por definições de segurança.

20. **(CESPE / Polícia Federal – 2018)** Uma empresa tem unidades físicas localizadas em diferentes capitais do Brasil, cada uma delas com uma rede local, além de uma rede que integra a comunicação entre as unidades. Essa rede de integração facilita a centralização do serviço de email, que é compartilhado para todas as unidades da empresa e outros sistemas de informação.

Se as redes locais das unidades da empresa estiverem interligadas por redes de operadoras de telecomunicação, então elas formarão a WAN (Wide Area Network) da empresa.

21. **(CESPE / Polícia Federal – 2018)** A conexão de sistemas como TVs, laptops e telefones celulares à Internet, e também entre si, pode ser realizada com o uso de comutadores (switches) de pacotes, os quais têm como função encaminhar a um de seus enlaces de saída o pacote que está chegando a um de seus enlaces de entrada.

22. **(CESPE / Polícia Federal – 2018)** Uma empresa tem unidades físicas localizadas em diferentes capitais do Brasil, cada uma delas com uma rede local, além de uma rede que integra a comunicação entre as unidades. Essa rede de integração facilita a centralização do serviço de email, que é compartilhado para todas as unidades da empresa e outros sistemas de informação. Tendo como referência inicial as informações apresentadas, julgue o item subsecutivo.

Em uma rede local que possui a topologia estrela, podem ser utilizados switches para integrar a comunicação entre os computadores.

23. **(CESPE / Polícia Federal – 2018)** Uma das vantagens da rede de computadores com tipologia mesh é a varredura de diversas possibilidades de roteamento para identificar a mais eficiente

24. **(CESPE / Polícia Federal – 2018)** Em redes de comunicação de dados, existem três modos de transmissão: o simplex, em que os dados circulam em apenas um sentido; o half-duplex, em que os dados circulam nos dois sentidos ao mesmo tempo; e o full-duplex, também conhecido por ligação de alternância.

25. **(CESPE / Polícia Federal – 2018)** Por se tratar de arquitetura ultrapassada e possuir pouco compartilhamento de recursos, redes do tipo cliente/servidor não podem ter mais que 100 clientes conectados ao respectivo servidor.

26. **(CESPE / Polícia Federal – 2018)** Uma empresa tem unidades físicas localizadas em diferentes capitais do Brasil, cada uma delas com uma rede local, além de uma rede que integra a comunicação entre as unidades. Essa rede de integração facilita a centralização do serviço de email, que é compartilhado para todas as unidades da empresa e outros sistemas de informação. Tendo como referência inicial as informações apresentadas, julgue o item subsecutivo.

Para viabilizar a comunicação de dados entre as unidades da empresa, podem ser utilizados serviços de interconexão com roteadores providos por operadoras de telecomunicação.

27. **(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.

28. **(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.

29. **(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

30. **(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

31. **(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

32. **(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.

33. **(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.

34. **(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.

35. **(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.

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

37. **(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.

38. **(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.

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



40. **(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.

41. **(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.

42. **(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.

43. **(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.

44. **(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.

45. **(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.

46. **(CESPE / Polícia Federal – 2018)** O padrão IEEE 802.11g permite que as redes locais das unidades da empresa operem sem cabeamento estruturado nos ambientes físicos e com velocidade mínima de 200 Mbps.

47. **(CESPE / ABIN – 2018)** Redes wi-fi e Bluetooth podem ser utilizadas para IoT, já NFC (Near Field Communication) não atende a demandas de IoT.

48. **(CESPE / TRE-BA – 2017)** O dispositivo de rede que opera nas camadas física, de enlace e de rede e que altera os endereços físicos em um pacote é denominado:

a) amplificador.
b) repetidor.
c) bridge.
d) hub.
e) roteador.

49. **(CESPE / DPU – 2016)** Switchs e roteadores são equipamentos utilizados para definir a origem e o destino de pacotes de dados que trafegam entre máquinas de usuários ou de servidores e podem ser utilizados para interligar várias redes de computadores entre si.

50. **(CESPE / FUB – 2016)** Para conectar-se a uma rede wireless, um computador do tipo notebook deve estar conectado a algum tipo de receptor para o recebimento do sinal, como, por exemplo, um receptor integrado.

51. **(CESPE / TELEBRAS – 2016)** Redes de computadores do tipo ponto a ponto apresentam a vantagem de fornecer elevado nível de segurança.

