Estratégia Concursos

Aula 00

TJ-MS (Técnico de Nível Superior - Analista de Sistemas Computacionais - Analista de Segurança de TI) Passo Estratégico de Conhecimentos Específicos - 2024 (Pós-Edital)

Autor:
Fernando Pedrosa Lopes

07 de Março de 2024

TOPOLOGIAS DE REDES

Sumário

CONTEÚDO

Redes de Computadores. Conceitos Básicos. Tipos de conexão. Direções de transmissão. Modos de transmissão. Classificações de redes. Meios de transmissão. Padrões de Redes.

ANÁLISE ESTATÍSTICA

Inicialmente, convém destacar o percentual de incidência do assunto, dentro da disciplina **Redes de Computadores** em concursos/cargos similares. Quanto maior o percentual de cobrança de um dado assunto, maior sua importância.

Obs.: *um mesmo assunto pode ser classificado em mais de um tópico devido à multidisciplinaridade de conteúdo*.

Assunto	Relevância na disciplina em concursos similares
Protocolo	8.9 %
1. IP (Internet Protocol)	2.7 %
2. HTTP (Hypertext Transfer Protocol)	1.8 %
3. SNMP (Simple NetWork Management Protocol)	1.8 %
4. Protocolos de Roteamento: RIP BGP e OSPF	0.9 %
5. SMTP (Simple Mail Transfer Protocol)	0.4 %
Gerência de Redes	8.9 %
Segurança de Redes	8.5 %
Sub-Redes	4.5 %
Transmissão de Dados	4.5 %
Arquiteturas de Rede	4.0 %
1. Ethernet	1.3 %

2. LAN (Local Area Network)	1.3 %
3. WAN (Wide Area Network)	1.3 %
Cabeamento	4.0 %
Armazenamento de Dados em Redes de Computadores	4.0 %
1. RAID (Redundant Array of Independent Disks)	2.2 %
2. NAS (Network Attached Storage)	1.3 %
3. SAN (Storage Area Network)	1.3 %
Redes sem Fio	3.6 %
Endereçamento IP	3.6 %
Topologias	2.7 %
Equipamentos de Redes	2.2 %
1. Roteadores	1.8 %
2. Switches	0.9 %
3. hub	0.4 %
Arquitetura TCP/IP	2.2 %
Modelo OSI	2.2 %
Acesso Remoto - VPN (Virtual Private Network) Software para Acesso Remoto e Team Viewer	2.2 %
Meios físicos de transmissão	1.8 %
DNS (Domain Name System)	1.8 %
Conceitos Básicos em Redes de Computadores	1.3 %
Firewall	1.3 %
VLAN	1.3 %
Proxy	1.3 %
Redes Linux	0.9 %

Serviços	0.9 %
QoS	0.9 %
MPLS	0.9 %
NAT (Network Address Translation)	0.9 %
Redes Windows	0.4 %
Telefonia	0.4 %

GLOSSÁRIO DE TERMOS

Faremos uma lista de termos que são relevantes ao entendimento do assunto desta aula. Caso tenha alguma dúvida durante a leitura, esta seção pode lhe ajudar a esclarecer.

Rede de Computador: Sistema de comunicação que conecta computadores e outros dispositivos para compartilhar recursos e informações.

Nó: Qualquer dispositivo que está conectado à rede, como um computador, impressora ou switch.

Link: Conexão física ou sem fio que conecta dois nós em uma rede.

Host: Um computador ou outro dispositivo em uma rede que oferece serviços a outros nós.

Topologia: A estrutura física ou lógica de uma rede, ou seja, como os nós da rede estão conectados.

Cliente: Um dispositivo ou programa que solicita serviços ou recursos de um servidor.

Servidor: Um computador ou programa que fornece serviços ou recursos para outros computadores (clientes) na rede.

Ponto-a-ponto: Uma conexão direta entre dois nós de uma rede.

Ponto-multiponto: Uma conexão onde um único nó (ponto) se comunica com vários outros nós.

Simplex: Um modo de comunicação onde os dados só podem ser transmitidos em uma direção.

Half-duplex: Modo de comunicação onde os dados podem ser transmitidos em ambas as direções, mas não ao mesmo tempo.

Full-duplex: Modo de comunicação onde os dados podem ser transmitidos em ambas as direções simultaneamente.

Unicast: Transmissão de dados de um único remetente para um único destinatário.

Multicast: Transmissão de dados de um único remetente para vários destinatários.

Broadcast: Transmissão de dados de um remetente para todos os nós na rede.

PAN (Personal Area Network): Rede que cobre uma área muito pequena, normalmente dentro do alcance de uma pessoa.

LAN (Local Area Network): Rede que cobre uma pequena área, como uma casa, escritório ou campus universitário.

MAN (Metropolitan Area Network): Rede que cobre uma área maior, como uma cidade ou região metropolitana.

WAN (Wide Area Network): Rede que cobre uma grande área geográfica, como um país ou o mundo inteiro.

Barramento (topologia): Uma topologia de rede onde todos os nós estão conectados a um único cabo (o "barramento").

Anel (topologia): Uma topologia de rede onde cada nó está conectado a exatamente dois outros nós, formando um circuito fechado, ou "anel".

Estrela (topologia): Uma topologia de rede onde todos os nós estão conectados a um nó central, formando uma "estrela".

Malha (topologia): Uma topologia de rede onde cada nó está conectado a todos os outros nós.

Cabo Coaxial: Um tipo de cabo que possui um condutor central cercado por um isolante, uma blindagem de metal e uma capa externa.

UTP (Unshielded Twisted Pair): Um tipo de cabo que possui pares de fios trançados juntos e não possui blindagem metálica.

STP (Shielded Twisted Pair): Um tipo de cabo que possui pares de fios trançados juntos e possui uma camada de blindagem metálica para reduzir a interferência eletromagnética.

Fibra Ótica: Um meio de transmissão que utiliza luz para transmitir informações, permitindo velocidades de transmissão muito altas.

Monomodo: Refere-se a um tipo de cabo de fibra óptica que permite apenas um único modo de propagação de luz.

Multimodo: Refere-se a um tipo de cabo de fibra óptica que permite vários modos de propagação de luz.

Ethernet (LAN): Um padrão de rede comum para redes locais, que utiliza o protocolo CSMA/CD.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection): Um método de controle de acesso ao meio usado para minimizar colisões de dados em redes Ethernet.

Token Ring (LAN): Um padrão de rede que utiliza um "token" para controlar o acesso ao meio e evitar colisões de dados.

Token: No contexto de uma rede Token Ring, um "token" é uma espécie de permissão que um nó precisa para transmitir dados na rede.

Wi-Fi (WLAN): Uma tecnologia que permite a comunicação sem fio entre dispositivos em uma LAN.

WEP (Wired Equivalent Privacy): Um protocolo de segurança obsoleto para redes Wi-Fi, que tem várias vulnerabilidades conhecidas.

WPA (Wi-Fi Protected Access): Um protocolo de segurança para redes Wi-Fi que melhorou a segurança em relação ao WEP.

WPA-2 (Wi-Fi Protected Access II): A segunda versão do protocolo WPA, que fornece segurança ainda mais forte do que o WPA original.

Access Point: Um dispositivo em uma rede sem fio que conecta dispositivos sem fio à rede.

Bluetooth (WPAN): Uma tecnologia de rede sem fio para a transferência de dados em curta distância.

WiMAX (Worldwide Interoperability for Microwave Access - WMAN): Uma tecnologia de rede sem fio para a transmissão de dados em longa distância, comumente usada para conectar redes LAN a redes WAN.

ROTEIRO DE REVISÃO

A ideia desta seção é apresentar um roteiro para que você realize uma revisão completa do assunto e, ao mesmo tempo, destacar aspectos do conteúdo que merecem atenção.

Introdução

Uma rede de computadores é uma estrutura de dispositivos interconectados que se comunicam para compartilhar recursos e informações. Estes dispositivos, ou "nós" de rede, podem ser computadores, servidores, impressoras, switches, roteadores, entre outros. As redes podem ser configuradas de diversas maneiras, chamadas de **topologias**, que determinam a forma como os nós se comunicam.

Redes de computadores tornaram-se um elemento fundamental do mundo moderno. Elas permitem a comunicação e o compartilhamento de recursos de maneira eficiente, proporcionando conectividade e facilitando o fluxo de informações, com aplicações que variam desde comércio eletrônico até infraestrutura e serviços de computação em nuvem.

A primeira forma de rede de computadores foi a ARPANET, desenvolvida na década de 1960 pelo Departamento de Defesa dos EUA. Desde então, as redes passaram por várias fases de desenvolvimento e evolução:

- Na década de 1970, o protocolo TCP/IP foi desenvolvido, o que permitiu a comunicação entre redes diferentes, resultando na formação da Internet.
- Na década de 1980, o desenvolvimento das LANs (Local Area Networks) permitiu a comunicação entre computadores próximos.
- Na década de 1990, a World Wide Web revolucionou o uso da Internet, tornando-a acessível a usuários não técnicos e possibilitando o crescimento explosivo da Internet.
- No século XXI, as redes têm se tornado cada vez mais sem fio e móveis, com o desenvolvimento de tecnologias como Wi-Fi, 3G, 4G e 5G.

- Atualmente, estamos na era da Internet das Coisas (IoT), onde não apenas computadores, mas todos os tipos de dispositivos estão sendo conectados à rede.

Conceitos Básicos

Antes de entrarmos em maiores detalhes sobre Redes de Computadores, vamos estabelecer uma nomenclatura e conceitos básicos que irão nos ajudar a entender melhor as próximas seções.

Nós, Links e Hosts:

Em uma rede, um nó representa qualquer dispositivo capaz de enviar ou receber dados. Isso pode incluir computadores, impressoras, switches, roteadores e outros dispositivos de rede. Os links, por sua vez, referem-se aos canais de comunicação que conectam esses nós. Eles podem ser cabos (como Ethernet ou fibra óptica) ou conexões sem fio (como Wi-Fi ou Bluetooth). Já os hosts são tipos específicos de nós que servem como ponto inicial ou final de transferências de dados.

Servidores e Clientes:

Na arquitetura cliente-servidor, que é amplamente utilizada em redes de computadores, o servidor é um nó que fornece recursos ou serviços. Por exemplo, um servidor web hospeda sites e os envia para os usuários quando solicitado. Os clientes, por outro lado, são nós que solicitam e utilizam esses recursos ou serviços.

Protocolos e Padrões:

Protocolos são conjuntos de regras que governam a comunicação entre nós em uma rede. Eles definem aspectos como formato e tamanho dos pacotes de dados, procedimentos de erro, endereçamento de dados, e muito mais. Alguns dos protocolos mais conhecidos incluem o TCP/IP, HTTP, FTP, entre outros. Padrões de redes, por outro lado, são diretrizes estabelecidas por organizações de normatização que garantem a interoperabilidade entre dispositivos de rede de diferentes fabricantes. Exemplos de tais organizações incluem a IEEE (Institute of Electrical and Electronics Engineers) e a IETF (Internet Engineering Task Force).

Tipos de Conexão

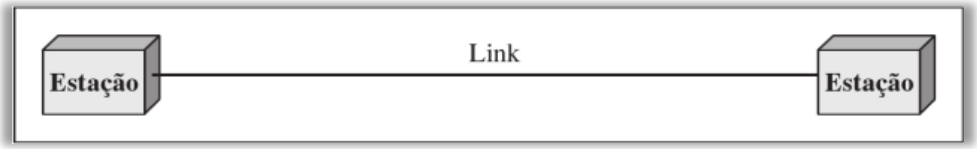
Redes são dois ou mais dispositivos conectados através de links. Um link, **também chamado de enlace, é um caminho de comunicação que transfere dados de um dispositivo para outro.** Para

fins de visualização, é mais simples imaginar qualquer link como uma reta entre dois pontos. Para ocorrer a comunicação, dois dispositivos devem ser conectados de alguma maneira ao mesmo link ao mesmo tempo.

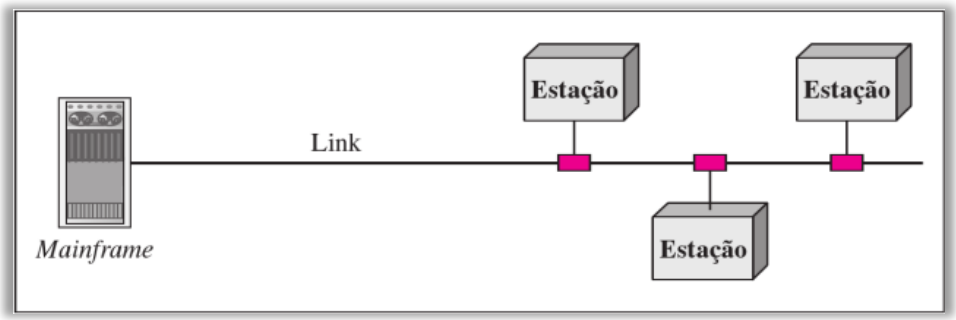
Existem dois tipos possíveis de conexão: **ponto-a-ponto e ponto-multiponto**. Ambos se diferenciam em relação à utilização de um link dedicado ou compartilhado.

No tipo de conexão **ponto a ponto** (PtP, do inglês Point-to-Point), uma conexão direta é estabelecida entre dois nós de uma rede. Ou seja, um nó (ponto) se comunica diretamente com outro nó (ponto). Este tipo de conexão é uma das formas mais simples de conectar dois dispositivos de rede.

Em uma rede ponto a ponto, cada dispositivo pode atuar como cliente ou servidor, dependendo da situação. Além disso, cada dispositivo na rede é responsável por sua própria segurança e gerenciamento. Por exemplo, em uma pequena rede de escritório, cada computador pode compartilhar seus arquivos e impressoras com outros computadores na rede sem a necessidade de um servidor central.



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



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

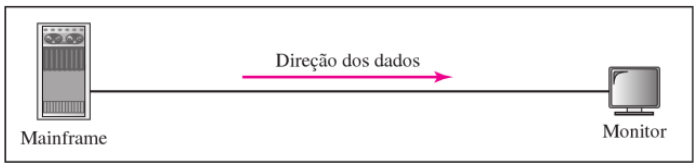
PONTO-MULTIPONTO	Conexão que fornece um link compartilhado entre mais de dois dispositivos.

Direções de Transmissão

A direção de transmissão se refere ao modo como os dados são transmitidos entre os dispositivos em uma rede. Existem três principais formas de transmissão: simplex, half-duplex e full-duplex.

Transmissão Unidirecional (Simplex):

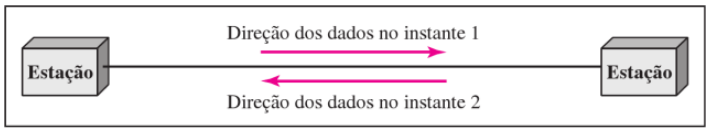
Na transmissão unidirecional, ou simplex, os dados fluem em uma única direção: do transmissor para o receptor. Após estabelecida a conexão, o transmissor só pode enviar dados, e o receptor só pode recebê-los. A comunicação não pode ocorrer na direção oposta.



Exemplo: Um exemplo típico de transmissão unidirecional é a transmissão de rádio ou televisão. A estação de rádio ou televisão (transmissor) envia sinais que são recebidos pelos rádios ou televisores (receptores) em casa. Os receptores não têm a capacidade de enviar sinais de volta à estação de rádio ou televisão.

Transmissão Bidirecional Alternada (Half-Duplex):

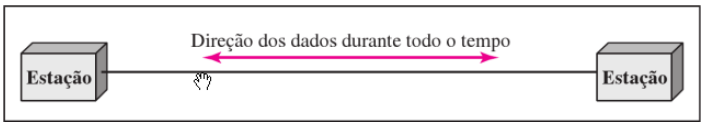
Na transmissão bidirecional alternada, ou half-duplex, os dados podem fluir em ambas as direções, mas não simultaneamente. Quando um dispositivo está transmitindo, o outro deve esperar para enviar seus dados.



Exemplo: Um exemplo comum de transmissão half-duplex é a utilização de walkie-talkies. Quando uma pessoa está falando (transmitindo), a outra pessoa precisa esperar para falar (receber). A comunicação não pode acontecer em ambos os sentidos ao mesmo tempo.

Transmissão Bidirecional Simultânea (Full-Duplex):

Na transmissão bidirecional simultânea, ou full-duplex, os dados podem fluir em ambas as direções simultaneamente. Isso permite que a comunicação ocorra em dois sentidos ao mesmo tempo, sem interrupções.



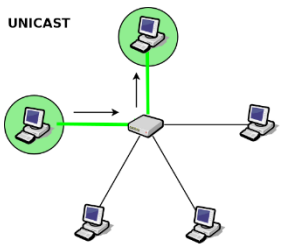
Exemplo: Um exemplo de transmissão full-duplex é uma chamada telefônica. Ambas as partes na chamada podem falar e ouvir ao mesmo tempo. Da mesma forma, na internet, muitas conexões são full-duplex, permitindo que os dados sejam enviados e recebidos ao mesmo tempo.

Modos de Transmissão

Os modos de transmissão descrevem a forma como os dados são enviados de um dispositivo para outro(s) em uma rede. Os três principais modos de transmissão são unicast, multicast e broadcast.

Transmissão Unicast:

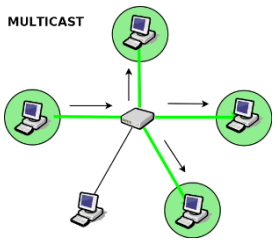
A transmissão unicast ocorre quando um único emissor envia informações a um único receptor. Em outras palavras, é uma transmissão de um-para-um. É o tipo mais comum de transmissão em redes de computadores.



Exemplo: Quando você acessa um website, seu computador (o cliente) estabelece uma conexão unicast com o servidor do website. Todas as informações trocadas entre o seu computador e o servidor são transmitidas exclusivamente entre esses dois pontos.

Transmissão Multicast:

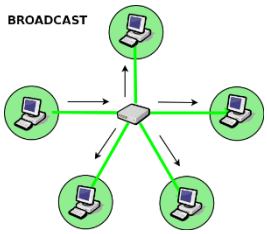
A transmissão multicast ocorre quando um emissor envia informações a um grupo de receptores. Dessa forma, é uma transmissão de um-para-muitos, mas o 'muitos' aqui é um conjunto definido de dispositivos que se inscreveram para receber tais informações, e não todos os dispositivos na rede.



Exemplo: Um exemplo comum de transmissão multicast é a transmissão de TV por IP (IPTV). O servidor de IPTV envia o mesmo fluxo de vídeo para vários clientes que se inscreveram para o serviço, utilizando apenas a largura de banda necessária para uma única transmissão.

Transmissão Broadcast:

A transmissão broadcast é uma forma de transmissão onde um emissor envia informações para todos os dispositivos em uma rede. Portanto, é uma transmissão de um-para-todos.



Exemplo: Um exemplo clássico de transmissão broadcast é o pedido de endereço ARP (Address Resolution Protocol) em uma rede local (LAN). Quando um dispositivo precisa conhecer o endereço físico (MAC) associado a um endereço IP em uma LAN, ele envia uma solicitação ARP em broadcast para todos os dispositivos na rede.

Classificações de Redes

Podemos classificar redes quanto à sua dimensão, arquitetura e topologia específica. Vamos essas classificações em detalhes.

Quanto à Dimensão ou Área Geográfica

Redes de computadores podem ser classificadas de acordo com a sua dimensão ou a área geográfica que cobrem. As quatro principais categorias são: Redes de Área Pessoal (PAN), Redes de Área Local (LAN), Redes de Área Metropolitana (MAN) e Redes de Área Ampla (WAN).

PAN (Personal Area Network):

Uma PAN é uma rede que cobre uma pequena área, geralmente dentro do alcance de uma pessoa. Normalmente, uma PAN inclui dispositivos como computadores, smartphones, tablets e periféricos (como impressoras ou fones de ouvido) que são usados por um único usuário.

Exemplo: Um exemplo de uma PAN seria a conexão Bluetooth entre o seu smartphone e os seus fones de ouvido sem fio.

LAN (Local Area Network):

Uma LAN é uma rede que abrange uma área geográfica limitada, como uma casa, escritório ou campus universitário. As LANs geralmente usam tecnologias como Ethernet ou Wi-Fi para conectar dispositivos em uma área relativamente pequena e geralmente são de propriedade de uma única organização ou indivíduo.

Exemplo: A rede Wi-Fi em sua casa, que conecta seus dispositivos, como seu computador, smartphone e smart TV, é um exemplo de uma LAN.

MAN (Metropolitan Area Network):

Uma MAN é uma rede que cobre uma área maior do que uma LAN, mas menor do que uma WAN - geralmente, uma cidade ou um subúrbio. As MANs são geralmente usadas para conectar várias LANs em uma área geográfica específica.

Exemplo: A rede de uma empresa de telecomunicações que fornece acesso à internet para várias residências e empresas em uma cidade é um exemplo de uma MAN.

WAN (Wide Area Network):

Uma WAN é uma rede que cobre uma grande área geográfica, como um país, um continente ou até mesmo o mundo inteiro. As WANs são geralmente compostas por várias LANs e MANs conectadas. A internet é um exemplo de uma WAN.

Exemplo: A internet, que conecta dispositivos e redes em todo o mundo, é o exemplo mais conhecido de uma WAN.

A tabela a seguir resume as classificações quanto às dimensões:

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.

Quanto à Arquitetura de Rede

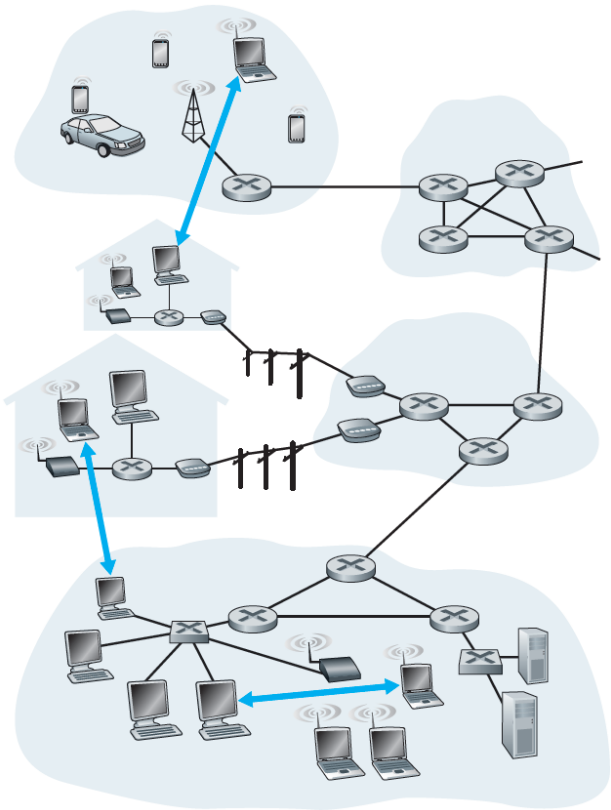
Quanto à arquitetura da rede, podemos classificá-la como Ponto-a-Ponto ou Cliente-Servidor.

Arquitetura Ponto a Ponto:

A arquitetura de rede ponto a ponto, também conhecida como rede Peer-to-Peer (P2P), é uma forma de rede em que cada nó da rede (ou "peer") atua tanto como cliente quanto como servidor. Nesse tipo de arquitetura, todos os computadores da rede têm o mesmo status e podem iniciar ou completar uma transação de dados.