52. **(CESPE / Prefeitura de São Paulo – 2016)** Com relação a redes de computadores, assinale a opção correta.

a) Computadores que utilizam o Linux não acessam computadores que usam o Windows, pois, em uma rede de computadores, não é possível a conexão entre sistemas operacionais diferentes.

b) Para a implantação de uma rede de computadores, são necessários, no mínimo, um computador servidor e quatro computadores clientes.

c) Access point é um dispositivo usado para a conexão de computadores em uma rede sem fio.

d) Para garantir o acesso de um computador a uma rede local, é suficiente conectar a placa de rede, dispensando-se qualquer tipo de configuração do usuário e do administrador de rede.

e) LAN (Local Area Network) é uma rede que conecta computadores localizados a, no máximo, dez metros de distância do servidor e fisicamente próximos uns aos outros.

53. **(CESPE / PC/AL – 2016)** Os conectores padrão do tipo RJ-45 são utilizados para conectar as placas de redes dos computadores aos cabos de redes locais.

54. **(CESPE / FUNPRESP-JUD – 2016)** O sucesso de aplicativos de mensagens instantâneas deve-se à comunicação assíncrona entre os usuários e à presença de recursos como compartilhamento peer-to-peer.

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

56. **(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.

57. **(CESPE / STJ – 2015)** A topologia física de uma rede representa a forma como os computadores estão nela interligados, levando em consideração os tipos de computadores envolvidos. Quanto a essa topologia, as redes são classificadas em homogêneas e heterogêneas.

58. **(CESPE / TELEBRÁS – 2015)** O acesso à Internet com o uso de cabo (Cable Modem) é, atualmente, uma das principais formas de acesso à rede por meio de TVs por assinatura, pois um cabo (geralmente coaxial) de transmissão de dados de TV é compartilhado para trafegar dados de usuário.

59. **(CESPE / TELEBRÁS – 2015)** As fibras ópticas do tipo monômodo apresentam, atualmente, taxas de transmissão máxima de 100 Gbps, que é um limite estabelecido pelo fabricante com base na demanda do mercado, e não um limite prático decorrente da incapacidade de se converterem sinais elétricos em ópticos a velocidades superiores a tal limite.

60. **(CESPE / MEC – 2015)** Nas redes em estrela, se houver rompimento de um cabo, consequentemente toda a rede parará de funcionar.

61. **(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.

62. **(CESPE / CADE – 2014)** Tamanho físico, tecnologia de transmissão e topologia são critérios utilizados para classificar as redes de computadores.

63. **(CESPE / CADE – 2014)** Para que uma rede de computadores seja classificada de acordo com o modelo cliente/servidor, faz-se necessário que tanto o cliente quanto o servidor estejam fisicamente no mesmo local.

64. **(CESPE / ICMBio – 2014)** Uma rede de dados, assim como os softwares, tem a função de transmitir informações e processá-las.

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

66. **(CESPE / CBM-CE – 2014)** Em uma rede que utiliza o modelo cliente/servidor, um computador com atributos de servidor pode atender a diversos clientes em uma mesma empresa.

67. **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.

68. **(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.

69. **(CESPE / MJ – 2013)** Uma rede local (LAN) permite conectar um número reduzido de computadores entre si, uma vez que ela é usada para comunicação em uma área geograficamente pequena. A recomendação técnica é de que esse número não ultrapasse cem computadores.

70. **(CESPE / TELEBRAS – 2013)** A arquitetura de rede Ethernet, definida pelo padrão IEEE 802.3, é geralmente montada em barramento ou em estrela, com cabos de par trançado e switches.

71. **(CESPE / Câmara dos Deputados – 2012)** Uma rede local (LAN — Local Area Network) é caracterizada por abranger uma área geográfica, em teoria, ilimitada. O alcance físico dessa rede permite que os dados trafeguem com taxas acima de 100 Mbps.

72. **(CESPE / TRE/RJ – 2012)** Redes LAN (Local Area Network) podem ser providas por mecanismos que estabeleçam a comunicação com fios, sem fios ou com ambos os meios de transmissão.

73. **(CESPE / Câmara dos Deputados – 2012)** AccessPoint ou hotspot é a denominação do ponto de acesso a uma rede bluetooth operada por meio de um hub.

74. **(CESPE / Polícia Federal – 2012)** Para proferir uma palestra acerca de crime organizado, um agente conectou dispositivo USB do tipo bluetooth no computador que lhe estava disponível. A respeito desse cenário, julgue o item abaixo.

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.