Características:

- **Descentralização**: As redes P2P são tipicamente descentralizadas, o que significa que não há um servidor central que controla todas as atividades da rede. Em vez disso, cada nó pode atuar como um servidor ou cliente.
- **Escalabilidade**: Redes P2P são altamente escaláveis. Novos nós podem ser adicionados à rede sem a necessidade de atualizações de infraestrutura central.
- **Compartilhamento de Recursos**: Em uma rede P2P, os recursos (como arquivos e impressoras) podem ser compartilhados diretamente entre os nós sem a necessidade de um servidor central.



Vantagens:

- **Custo-benefício**: Como não há necessidade de um servidor central ou infraestrutura complexa, as redes P2P são geralmente mais econômicas para configurar e manter do que as redes tradicionais baseadas em servidor.
- **Resiliência**: Dada a sua natureza descentralizada, as redes P2P são resilientes a falhas. Se um nó falhar, os outros nós da rede não são afetados e podem continuar a funcionar normalmente.

Desvantagens:

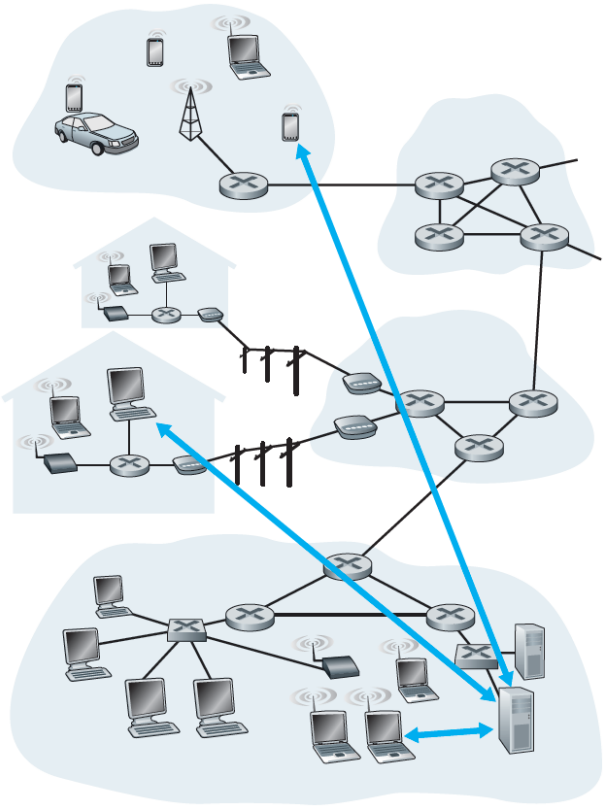
- **Segurança**: Como cada nó pode atuar como servidor, a segurança é muitas vezes um desafio nas redes P2P. A ausência de um servidor central para gerenciar a segurança pode tornar a rede vulnerável a ataques.
- **Gerenciamento**: O gerenciamento de redes P2P pode ser complexo, especialmente à medida que a rede cresce. Dado que cada nó é gerenciado individualmente, tarefas como a aplicação de atualizações de segurança e software podem ser mais complexas do que em uma rede baseada em servidor.

Arquitetura Cliente-Servidor:

A arquitetura de rede cliente-servidor é um modelo de comunicação de rede onde um servidor centralizado fornece serviços ou recursos para os clientes (nós). Esses servidores são máquinas que armazenam, processam e gerenciam recursos de rede, como arquivos, aplicativos, páginas da web e bancos de dados.

Características:

- **Centralização**: As redes cliente-servidor têm um servidor central que gerencia a rede, processa as solicitações dos clientes e fornece os recursos solicitados.
- **Função Diferenciada**: Nesta rede, os nós desempenham funções distintas. O servidor fornece recursos e gerencia a rede, enquanto os clientes consomem esses recursos.
- **Segurança Gerenciada**: Além disso, o servidor central geralmente contém medidas de segurança para proteger os dados e recursos da rede.



Vantagens:

- **Eficiência**: Como o servidor é dedicado ao processamento de solicitações e ao gerenciamento de recursos, as redes cliente-servidor tendem a ser mais eficientes do que as redes peer-to-peer, especialmente para redes maiores.
- **Segurança Melhorada**: O servidor central pode ser equipado com medidas de segurança para proteger a rede contra ataques, tornando a rede cliente-servidor mais segura do que as redes peer-to-peer.
- **Facilidade de Manutenção**: São mais fáceis de gerenciar porque todas as atualizações, configurações de segurança e gerenciamento de recursos podem ser feitos a partir do servidor central.

Desvantagens:

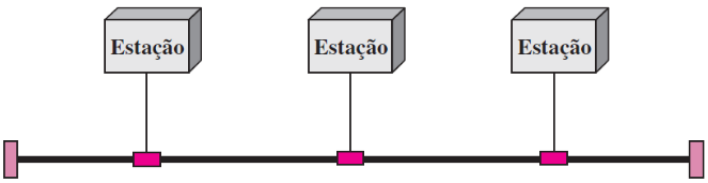
- **Custo Mais Elevado**: Podem ser mais caras de implementar e manter, devido ao custo do servidor e da necessidade de pessoal de TI especializado para gerenciar a rede.
- **Ponto Único de Falha**: Se o servidor falhar, todos os clientes serão afetados. Assim, as redes cliente-servidor têm um ponto único de falha.

Quanto à Topologia de Rede

A topologia de rede descreve o layout de uma rede de computadores, incluindo como os diferentes nós (ou seja, computadores ou outros dispositivos de rede) estão conectados entre si. A topologia escolhida pode afetar a performance, a robustez e a facilidade de gerenciamento da rede. Vamos discutir quatro topologias comuns: Barramento, Anel, Estrela e Malha.

Topologia de Barramento:

Na topologia de barramento, todos os dispositivos são conectados a um único cabo, chamado barramento. Os dados enviados por um dispositivo são propagados ao longo do barramento e todos os dispositivos na rede veem os dados, mas apenas o destinatário pretendido os processa.



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

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

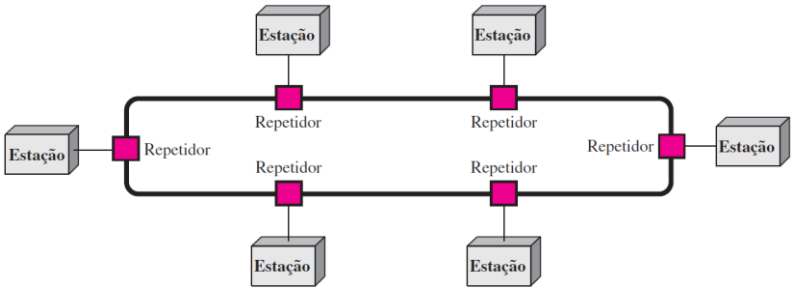
Outra característica dessa topologia é que todas as estações de trabalho podem enviar dados em qualquer direção, mas jamais simultaneamente. Quando uma estação de trabalho estiver transmitindo dados, todas as outras devem ficar em espera até que ela finalize e que o barramento fique disponível. Só então,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

Vantagens: Simplicidade de instalação e baixo custo.

Desvantagens: Se o barramento falhar, toda a rede cai. Além disso, pode ser mais difícil isolar falhas na rede.

Topologia de Anel:

Na topologia de anel, cada dispositivo tem uma conexão dedicada apenas com dois dispositivos em ambos os lados, formando um anel. A comunicação acontece em uma única direção, com cada bit de dados seguindo ao longo do anel até atingir seu destino.



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

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

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

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

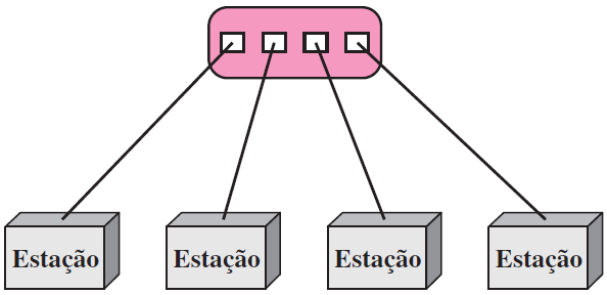
O envelope continua percorrendo o anel para a próxima estação, e a próxima, e a próxima, até chegar à estação que enviou os dados. Essa estação abre o envelope, verifica o sinal recebido, confirma que a estação de destino recebeu as informações enviadas e devolve o token para a rede para que ele continue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

Vantagens: Pode manejar maior tráfego do que a topologia de barramento.

Desvantagens: Uma falha em qualquer dispositivo pode interromper a comunicação em todo o anel.

Topologia Estrela:

Na topologia de estrela, todos os dispositivos estão conectados a um hub central. O hub central pode ser um switch, um roteador ou um servidor. Dados entre dispositivos devem passar pelo hub central.



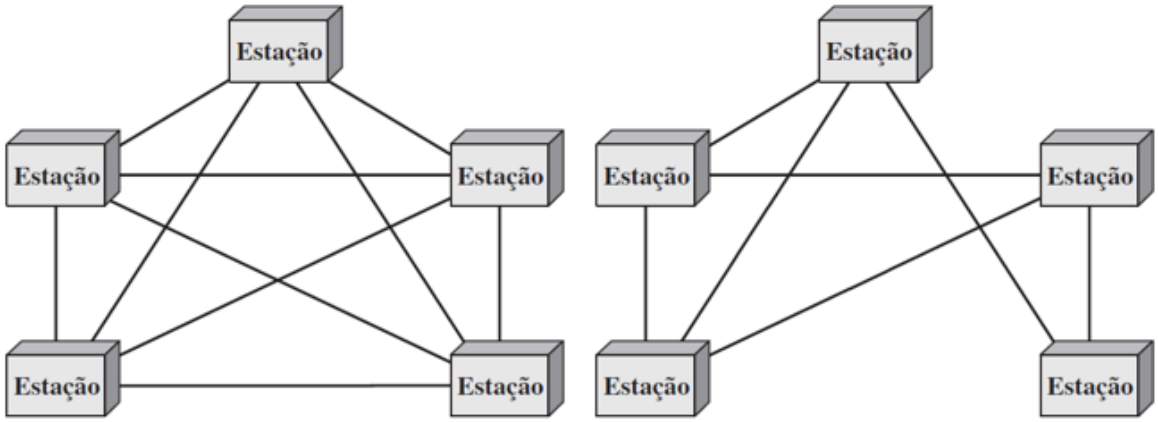
Trata-se da topologia mais utilizada atualmente por facilitar a adição de novas estações de trabalho e pela fácil identificação ou isolamento de falhas. No primeiro caso, para adicionar ou remover uma nova estação de trabalho, basta conectá-la ou desconectá-la da porta do nó central. No segundo caso,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

Vantagens: Robusto a falhas individuais de dispositivos (exceto o hub central). Fácil de gerenciar e adicionar novos dispositivos.

Desvantagens: Se o hub central falhar, toda a rede cai. Custo maior devido ao uso de um hub central.

Topologia de Malha:

Na topologia de malha, cada dispositivo está conectado a todos os outros dispositivos na rede, geralmente usada para redes com requisitos de alta redundância.



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.

As principais desvantagens de uma topologia em malha estão relacionadas à escalabilidade e ao custo, isto é, crescimento da quantidade de cabeamento e o número de portas necessárias para sua implementação. Em primeiro lugar, como cada dispositivo tem de estar conectado a cada um dos demais, a instalação e a reconstrução são trabalhosas. Em segundo, o volume de cabos pode ser maior que o espaço disponível seja capaz de acomodar (nas paredes, tetos ou pisos). Finalmente, o hardware necessário para conectar cada link (portas, placas e/ou cabos) pode ter um custo proibitivo. Por tais razões, uma topologia de malha normalmente é implementada de forma limitada, para poucas máquinas.

Vantagens: Alta redundância e robustez. Se um dispositivo falhar, a rede ainda pode funcionar.

Desvantagens: É cara e complexa de implementar e gerenciar devido ao grande número de conexões necessárias.