75. **(CESPE / TRT-RN – 2011)** Um hub é um equipamento que permite a integração de uma ou mais máquinas em uma rede de computadores, além de integrar redes entre si, com a característica principal de escolher qual é a principal rota que um pacote de dados deve percorrer para chegar ao destinatário da rede.

76. **(CESPE / PREVIC – 2011)** WAN é uma rede geográfica que surgiu da necessidade de se compartilhar recursos especializados para uma maior comunidade de usuários geograficamente dispersos. Por terem um custo de comunicação elevado, essas redes são, em geral, públicas, ou seja, o sistema de comunicação é mantido, gerenciado e de propriedade de grandes operadoras (públicas ou privadas) e seu acesso é público.

77. **(CESPE / PREVIC – 2011)** A topologia em anel proporciona uma economia considerável relativamente ao número de conexões, ao se considerar os sistemas geograficamente distribuídos. Esse tipo de topologia apresenta fatores limitantes que inviabilizam a sua utilização, como, por exemplo, o aumento de pontos intermediários entre os pontos finais do canal de comunicação.

78. **(CESPE / PREVIC – 2011)** Na topologia em estrela, cada nó é interligado a um nó central (mestre), através do qual todas as mensagens devem passar. Este nó age, assim, como centro de controle da rede, interligando os demais nós (escravos). Nada impede que haja comunicações simultâneas entre os nós, desde que as estações envolvidas sejam diferentes.

79. **(CESPE / PREVIC – 2011)** A fibra óptica é imune a interferências eletromagnéticas e, portanto, a fenômenos de indução eletromagnética, sendo apropriada para transmitir sinais luminosos e não elétricos.

80. **(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).

81. **(CESPE / MEC – 2011)** Na arquitetura peer-to-peer (P2P) pura, as aplicações podem assumir simultaneamente os papéis de cliente e de servidor, o que lhes confere grande escalabilidade e facilidade de gerenciamento.

82. **(CESPE / Banco da Amazônia – 2010)** A Internet funciona a partir do modelo cliente/servidor, no qual os computadores dos usuários operam como clientes conectados aos servidores que funcionam como provedores de acesso e de serviços de correio eletrônico, transferência de arquivos e acesso a páginas web.

83. **(CESPE / Ministério da Saúde – 2010)** A Internet funciona a partir de um modelo cliente/servidor, em que servidores são os usuários que produzem informações (documentos, imagens, programas) e os clientes são os provedores de acesso que contratam as empresas de telecomunicação para oferecerem serviços de conexão à rede.

84. **(CESPE / SEFAZ/ES – 2010)** Para a conexão de um computador à Internet, é necessário ter, entre outros componentes de hardware, uma placa de rede ou um modem. A placa é usada no caso de o computador pertencer a uma rede de comunicação, enquanto que o modem é necessário quando a conexão é realizada via linha telefônica.

85. **(CESPE / MPU – 2010)** Um modem ADSL permite que, em um mesmo canal de comunicação, trafeguem sinais simultâneos de dados e de voz. Por isso, com apenas uma linha telefônica, um usuário pode acessar a Internet e telefonar ao mesmo tempo.

86. **(CESPE / MPU – 2010)** Determinada empresa pretende adquirir computadores para alguns dos seus funcionários e recebeu oferta de notebooks com as seguintes especificações: processador Intel® Celeron 900 (2.2 GHz, 1 MB L2 cache, 800 MHz FSB); memória RAM de 2 GB DDR2 800 MHz (2 × 1 GB); gravador de DVD/CD dual layer; rede sem fio padrão 802.11g, de 2,4 GHz; placa de rede integrada 10/100 Ethernet; sistema operacional Linux de 64 bits. Considerando as informações acima, julgue o item que se segue.

Os notebooks terão problemas com acesso às redes sem fio mais modernas, uma vez que o padrão 802.11g é incompatível com o padrão 802.11n de 2,4 GHz utilizado por essas redes.

87. **(CESPE / ANEEL – 2010)** A fibra óptica é um filamento de vidro, constituído de material dielétrico, formado de duas partes principais: o núcleo, por onde se propaga a luz, e a casca, que serve para manter a luz confinada no núcleo.

88. **(CESPE / TRE-PR – 2009)** A Internet se caracteriza por ser uma rede do tipo cliente/servidor, na qual cada computador independe um do outro e compartilha os dados sem uma centralização, e qualquer computador do tipo cliente é um servidor independente de informações ou serviços.

89. **(CESPE / MIN – 2009)** O termo Wi-Fi é entendido como uma tecnologia de interconexão entre dispositivos sem fios na qual é usado o protocolo IEEE 802.11.