A tabela a seguir resume as topologias e seus tipos de enlace e direção de transmissão:

TOPOLOGIA física	DIREÇÃO DE TRANSMISSÃO	Tipo de ENLACE
Barramento	Half-Duplex	Multiponto
Anel	Simplex	Ponto-a-Ponto
Estrela	Half-Duplex (se usar Hub)	Ponto-a-Ponto

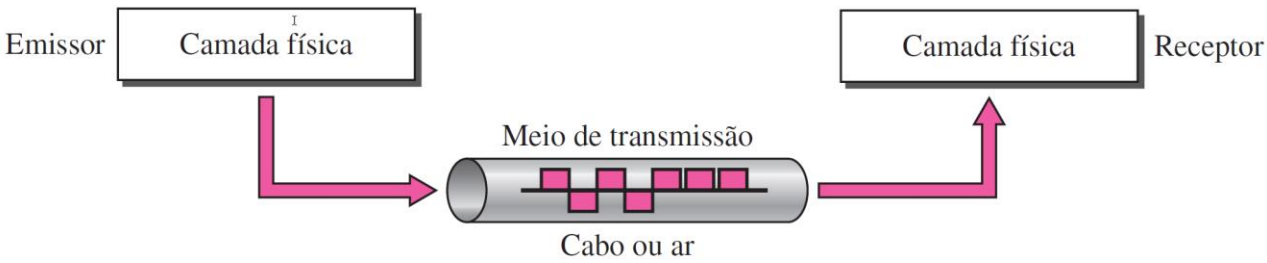
	Full-Duplex (se usar Switch)	
Malha	Depende	Ponto-a-Ponto

Meios de Transmissão

Os meios de transmissão referem-se ao material físico que é usado para enviar informações de um dispositivo para outro em uma rede. Vamos abordar três meios comuns de transmissão: Cabo Coaxial, Par Trançado e Fibra Óptica.

Em telecomunicações, meios de transmissão são divididos em duas categorias: meios guiados e não-guiados.

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



Cabo Coaxial

O cabo coaxial é composto por um núcleo de cobre condutor envolvido por uma camada isolante, que é então envolvida por uma blindagem de malha de cobre, e finalmente por uma capa exterior. Ele é chamado de "coaxial" porque os dois condutores estão ao longo do mesmo eixo.

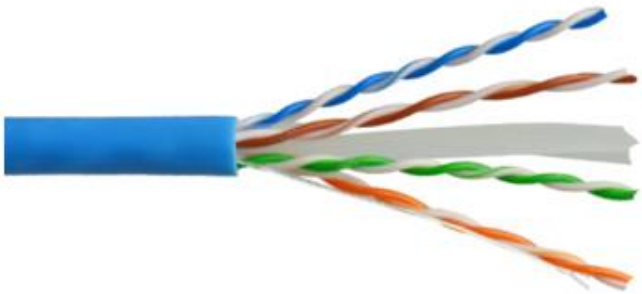
Foi utilizado até meados da década de 90 em redes de computadores, quando começou a ser substituído pelo cabo de par trançado. Ele ainda é utilizado em telecomunicações, basta dar uma olhadinha no decodificador da sua TV por Assinatura. **O cabo que chega na sua casa/prédio e que entra em um modem é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

Vantagens: O cabo coaxial tem uma grande capacidade de largura de banda e pode ser usado em longas distâncias. A blindagem oferece uma boa proteção contra interferências e ruídos.

Desvantagens: É mais caro e mais difícil de instalar do que o cabo de par trançado.

Cabo de Par Trançado

Este cabo é feito de pares de fios de cobre trançados. A versão não blindada (UTP) é a mais comum. A versão blindada (STP) adiciona uma camada de blindagem para melhor proteção contra interferências.



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.

Veja as possíveis categorias de cabos de par trançado:

CATEGORIA	taxa máxima de transmissão	Largura de banda	DISTÂNCIA MÁXIMA
CAT3	Até 10 MBPS	16 MHz	100 Metros
CAT4	Até 16 MBPS	20 MHz	100 Metros
CAT5	Até 100 MBPS	100 MHz	100 Metros
CAT5e	Até 1000 MBPS (1G)	100 MHz	100 Metros
CAT6	Até 10000 MBPS (10G)	250 MHz	100 Metros
CAT6A	Até 10000 MBPS (10G)	500 MHz	100 Metros
CAT7	Até 10000 MBPS (10G)	600 MHz	100 Metros
CAT7A	Até 10000 MBPS (10G)	1000 MHz	100 Metros
CAT8	Até 40000 MBPS (40G)	2000 MHz	100 Metros

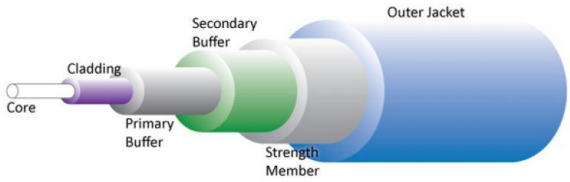
Os cabos de par trançado possuem quatro pares de fios, sendo alguns utilizados para transmissão e outros para recepção, permitindo uma comunicação *full duplex*. Para facilitar a identificação, os pares são coloridos e a ordem dos fios dentro do conector é padronizada. Eles podem ser utilizados na transmissão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

Vantagens: O cabo de par trançado é barato e fácil de instalar. É adequado para a maioria das aplicações de rede doméstica e empresarial.

Desvantagens: Ele tem uma menor capacidade de largura de banda em comparação com o cabo coaxial e a fibra óptica. A versão não blindada é suscetível a interferências e ruídos.

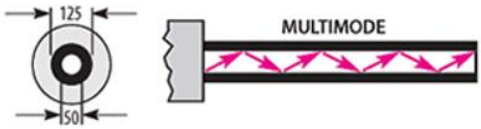
Cabo de Fibra Ótica

A fibra óptica usa feixes de luz para transmitir informações, em vez de sinais elétricos. Um cabo de fibra óptica é composto por um ou mais fios de fibra, cada um revestido por várias camadas de material protetor.

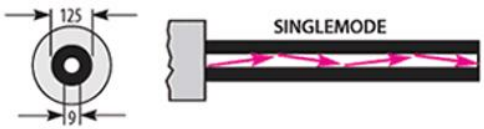


Consiste em uma Casca e um Núcleo (em geral, de vidro) para transmissão de luz. Possui capacidade de transmissão virtualmente infinita, é imune a interferências eletromagnéticas e consegue ligar distâncias maiores sem a necessidade de repetidores. Como desvantagens, ele é incapaz de fazer curvas acentuadas, além de ter um custo de instalação e manutenção muito alto em relação ao par trançado

Há dois tipos de fibra: **Monomodo e Multimodo**.



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



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

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

Vantagens: A fibra óptica tem uma capacidade de largura de banda extremamente alta e pode transmitir dados a grandes distâncias. Ela é imune a interferências eletromagnéticas e fornece uma excelente segurança dos dados.

Desvantagens: A fibra óptica é mais cara e requer equipamentos e habilidades especializadas para instalar e manter.

Padrões de Redes

Padrões de Redes são uma especificação completamente testada que é útil e seguida por aqueles que trabalham com Internet – trata-se de uma regulamentação formal que deve ser seguida. **O Padrão IEEE 802 é um grupo de normas que visa padronizar redes locais e metropolitanas nas camadas física e de enlace do Modelo OSI.** Na tabela a seguir, é possível ver diversos padrões diferentes de redes de computadores:

PADRÃO	NOME
IEEE 802.3	Ethernet (LAN)
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)

Nesta aula, iremos abordar cinco padrões de redes comuns: Ethernet, Token Ring, Wireless, Bluetooth e WiMAX.

Padrão Ethernet (IEEE 802.3)

Ethernet é o padrão de tecnologia mais amplamente utilizado para redes locais de computadores (LANs). Foi desenvolvido no início da década de 1970 por Robert Metcalfe e seus colegas da Xerox PARC e tornou-se o padrão de fato para LANs em todo o mundo devido à sua confiabilidade, velocidade e flexibilidade.

Estrutura e Operação:

A Ethernet usa um método de acesso chamado CSMA/CD (Carrier Sense Multiple Access with Collision Detection) para transmitir dados entre dispositivos em uma rede. Cada dispositivo na rede verifica se o meio de transmissão (o cabo Ethernet) está livre antes de transmitir. Se dois dispositivos tentarem transmitir ao mesmo tempo, ocorrerá uma colisão. Quando isso acontece,

os dispositivos detectam a colisão, param de transmitir e depois tentam novamente após um período de tempo aleatório.

CSMA/CD:

CSMA/CD é um protocolo de controle de acesso ao meio (MAC) utilizado principalmente em redes Ethernet. Vamos destrinchar este acrônimo para entender melhor:

- **Carrier Sense (Verificação de Portadora)**: Significa que cada dispositivo na rede "ouve" ou verifica o meio de transmissão antes de enviar dados. Se o meio estiver ocupado (ou seja, se os dados estiverem sendo transmitidos), o dispositivo aguardará até que o meio esteja livre.
- **Multiple Access (Acesso Múltiplo)**: Significa que todos os dispositivos na rede têm permissão para acessar o meio de transmissão e enviar dados. Não há um dispositivo de controle central que gerencie quem pode e quem não pode transmitir.
- **Collision Detection (Detecção de Colisão)**: Refere-se à capacidade do dispositivo de detectar se uma colisão ocorreu. Uma colisão ocorre quando dois dispositivos transmitem dados ao mesmo tempo. Se uma colisão for detectada, cada dispositivo interromperá sua transmissão, aguardará um período de tempo aleatório e tentará transmitir novamente.

No geral, o CSMA/CD é um método de gerenciamento de tráfego em redes onde os dispositivos podem começar a transmitir sempre que detectam que o canal está inativo. Se ocorrer uma colisão, os transmissores param e tentam transmitir novamente após um intervalo de tempo aleatório. Isso garante que todos os dispositivos na rede tenham uma chance justa de transmitir seus dados, minimizando ao mesmo tempo as colisões.

Cabeamento:

Existem vários tipos diferentes de cabos usados em redes Ethernet, incluindo cabo coaxial, cabo de par trançado (como Cat5, Cat6 e Cat7) e fibra óptica. O tipo de cabo usado depende das necessidades específicas da rede, como a distância entre dispositivos, a velocidade de transmissão necessária e o ambiente de rede.

Switches e Roteadores:

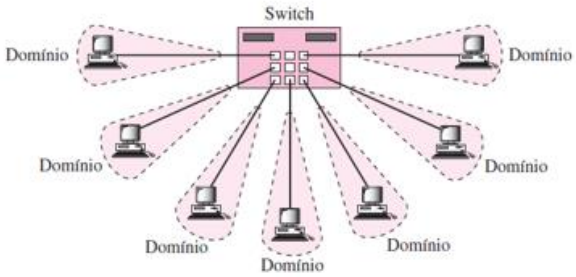
Um switch Ethernet conecta vários dispositivos em uma rede local, permitindo que eles comuniquem diretamente entre si a altas velocidades. Um roteador Ethernet conecta redes locais a outras redes, incluindo a Internet, permitindo a comunicação entre dispositivos em redes diferentes.

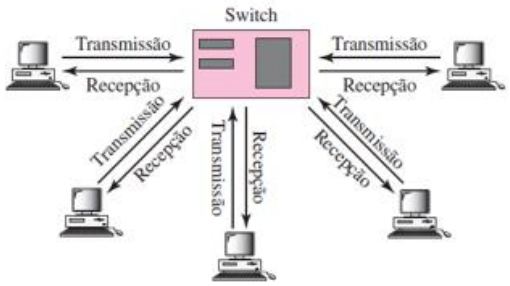
Um switch ou roteador é importante em uma rede Ethernet para diminuir o Domínio de Colisão da rede.

Um **domínio de colisão**, no contexto de redes de computadores, é uma parte da rede onde pacotes de dados podem colidir uns com os outros ao serem enviados ao mesmo tempo. Em uma rede Ethernet, por exemplo, se dois dispositivos na mesma rede tentarem transmitir dados simultaneamente, isso pode resultar em uma colisão de dados. Essa área da rede onde as colisões podem ocorrer é conhecida como um "domínio de colisão".

Agora, um switch de rede ou roteador pode ser usado para dividir uma grande rede em múltiplos e menores domínios de colisão, cada um com um número menor de dispositivos. Isso é feito para aumentar a eficiência geral da rede, minimizando a possibilidade de colisões.

Um switch de rede é capaz de criar domínios de colisão separados para cada uma de suas portas. Portanto, se você tem um switch com 24 portas, você tem 24 domínios de colisão separados. Isso é possível porque um switch é um dispositivo inteligente que mantém uma tabela de endereços MAC de todos os dispositivos conectados. Quando um pacote chega, o switch sabe exatamente para qual porta encaminhar o pacote, eliminando a necessidade de enviar o pacote para todas as outras portas (como acontece com um hub), o que por sua vez reduz a chance de colisões.

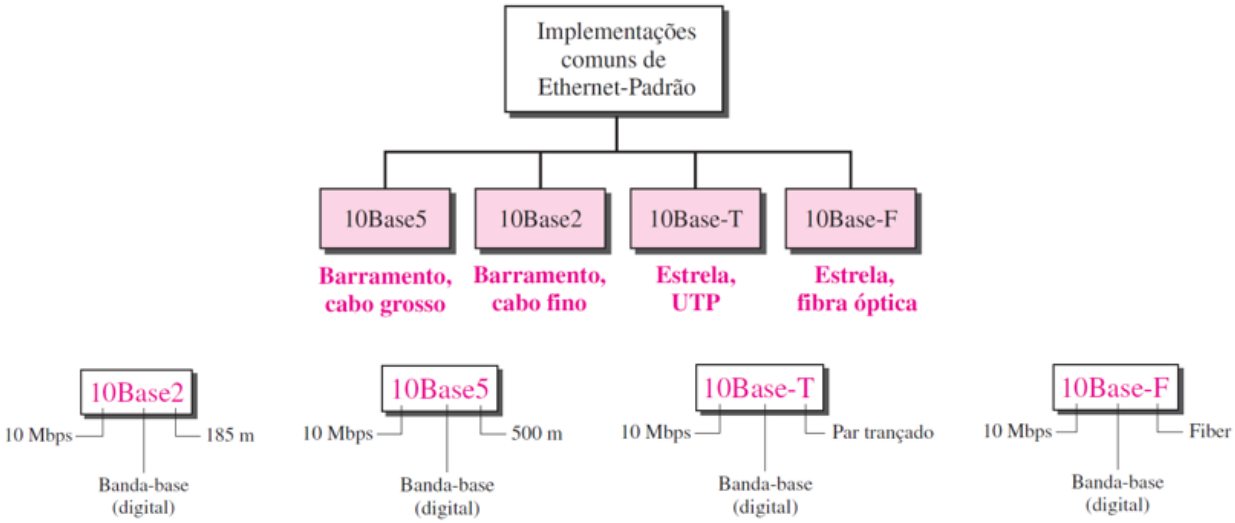




Os roteadores também ajudam a dividir uma rede em diferentes domínios de colisão, mas eles vão além e também dividem a rede em diferentes domínios de broadcast. Um domínio de broadcast é a parte da rede onde os pacotes de broadcast (pacotes destinados a todos os dispositivos na rede) podem alcançar. Cada porta em um roteador é um domínio de colisão separado e também um domínio de broadcast separado. Ao separar os domínios de broadcast, os roteadores podem melhorar ainda mais o desempenho da rede, pois os pacotes de broadcast não sobrecarregam os dispositivos que não precisam deles.

Evoluções (Gerações) da Ethernet:

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



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

EVOLUÇÃO DOS PADRÕES ETHERNET	
PADRÃO (CABO DE PAR TRANÇADO ou fibra óptica)	PADRÃO – TAXA máxima DE TRANSMISSÃO
Ethernet	10BASE-T / 10 Mbps
Fast Ethernet	100BASE-T / 100 Mbps
Gigabit Ethernet	1000BASE-T / 1000 Mbps
10G Ethernet	10GBASE-T / 10000 Mbps

Vantagens e Desvantagens:

Como vantagens, podemos citar que Ethernet é um padrão maduro e comprovado, com suporte generalizado em praticamente todos os dispositivos de rede modernos. Ele fornece uma conexão de rede confiável e de alta velocidade, e o custo do equipamento Ethernet e do cabeamento é relativamente baixo.

No entanto, a Ethernet também tem algumas desvantagens. A instalação de cabos Ethernet pode ser problemática em alguns ambientes e a necessidade de cabos físicos limita a mobilidade dos dispositivos conectados. Além disso, como a Ethernet usa CSMA/CD para gerenciar a transmissão de dados, o desempenho pode diminuir em redes muito ocupadas devido a colisões.

Padrão Token Ring (IEEE 802.5)

Token Ring é um protocolo de rede que foi desenvolvido e patenteado pela IBM na década de 1980. Embora seja menos comum hoje em dia, por ter sido amplamente substituído pelo Ethernet em muitos contextos, o Token Ring foi uma tecnologia de rede importante e influente. Vamos discutir sua estrutura, operação, vantagens e desvantagens.

Estrutura e Operação:

Em uma rede Token Ring, as máquinas estão dispostas em uma configuração lógica de anel, embora a estrutura física possa não ser um anel. A comunicação entre máquinas é gerenciada por uma "testemunha" ou "token" que circula pela rede.

Funciona assim: uma máquina na rede pode transmitir dados apenas quando possui o token. Quando uma máquina conclui sua transmissão, ela passa o token para a próxima máquina no anel. Isso continua em torno do anel, com cada máquina tendo a chance de transmitir quando recebe o token.

Evolução do Token Ring:

As redes Token Ring originalmente operavam a 4 Mbps, mas as versões posteriores aumentaram essa velocidade para 16 Mbps. Versões ainda mais recentes do protocolo, como FDDI (Fiber Distributed Data Interface) e CDDI (Copper Distributed Data Interface), conseguem operar a velocidades de até 100 Mbps.

Cabeamento Token Ring:

Assim como o Ethernet, o Token Ring pode usar vários tipos de cabos. As redes Token Ring geralmente usam um cabo de par trançado, mas também podem usar cabo coaxial ou fibra óptica.

Vantagens e Desvantagens:

Uma grande vantagem do Token Ring é que ele evita colisões que podem ocorrer em redes Ethernet ao usar o token para gerenciar o acesso ao meio de transmissão. Isso pode resultar em um melhor desempenho em redes muito ocupadas.

No entanto, as redes Token Ring tendem a ser mais caras de instalar e manter do que as redes Ethernet, em parte porque o equipamento Token Ring é menos comum e, portanto, geralmente mais caro. Além disso, a falha de uma única máquina pode potencialmente interromper toda a

rede, embora muitas redes Token Ring sejam configuradas para evitar isso "pulando" máquinas inativas.

No geral, embora as redes Token Ring sejam menos comuns hoje do que no passado, elas ainda têm usos em determinados contextos, especialmente onde a alta demanda e a colisão de tráfego podem ser um problema para as redes Ethernet.

Padrão Wi-Fi (802.11)

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

Componentes principais de uma rede Wi-Fi:

- **Estação**: Uma estação é qualquer dispositivo que possa se conectar a uma rede Wi-Fi. Pode ser um computador, smartphone, tablet, smart TV, etc.
- **Ponto de acesso (Access Point - AP)**: Um ponto de acesso é um dispositivo que permite que as estações se conectem à rede sem fio. Ele transmite um sinal de Wi-Fi que as estações podem detectar e se conectar.

Como o Wi-Fi funciona:

O Wi-Fi opera em bandas de frequência específicas que estão disponíveis para uso sem necessidade de licença. As mais comuns são 2,4 GHz e 5 GHz. Dentro dessas bandas de frequência, há canais específicos que podem ser selecionados para uso.

O Wi-Fi usa ondas de rádio para transmitir informações entre seu dispositivo e um roteador próximo. Os dados são enviados e recebidos através de ondas de rádio, e é assim que as informações como e-mails, páginas da web ou música chegam ao seu dispositivo.

Versões do Padrão IEEE 802.11:

O padrão IEEE 802.11 tem várias versões, incluindo 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax, que também são conhecidos por nomes de marca como Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac) e Wi-Fi 6 (802.11ax).

Cada uma dessas versões melhorou a velocidade, o alcance ou a eficiência da transmissão de dados em relação à versão anterior. Por exemplo, o 802.11n (Wi-Fi 4) introduziu a tecnologia MIMO (Multiple Input Multiple Output), que permite o uso de várias antenas para melhorar o desempenho, enquanto o 802.11ac (Wi-Fi 5) opera apenas na frequência de 5 GHz e permite uma largura de canal mais ampla, o que leva a uma velocidade de transmissão de dados mais rápida. O 802.11ax (Wi-Fi 6) melhorou a eficiência em ambientes com muitos dispositivos conectados e também a velocidade máxima de transmissão de dados.

A tabela a seguir resume a evolução das versões de Wi-Fi:

EVOLUÇÃO DO PADRÃO wi-fi (802.11)[1]		
PADRÃO	FREQUÊNCIA	TAXA máxima DE TRANSMISSÃO
IEEE 802.11b	2.4 Ghz	11 Mbps
IEEE 802.11a	5.0 Ghz	54 Mbps
IEEE 802.11g	2.4 Ghz	54 Mbps
IEEE 802.11n	2.4 ou 5.0 Ghz	150, 300 até 600 Mbps
IEEE 802.11ac	5.0 Ghz	500 Mbps, 1 Gbps ou +

Segurança:

As redes Wi-Fi podem ser protegidas por várias medidas de segurança, como WEP, WPA, WPA2 e a mais recente WPA3. Essas tecnologias criptografam os dados transmitidos pela rede para protegê-los de interceptação não autorizada.

Veja alguns riscos aos quais redes Wi-Fi estão suscetíveis:

RISCOS DE REDES wireless
Por se comunicarem por meio de sinais de rádio, não há a necessidade de acesso físico a um ambiente restrito, como ocorre com as redes cabeadas. Por essa razão, dados transmitidos por clientes legítimos podem ser interceptados por qualquer pessoa próxima com um mínimo de equipamento (Ex: um notebook ou tablet).
Por terem instalação bastante simples, muitas pessoas as instalam em casa (ou mesmo em empresas, sem o conhecimento dos administradores de rede), sem qualquer cuidado com configurações mínimas de segurança, e podem vir a ser abusadas por atacantes, por meio de uso não autorizado ou de "sequestro".
Em uma rede wireless pública (como as disponibilizadas – por exemplo – em aeroportos, hotéis, conferências, etc) os dados que não estiverem criptografados podem ser indevidamente coletados e lidos por atacantes.

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

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

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

WEP (*Wired Equivalent Privacy*): primeiro mecanismo de segurança a ser lançado – é considerado frágil e, por isto, o uso deve ser evitado;

WPA (*Wi-Fi Protected Access*): mecanismo desenvolvido para resolver algumas das fragilidades do WEP – é o nível mínimo de segurança que é recomendado atualmente;

WPA-2 (*Wi-Fi Protected Access 2*): similar ao WPA, mas com criptografia considerada mais forte – é o mecanismo mais recomendado atualmente.

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

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

Infraestrutura: comunicação que faz uso de equipamento para centralizar fluxo da informação na WLAN (Ex: Access Point ou Hotspot) e permite um alcance maior (Ex: 500m). Em outras palavras, toda comunicação entre equipamentos deve passar pelo Access Point.

Padrão Bluetooth (802.15)

Bluetooth é uma tecnologia de rede sem fio projetada para a transferência de dados em curta distância. Desenvolvida pela Ericsson em 1994, a tecnologia Bluetooth é agora gerenciada pelo Bluetooth Special Interest Group (SIG).