90. **(CESPE / Polícia Federal – 2009)** Um computador permitiu acesso à Internet por meio de uma rede wi-fi, padrão IEEE 802.11b, em que uma portadora de 2,4 GHz de freqüência foi utilizada para a transmissão de dados a taxas de até 11 Mbps. Nessa situação, apesar de se poder transmitir a taxas de até 11 Mbps, essa taxa é compartilhada com os diversos usuários que estão na mesma rede wi-fi e, na medida em que um usuário se distancia do access point dessa rede, a sua taxa de transmissão tende a diminuir.

91. **(CESPE / MIN – 2009)** A terceira geração de padrões e de tecnologias de telefonia móvel, denominada 3G, permite conexão com a Internet.

92. **(CESPE / ANATEL – 2009)** Uma rede residencial de computadores, que atende aos moradores de uma residência e está conectada à Internet, por meio de acesso ADSL, denomina-se PAN (Personal Area Network).

93. **(CESPE / CLDF – 2006)** Internet banda larga, downloads mais rápidos, conexão limpa, alta velocidade... as promessas são as mais variadas, porém, a realidade é bem diferente das propagandas. Quando o usuário resolve, finalmente, abolir o telefone para contratar um serviço de banda larga, vem a frustração: não há cobertura da operadora para instalar a conexão rápida. Pior, às vezes não há sequer a presença de um bom provedor de serviços na sua área, como é o caso de quem mora em cidades menores.

Em 2006, tudo pode mudar. Operadoras telefônicas e provedores de acesso estão esperando o início do ano para, aos poucos, divulgarem novidades em planos de acesso mais baratos e mais rápidos. E, nessa reviravolta, um dos grandes destaques é o WiMAX, uma tecnologia que permite conexões em alta velocidade sem o uso de fios e, conseqüentemente, sem aquela parafernália de cabos e ligações comuns à infra-estrutura das conexões ADSL e a cabo.

Internet: <http://tecnologia.uol.com.br>. Acesso em jan./2006.

Tendo o texto anterior como referência inicial, julgue o item seguinte, relacionado a conceitos de Internet.

É correto inferir-se que, ao permitir uma conexão "em alta velocidade sem o uso de fios", o acesso à Internet em banda larga por meio da tecnologia WiMAX dispensa o uso de modem, necessário em conexões ADSL e a cabo.

94. **(CESPE / DATAPREV – 2006)** Redes locais — Local Area Networks (LANs) — normalmente cobrem pequenas áreas geográficas, operam a baixas taxas de transmissão e com pequena ocorrência de erros.

GABARITO – CESPE

1. ERRADO
2. CORRETO
3. CORRETO
4. ANULADA
5. ERRADO
6. ERRADO
7. CORRETO
8. CORRETO
9. ERRADO
10. ERRADO
11. ERRADO
12. CORRETO
13. ERRADO
14. CORRETO
15. CORRETO
16. LETRA E
17. CORRETO
18. CORRETO
19. ERRADO
20. CORRETO
21. CORRETO
22. CORRETO
23. CORRETO
24. ERRADO
25. ERRADO
26. CORRETO
27. CORRETO
28. ERRADO
29. LETRA D
30. LETRA C
31. LETRA A
32. CORRETO
33. ERRADO
34. CORRETO
35. CORRETO
36. CORRETO
37. ERRADO
38. ERRADO
39. ERRADO
40. CORRETO
41. ERRADO
42. ERRADO
43. CORRETO
44. CORRETO
45. ERRADO
46. ERRADO
47. ERRADO
48. LETRA E
49. CORRETO
50. CORRETO
51. ERRADO
52. LETRA C
53. CORRETO
54. ERRADO
55. ERRADO
56. CORRETO
57. ERRADO
58. CORRETO
59. ANULADA
60. ERRADO
61. CORRETO
62. CORRETO
63. ERRADO
64. ERRADO
65. ERRADO
66. CORRETO
67. ERRADO
68. CORRETO
69. ERRADO
70. CORRETO
71. ERRADO
72. CORRETO
73. ERRADO
74. ERRADO
75. ERRADO
76. CORRETO
77. CORRETO
78. CORRETO
79. CORRETO
80. ERRADO
81. ERRADO
82. CORRETO
83. ERRADO
84. CORRETO
85. CORRETO
86. ERRADO
87. CORRETO
88. ERRADO
89. CORRETO
90. CORRETO
91. CORRETO
92. ERRADO
93. ERRADO
94. 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.