Como o Bluetooth funciona:

O Bluetooth opera na faixa de frequência de 2,4 GHz, que é a mesma faixa utilizada por muitos outros dispositivos sem fio, incluindo o Wi-Fi. No entanto, o Bluetooth usa uma técnica chamada "espalhamento espectral por salto em frequência" para minimizar a interferência. Isso significa que ele muda rapidamente de frequência (ou "salta") dentro da banda de 2,4 GHz, tornando menos provável que interfira ou seja interferido por outros dispositivos.

Pares e Conexões:

Uma das características mais notáveis do Bluetooth é a sua capacidade de emparelhar dispositivos. Quando dois dispositivos Bluetooth estão próximos um do outro, eles podem estabelecer uma conexão ou "pareamento". Uma vez emparelhados, os dispositivos podem se comunicar uns com os outros automaticamente sem a necessidade de configurações adicionais.

Classes de Bluetooth:

Existem várias classes de dispositivos Bluetooth, cada uma com um alcance diferente. Por exemplo, a Classe 1 é a mais poderosa, com um alcance de até 100 metros. A Classe 2 é a mais comum em dispositivos móveis, com um alcance de até 10 metros. A Classe 3 é a menos poderosa, com um alcance de apenas cerca de 1 metro.

Veja na tabela:

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

Perfis Bluetooth:

O Bluetooth suporta muitos "perfis" diferentes, que são especificações para como a tecnologia é usada para uma determinada finalidade. Alguns perfis comuns incluem o perfil de distribuição de áudio avançado (A2DP) para áudio de alta qualidade, o perfil de controle remoto de áudio/vídeo (AVRCP) para controle remoto de dispositivos de mídia, e o perfil de fone de ouvido (HSP) para fones de ouvido e microfones.

Bluetooth LE (Low Energy):

Bluetooth Low Energy (BLE), também conhecido como Bluetooth Smart, foi introduzido com a versão 4.0 do padrão Bluetooth. BLE é uma versão de energia mais eficiente do Bluetooth projetada para dispositivos de baixo consumo de energia, como sensores de fitness, rastreadores de localização e dispositivos vestíveis.

Padrão WiMAX

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

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

QUESTÕES ESTRATÉGICAS

Nesta seção, apresentamos e comentamos uma amostra de questões objetivas selecionadas estrategicamente: são questões com nível de dificuldade semelhante ao que você deve esperar para a sua prova e que, em conjunto, abordam os principais pontos do assunto.

A ideia, aqui, não é que você fixe o conteúdo por meio de uma bateria extensa de questões, mas que você faça uma boa revisão global do assunto a partir de, relativamente, poucas questões.

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

a) WPA.

b) WiFi.

c) WPS.

d) WEP.

e) WPA2.

Comentários:

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

Gabarito: Letra E

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

a) Satélite.

b) PLC (comunicação pelo cabo de energia).

c) Fibra ótica.

d) Sem fio Wi-Fi.

e) Cabo ADSL.

Comentários:

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

Gabarito: Letra C

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

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

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

a) Portal Internet.

b) Servidor.

c) Web server.

d) Cliente Internet.

e) Provedor.

Comentários:

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

Gabarito: Letra E

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

a) TI-578.

b) RX-45.

c) RJ-45.

d) BSI-8.

e) ATC-32.

Comentários:

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

Gabarito: Letra C

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

a) SSID.

b) TKP

c) WEP.

d) WiFi.

e) WPA.

Comentários:

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

Gabarito: Letra E

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

a) 11 Mbps.

b) 20 Mbps.

c) 54 Mbps.

d) 100 Mbps.

e) 200 Mbps.

Comentários:

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 +

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

Gabarito: Letra A

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

a) Anel.

b) Estrela.

c) Distribuída.

d) Ramificada.

e) Barramento.

Comentários:

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

Gabarito: Letra B

8. **(FCC / Prefeitura de São José do Rio Preto/SP – 2019)** Ao entrar em contato com a Central de Serviços da organização onde trabalha para relatar dificuldades em conectar o computador à internet, o atendente solicitou ao Agente Administrativo a realização de um procedimento que envolvia a identificação de um componente da rede conhecido como RJ45, que é:

a) o conector na extremidade do cabo de rede.

b) o botão usado para reiniciar o roteador.

c) o aparelho que transmite o sinal de internet via wireless.

d) a antena do roteador de internet.

e) o cabo de rede que liga o roteador ao computador.

Comentários:

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

Gabarito: Letra A

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

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

b) Uma empresa possui um enorme volume de dados e precisa interligar o servidor principal aos outros computadores. Para permitir esta conexão deve-se utilizar uma SAN − Servidor Area Network que conecta diversas máquinas a um servidor central.

c) Há diversos dispositivos em uma residência que precisam se comunicar dentro de uma distância bastante limitada. Para isso deve ser utilizada uma rede PAN − Private Area Network, que utiliza tecnologias como Wi-Fi e bluetooth.

d) Deseja-se conectar redes de escritórios de uma mesma empresa ou de vários campi de universidades. A melhor solução é utilizar uma WLAN − Wireless Local Area Network, a versão wireless (sem fio) de uma LAN que alcança centenas de quilômetros.

e) Uma empresa presta serviços online 24 horas para países localizados em diferentes continentes. Deve-se utilizar uma WAN − Wide Area Network, que vai além da MAN − Metropolitan Area Network, conseguindo alcançar uma área maior, como um país ou mesmo um continente.

Comentários:

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

Gabarito: Letra E

10. **(FCC / DPE-RS – 2017)** Considere uma rede de computadores instalada e em funcionamento que é caracterizada pelo seu alcance local, por se tratar de uma rede interna de curto alcance. De acordo com sua extensão geográfica, essa rede é classificada como: a) Metropolitan Area Network − MAN.

b) Local Area Network − LAN.

c) Wide Area Network − WAN.

d) Storage Area Network − SAN.

e) Popular Area Network − PAN.

Comentários:

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

Gabarito: Letra B

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

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

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

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

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

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

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

a) I, II e III.

b) I, III e IV.

c) III e IV.

d) I e II.

e) II e IV.

Comentários:

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

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

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

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

Gabarito: Letra A

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

a) 5 ou superior

b) 5a ou superior

c) 6a

d) 5e ou 6e

e) 6 ou superior

Comentários:

CATEGORIA	Taxa máxima de transmissão	Largura de banda	DISTÂNCIA MÁXIMA
CAT3	Até 10 MBPS	16 MHz	100 Metros
CAT4	Até 16 MBPS	20 MHz	100 Metros
CAT5	Até 100 MBPS	100 MHz	100 Metros
CAT5e	Até 1000 MBPS (1G)	100 MHz	100 Metros
CAT6	Até 10000 MBPS (10G)	250 MHz	100 Metros
CAT6A	Até 10000 MBPS (10G)	500 MHz	100 Metros
CAT7	Até 10000 MBPS (10G)	600 MHz	100 Metros
CAT7A	Até 10000 MPBS (10G)	1000 MHz	100 Metros
CAT8	Até 40000 MBPS (40G)	2000 MHz	100 Metros

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

Gabarito: Letra A

13. **(FGV / COMPESA – 2016)** As redes de difusão admitem diversas topologias. Com relação às redes de difusão, analise as afirmativas a seguir.

I. Em uma rede de difusão de barramento, em um dado instante, pode haver, no máximo, uma máquina desempenhando a função de mestre e podendo realizar uma transmissão.

II. Em uma rede Ethernet, se dois ou mais pacotes colidirem, cada computador fará uma nova tentativa de reenvio do seu pacote no momento em que a colisão é sinalizada.

III. Em uma topologia em anel típica não há a necessidade de se definir alguma regra para arbitrar os acessos simultâneos ao anel.

Está correto o que se afirma em:

a) I, apenas.

b) II, apenas.

c) III, apenas.

d) I e II, apenas.

e) I, II e III.

Comentários:

(I) Correto. Em um barramento, em qualquer instante, no máximo uma máquina poderá realizar uma transmissão e ela será chamada de mestre. Nesse momento, outras máquinas serão impedidas de enviar qualquer tipo de mensagem, sendo necessário haver um mecanismo para detectar colisões; (II) Errado, se fosse no momento em que a colisão era sinalizada, ambos enviariam novamente e haveria uma nova colisão. Logo, cada computador fará uma nova tentativa de reenvio do seu pacote em um tempo aleatório para evitar nova colisão; (III) Errado, há necessidade de se definir algum mecanismo para arbitrar os acessos simultâneos ao anel – esse mecanismo é a posse do token.

Gabarito: Letra A

14. **(FGV / Câmara Municipal de Caruaru – PE – 2015)** As figuras a seguir ilustram a topologia e o conector empregado nos cabos de par trançado UTP, utilizados na implementação da rede de computadores padrão Ethernet, com acesso à Internet, da Câmara Municipal de Caruaru.

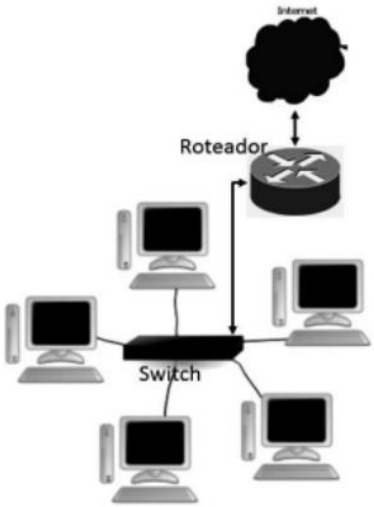


Figura I

Figura II

A topologia física e a sigla pelo qual é conhecido o conetor são, respectivamente,

a) estrela e RG58.

b) barramento e RG586

c) anel e RJ45

d) barramento e RJ45

e) estrela e RJ-45

Comentários:

A Topologia Física é claramente uma Topologia em Estrela, visto que as estações estão ligadas através de uma conexão ponto-a-ponto dedicada a um nó central controlador – no caso, um switch. E o conector é claramente um Conector RJ-45, responsável por conectar cabos de par trançado.

Gabarito: Letra E

15. (FGV / SUSAM – 2014) As figuras a seguir mostram a tecnologia e o tipo de cabo empregados na implementação das atuais redes de computadores *Fast Ethernet* cabeadas.

Figura I

Figura II

A conexão é feita por meio desse cabo, com um conector específico e utiliza a um link ponto a ponto entre e o computador e a porta do concentrador.

A topologia física e o conector são conhecidos, respectivamente, por:

a) estrela e RJ-45.

b) estrela e HDMI.

c) anel e RJ-45.

d) barramento e HDMI.

e) barramento e RJ 45.

Comentários:

A Topologia Física é claramente uma Topologia em Estrela, visto que as estações estão ligadas através de uma conexão ponto-a-ponto dedicada a um nó central controlador – no caso, um concentrador. E o conector é claramente um Conector RJ-45, responsável por conectar cabos de par trançado.

Gabarito: Letra A

16. (FGV / AL-MT – 2013) Com relação à tecnologia estrela utilizada na implementação de redes de computadores, assinale V para a afirmativa verdadeira e F para a falsa.

( ) Desabilita um link em caso de falha, permanecendo os demais ativos.

( ) Utiliza ligações multiponto nas conexões, exceto a do servidor que é ponto a ponto dedicado.

( ) Obriga o remanejamento de todas as conexões, quando da integração de uma nova máquina à rede.

As afirmativas são, respectivamente,

a) F, V e F

b) F, V e V

c) V, F e F

d) V, V e F

e) F, F e V

Comentários:

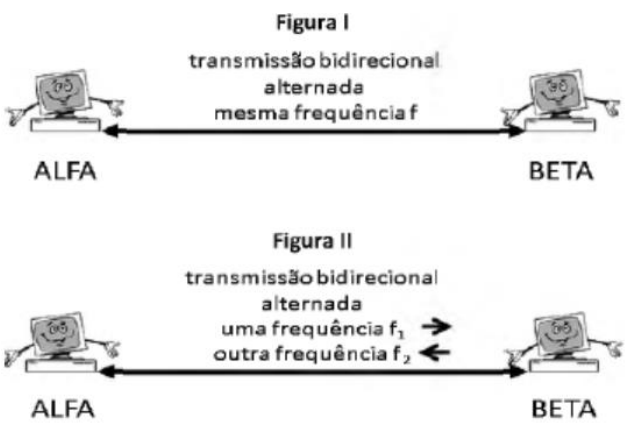
(I) Verdadeiro. Na topologia em estrela, um problema afeta apenas um nó – os restantes permanecem ativos.

(II) Falso. Só há ligações entre estação e nó central e, não, entre estações – e são ponto-a-ponto.

(III) Falso. Não é necessário remanejar as conexões ao adicionar novas máquinas na rede.

Gabarito: Letra C

17. As figuras I e II representam dois modos de transmissão de dados.



Os modos I e II são denominados, respectivamente,

a) half-duplex e full-duplex.

b) full-duplex e half-duplex.

c) full-duplex e biplex.

d) simplex e biplex.

e) biplex e simplex.

Comentários:

Observem que a imagem mostra uma transmissão bidirecional, logo não pode ser um modo de transmissão *simplex*. Observem também que, na Figura I, temos transmissor e receptor se comunicando na mesma frequência, logo só pode ser uma comunicação *half-duplex*, caso contrário haveria uma colisão na troca de mensagens. Já na Figura II, temos transmissor e receptor se comunicando em frequências diferentes, logo só pode ser uma comunicação *full-duplex*, dessa forma não há chances de colisão.

Gabarito: Letra A

18. **(CESGRANRIO / CEF –2021)** A computação distribuída permite que as máquinas integrantes de uma rede, que utiliza esse modelo computacional, executem o seu próprio processamento. Esse cenário permite que as organizações se beneficiem da integração de serviços, por meio da interconexão oferecida pelas redes de computadores, otimizando recursos e maximizando o poder de seu parque computacional. Nesse cenário, o modelo de redes ponto a ponto se caracteriza por:

a) agrupar um conjunto de computadores, localizados em ambientes físicos distintos, para processar grandes volumes de dados.

b) existir um servidor frontal (front-end) que se comunica com outro servidor traseiro (back-end), este responsável pelos dados do processamento.

c) inexistir a figura de um servidor dedicado, já que qualquer equipamento pode desempenhar a função de servidor de um determinado serviço.

d) interligar um conjunto de computadores, de forma que pareça um supercomputador com considerável poder computacional.

e) oferecer um modelo em que existe a figura de um equipamento servidor, responsável por atender às requisições de equipamentos clientes.

Comentários:

(a) Errado. A descrição se assemelha mais a uma rede de computação em grade (grid computing) do que a uma rede ponto a ponto;

(b) Errado. Este cenário descreve uma arquitetura cliente-servidor com servidores front-end e back-end, não uma rede ponto a ponto;

(c) Correto. Em uma rede ponto a ponto, não existe a figura de um servidor dedicado. Qualquer equipamento na rede pode atuar tanto como cliente quanto como servidor;

(d) Errado. Interligar computadores para parecer um supercomputador é característico da computação em grade, não de redes ponto a ponto;

(e) Errado. Este cenário descreve uma rede cliente-servidor, onde um equipamento servidor centralizado atende às requisições dos clientes, o que não é característico de redes ponto a ponto.

Gabarito: Letra C

19. **(CESGRANRIO / CEFET-RJ – 2014)** Os tipos de rede digital podem ser classificados em função dos seus alcances geográficos. A rede com alcance de até 500 metros, utilizada em escritórios ou andares de um edifício, é denominada rede local e é conhecida pela sigla:

a) LAN

b) RAN

c) CAN

d) MAN

e) WAN

Comentários:

Apesar de a questão ter mencionado um alcance de até 500 metros, não se atenham tanto a medidas precisas – pensem sempre em uma variação de valores! Até 500 metros é uma LAN.

Gabarito: Letra A

20. **(CESGRANRIO / TRANSPETRO – 2011)** A figura abaixo mostra uma topologia típica de uma rede industrial de comunicação onde todos os dispositivos compartilham o mesmo meio físico de comunicação. O controle pode ser centralizado ou distribuído. Além de possuir alto poder de expansão, nós com falha não prejudicam necessariamente os demais. Qual a topologia descrita?

a) Anel

b) Barramento

c) Ponto-a-Ponto

d) Árvore

e) Estrela

Comentários:

Como todos os dispositivos compartilham o mesmo meio físico de comunicação, com alto poder de expansão e cuja falha em um nó não prejudicam necessariamente os demais, trata-se da topologia em barramento. Quando a questão fala que o controle pode ser centralizado ou

distribuído, eu presumo que ela quis dizer que pode ser utilizado em uma arquitetura cliente-servidor ou em uma arquitetura ponto a ponto.

Gabarito: Letra B

QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

A ideia do questionário é elevar o nível da sua compreensão no assunto e, ao mesmo tempo, proporcionar uma outra forma de revisão de pontos importantes do conteúdo, a partir de perguntas que exigem respostas subjetivas.

São questões um pouco mais desafiadoras, porque a redação de seu enunciado não ajuda na sua resolução, como ocorre nas clássicas questões objetivas.

O objetivo é que você realize uma auto explicação mental de alguns pontos do conteúdo, para consolidar melhor o que aprendeu ;)

Além disso, as questões objetivas, em regra, abordam pontos isolados de um dado assunto. Assim, ao resolver várias questões objetivas, o candidato acaba memorizando pontos isolados do conteúdo, mas muitas vezes acaba não entendendo como esses pontos se conectam.

Assim, no questionário, buscaremos trazer também situações que ajudem você a conectar melhor os diversos pontos do conteúdo, na medida do possível.

É importante frisar que não estamos adentrando em um nível de profundidade maior que o exigido na sua prova, mas apenas permitindo que você compreenda melhor o assunto de modo a facilitar a resolução de questões objetivas típicas de concursos, ok?

Nosso compromisso é proporcionar a você uma revisão de alto nível!

Vamos ao nosso questionário:

Perguntas

1. O que é uma rede de computadores e por que ela é importante?
2. O que diferencia a transmissão de dados no modo simplex, half-duplex e full-duplex?

3. Quais são as diferenças entre unicast, multicast e broadcast?
4. Qual a diferença entre uma rede PAN, LAN, MAN e WAN?
5. Descreva as características principais de uma topologia de rede em estrela.
6. Quais são as vantagens e desvantagens da arquitetura de rede cliente-servidor?
7. O que são meios de transmissão em uma rede e quais os tipos mais comuns?
8. O que é o CSMA/CD e em que tipo de rede ele é comumente usado?
9. O que é um domínio de colisão e como um switch ajuda a controlá-lo?
10. Quais são as características principais da tecnologia Bluetooth e onde ela é comumente usada?
11. O que é o protocolo Ethernet e como ele funciona?
12. O que é o protocolo Token Ring e como ele funciona?
13. Quais são as diferenças entre os protocolos de segurança WEP, WPA e WPA2?
14. O que é WiMAX e onde é comumente usado?
15. O que é um cabo de fibra ótica e quais são suas vantagens sobre outros tipos de cabos?
16. Quais são as principais características das topologias de barramento e anel?
17. Como a arquitetura ponto a ponto difere da arquitetura cliente-servidor?
18. O que são UTP e STP?
19. O que significa se uma fibra óptica é monomodo ou multimodo?
20. O que é um Access Point em uma rede Wi-Fi?

Perguntas e Respostas

1. O que é uma rede de computadores e por que ela é importante?
   Resposta: Uma rede de computadores é um conjunto de computadores e outros dispositivos interconectados que podem compartilhar recursos e informações. Ela é importante porque permite a comunicação e a colaboração eficientes, economizando tempo e esforço e facilitando o compartilhamento de recursos.

2. O que diferencia a transmissão de dados no modo simplex, half-duplex e full-duplex?
   Resposta: Em modo simplex, a transmissão ocorre apenas em uma direção. No half-duplex, a transmissão pode ocorrer em ambas as direções, mas não simultaneamente. No full-duplex, a transmissão pode ocorrer em ambas as direções ao mesmo tempo.

3. Quais são as diferenças entre unicast, multicast e broadcast?
   Resposta: Unicast é uma transmissão de um emissor para um receptor único. Multicast é uma transmissão de um emissor para múltiplos receptores específicos. Broadcast é uma transmissão de um emissor para todos os receptores na rede.

4. Qual a diferença entre uma rede PAN, LAN, MAN e WAN?
   Resposta: A diferença está no alcance geográfico. PAN é uma rede de alcance pessoal,

cobrindo um alcance muito pequeno. LAN é uma rede local, cobrindo, por exemplo, um escritório ou casa. MAN é uma rede metropolitana, cobrindo uma cidade ou área metropolitana. WAN é uma rede de longo alcance, que pode abranger um país ou até mesmo o mundo inteiro.

5. Descreva as características principais de uma topologia de rede em estrela.
   Resposta: Na topologia em estrela, todos os nós estão conectados a um nó central, como um switch ou hub. Se um nó falhar, apenas essa conexão é afetada, tornando a rede bastante robusta. No entanto, se o nó central falhar, toda a rede será afetada.

6. Quais são as vantagens e desvantagens da arquitetura de rede cliente-servidor?
   Resposta: As vantagens incluem centralização do controle, facilidade de manutenção e alta eficiência para grandes redes. As desvantagens incluem dependência do servidor - se o servidor falhar, os serviços serão interrompidos - e potenciais gargalos de desempenho se muitos clientes acessarem o servidor simultaneamente.

7. O que são meios de transmissão em uma rede e quais os tipos mais comuns?
   Resposta: Meios de transmissão são os materiais ou formas através das quais os dados são transmitidos de um dispositivo para outro em uma rede. Os tipos mais comuns são cabos (como cabo coaxial, cabos de par trançado e cabos de fibra óptica) e transmissão sem fio.

8. O que é o CSMA/CD e em que tipo de rede ele é comumente usado?
   Resposta: CSMA/CD (Carrier Sense Multiple Access with Collision Detection) é um método de controle de acesso ao meio que ajuda a minimizar colisões de dados em redes Ethernet. Ele permite que vários dispositivos usem o mesmo meio de transmissão, detectando colisões e fazendo retransmissões quando necessário.

9. O que é um domínio de colisão e como um switch ajuda a controlá-lo?
   Resposta: Um domínio de colisão é uma parte da rede onde pacotes de dados podem colidir uns com os outros. Um switch ajuda a controlar domínios de colisão, pois cada porta do switch representa um domínio de colisão separado, reduzindo a probabilidade de colisões e melhorando o desempenho geral da rede.

10. Quais são as características principais da tecnologia Bluetooth e onde ela é comumente usada?
    Resposta: O Bluetooth é uma tecnologia de rede sem fio de curto alcance que permite a conexão e a comunicação entre dispositivos próximos. Ele é comumente usado para conectar dispositivos como fones de ouvido, teclados, mouses e dispositivos móveis a computadores ou outros dispositivos.

11. O que é o protocolo Ethernet e como ele funciona?
    Resposta: O Ethernet é um padrão de rede usado principalmente em redes LAN. Ele usa o método de controle de acesso ao meio CSMA/CD para permitir que múltiplos dispositivos compartilhem o mesmo meio de transmissão, minimizando as colisões de dados.

12. O que é o protocolo Token Ring e como ele funciona?
    Resposta: Token Ring é um protocolo de rede que opera em uma topologia de anel. Ele usa um "token" que circula pela rede. O nó que possui o token tem o direito de transmitir dados, evitando assim as colisões.

13. Quais são as diferenças entre os protocolos de segurança WEP, WPA e WPA2?
    Resposta: WEP é um protocolo de segurança mais antigo e menos seguro, com várias vulnerabilidades conhecidas. WPA melhorou a segurança, mas ainda tinha algumas fraquezas. WPA2 é o protocolo mais seguro dos três, oferecendo uma criptografia forte e outros recursos de segurança aprimorados.

14. O que é WiMAX e onde é comumente usado?
    Resposta: WiMAX é uma tecnologia de rede sem fio que oferece transmissão de alta velocidade de dados em longas distâncias. É comumente usado para conectar redes LAN a redes WAN, ou para fornecer acesso à internet em áreas onde o acesso por cabo ou DSL não está disponível.

15. O que é um cabo de fibra ótica e quais são suas vantagens sobre outros tipos de cabos?
    Resposta: Um cabo de fibra ótica é um meio de transmissão que usa luz para transmitir dados. Suas vantagens incluem alta capacidade de transmissão de dados (largura de banda), baixa perda de sinal, resistência à interferência eletromagnética e segurança aprimorada.

16. Quais são as principais características das topologias de barramento e anel?
    Resposta: Em uma topologia de barramento, todos os dispositivos estão conectados a um único cabo central, ou "barramento". Uma falha em um dispositivo pode afetar toda a rede. Em uma topologia de anel, os dispositivos estão conectados em um loop fechado, e os dados circulam em uma única direção ao redor do anel.

17. Como a arquitetura ponto a ponto difere da arquitetura cliente-servidor?
    Resposta: Na arquitetura ponto a ponto, todos os dispositivos na rede agem tanto como clientes quanto como servidores, e cada dispositivo pode se comunicar diretamente com qualquer outro. Na arquitetura cliente-servidor, alguns dispositivos (servidores) fornecem serviços, e outros dispositivos (clientes) usam esses serviços.

18. O que são UTP e STP?
    Resposta: UTP (Unshielded Twisted Pair) e STP (Shielded Twisted Pair) são tipos de cabo de

par trançado. UTP é mais comum e menos caro, mas é mais suscetível a interferência eletromagnética. STP tem uma blindagem adicional para proteger contra interferências.

19. O que significa se uma fibra óptica é monomodo ou multimodo?
    Resposta: Monomodo e multimodo referem-se ao número de caminhos de luz, ou "modos", que podem viajar através de uma fibra óptica. Fibra monomodo permite apenas um modo e é usada para transmissões de longa distância. Fibra multimodo permite vários modos e é usada para transmissões de curta distância.

20. O que é um Access Point em uma rede Wi-Fi?
    Resposta: Um Access Point é um dispositivo em uma rede Wi-Fi que permite que dispositivos sem fio se conectem à rede. Ele serve como um ponto de conexão entre os dispositivos sem fio e a rede com fio.

LISTA DE QUESTÕES ESTRATÉGICAS

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

   a) WPA.

   b) WiFi.

   c) WPS.

   d) WEP.

   e) WPA2.

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

   a) Satélite.

   b) PLC (comunicação pelo cabo de energia).

c) Fibra ótica.

d) Sem fio Wi-Fi.

e) Cabo ADSL.

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

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

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

a) Portal Internet.

b) Servidor.

c) Web server.

d) Cliente Internet.

e) Provedor.

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

a) TI-578.

b) RX-45.

c) RJ-45.

d) BSI-8.

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

a) SSID.

b) TKP

c) WEP.

d) WiFi.

e) WPA.

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

a) 11 Mbps.

b) 20 Mbps.

c) 54 Mbps.

d) 100 Mbps.

e) 200 Mbps.

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

a) Anel.

b) Estrela.

c) Distribuída.

d) Ramificada.

e) Barramento.

8. **(FCC / Prefeitura de São José do Rio Preto/SP – 2019)** Ao entrar em contato com a Central de Serviços da organização onde trabalha para relatar dificuldades em conectar o computador à internet, o atendente solicitou ao Agente Administrativo a realização de um procedimento que envolvia a identificação de um componente da rede conhecido como RJ45, que é:

a) o conector na extremidade do cabo de rede.

b) o botão usado para reiniciar o roteador.

c) o aparelho que transmite o sinal de internet via wireless.

d) a antena do roteador de internet.

e) o cabo de rede que liga o roteador ao computador.

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

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

b) Uma empresa possui um enorme volume de dados e precisa interligar o servidor principal aos outros computadores. Para permitir esta conexão deve-se utilizar uma SAN − Servidor Area Network que conecta diversas máquinas a um servidor central.

c) Há diversos dispositivos em uma residência que precisam se comunicar dentro de uma distância bastante limitada. Para isso deve ser utilizada uma rede PAN − Private Area Network, que utiliza tecnologias como Wi-Fi e bluetooth.

d) Deseja-se conectar redes de escritórios de uma mesma empresa ou de vários campi de universidades. A melhor solução é utilizar uma WLAN − Wireless Local Area Network, a versão wireless (sem fio) de uma LAN que alcança centenas de quilômetros.

e) Uma empresa presta serviços online 24 horas para países localizados em diferentes continentes. Deve-se utilizar uma WAN − Wide Area Network, que vai além da MAN − Metropolitan Area Network, conseguindo alcançar uma área maior, como um país ou mesmo um continente.

10. **(FCC / DPE-RS – 2017)** Considere uma rede de computadores instalada e em funcionamento que é caracterizada pelo seu alcance local, por se tratar de uma rede interna de curto alcance. De acordo com sua extensão geográfica, essa rede é classificada como: a) Metropolitan Area Network − MAN.

b) Local Area Network − LAN.

c) Wide Area Network − WAN.

d) Storage Area Network − SAN.

e) Popular Area Network − PAN.

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

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

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

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

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

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

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

a) I, II e III.

b) I, III e IV.

c) III e IV.

d) I e II.

e) II e IV.

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

a) 5 ou superior

b) 5a ou superior

c) 6a

d) 5e ou 6e

e) 6 ou superior

13. (FGV / COMPESA – 2016) As redes de difusão admitem diversas topologias. Com relação às redes de difusão, analise as afirmativas a seguir.

I. Em uma rede de difusão de barramento, em um dado instante, pode haver, no máximo, uma máquina desempenhando a função de mestre e podendo realizar uma transmissão.

II. Em uma rede Ethernet, se dois ou mais pacotes colidirem, cada computador fará uma nova tentativa de reenvio do seu pacote no momento em que a colisão é sinalizada.

III. Em uma topologia em anel típica não há a necessidade de se definir alguma regra para arbitrar os acessos simultâneos ao anel.

Está correto o que se afirma em:

a) I, apenas.

b) II, apenas.

c) III, apenas.

d) I e II, apenas.

e) I, II e III.

14. (FGV / Câmara Municipal de Caruaru – PE – 2015) As figuras a seguir ilustram a topologia e o conector empregado nos cabos de par trançado UTP, utilizados na implementação da rede de computadores padrão Ethernet, com acesso à Internet, da Câmara Municipal de Caruaru.

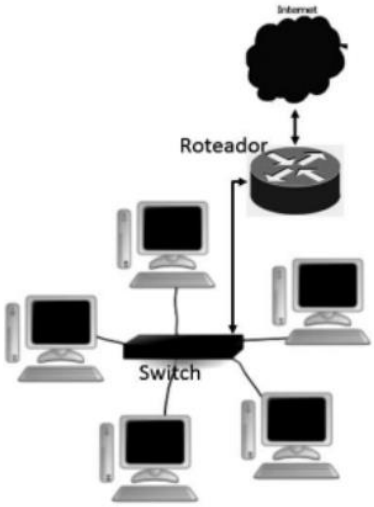


Figura I

Figura II

A topologia física e a sigla pelo qual é conhecido o conetor são, respectivamente,

a) estrela e RG58.

b) barramento e RG586

c) anel e RJ45

d) barramento e RJ45

e) estrela e RJ-45

15. (FGV / SUSAM – 2014) As figuras a seguir mostram a tecnologia e o tipo de cabo empregados na implementação das atuais redes de computadores *Fast Ethernet* cabeadas.

Figura I

Figura II

A conexão é feita por meio desse cabo, com um conector específico e utiliza a um link ponto a ponto entre e o computador e a porta do concentrador.

A topologia física e o conector são conhecidos, respectivamente, por:

a) estrela e RJ-45.

b) estrela e HDMI.

c) anel e RJ-45.

d) barramento e HDMI.

e) barramento e RJ 45.

16. (FGV / AL-MT – 2013) Com relação à tecnologia estrela utilizada na implementação de redes de computadores, assinale V para a afirmativa verdadeira e F para a falsa.

( ) Desabilita um link em caso de falha, permanecendo os demais ativos.

( ) Utiliza ligações multiponto nas conexões, exceto a do servidor que é ponto a ponto dedicado.

( ) Obriga o remanejamento de todas as conexões, quando da integração de uma nova máquina à rede.

As afirmativas são, respectivamente,

a) F, V e F

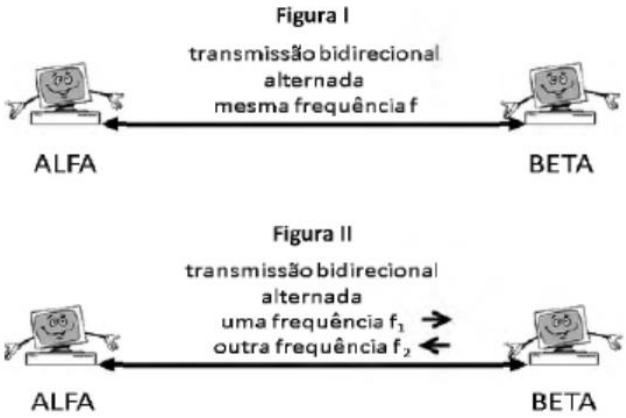
b) F, V e V

c) V, F e F

d) V, V e F

e) F, F e V

17. As figuras I e II representam dois modos de transmissão de dados.



Os modos I e II são denominados, respectivamente,

a) half-duplex e full-duplex.

b) full-duplex e half-duplex.

c) full-duplex e biplex.

d) simplex e biplex.

e) biplex e simplex.

18. **(CESGRANRIO / CEF –2021)** A computação distribuída permite que as máquinas integrantes de uma rede, que utiliza esse modelo computacional, executem o seu próprio processamento. Esse cenário permite que as organizações se beneficiem da integração de serviços, por meio da interconexão oferecida pelas redes de computadores, otimizando recursos e maximizando o poder de seu parque computacional. Nesse cenário, o modelo de redes ponto a ponto se caracteriza por:

a) agrupar um conjunto de computadores, localizados em ambientes físicos distintos, para processar grandes volumes de dados.

b) existir um servidor frontal (front-end) que se comunica com outro servidor traseiro (back-end), este responsável pelos dados do processamento.

c) inexistir a figura de um servidor dedicado, já que qualquer equipamento pode desempenhar a função de servidor de um determinado serviço.

d) interligar um conjunto de computadores, de forma que pareça um supercomputador com considerável poder computacional.

e) oferecer um modelo em que existe a figura de um equipamento servidor, responsável por atender às requisições de equipamentos clientes.

19. **(CESGRANRIO / CEFET-RJ – 2014)** Os tipos de rede digital podem ser classificados em função dos seus alcances geográficos. A rede com alcance de até 500 metros, utilizada em escritórios ou andares de um edifício, é denominada rede local e é conhecida pela sigla:

a) LAN

b) RAN

c) CAN

d) MAN

e) WAN

20. **(CESGRANRIO / TRANSPETRO – 2011)** A figura abaixo mostra uma topologia típica de uma rede industrial de comunicação onde todos os dispositivos compartilham o mesmo meio físico de comunicação. O controle pode ser centralizado ou distribuído. Além de possuir alto poder de expansão, nós com falha não prejudicam necessariamente os demais. Qual a topologia descrita?

a) Anel

b) Barramento

c) Ponto-a-Ponto

d) Árvore

e) Estrela

Gabaritos

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

14. E
15. A
16. C
17. A
18. C
19. A
20. B

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

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

1. 

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

2. 

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

3. 

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

4. 

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

5. 

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

6. 

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

7. 

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

8. 

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

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