TECNOLOGIA DA INFORMAÇÃO

Redes – Parte II

Livro Eletrônico

GRAN CURSOS ONLINE

SUMÁRIO

Apresentação

Querido(a) amigo(a), tudo bem!

Hoje daremos continuidade ao estudo sobre **Redes de Computadores (Parte II)**.

E, por fim, muitas questões para reforçar o aprendizado dessa temática. Vamos nessa!

Grande abraço!

REDES - PARTE II

1. Projetando a Topologia (Layout) da Rede

A topologia refere-se ao **layout**, forma como as máquinas/cabos estarão dispostos na rede e como as informações irão trafegar nesse ambiente.

A **forma** com que os cabos são conectados - a que genericamente chamamos **topologia da rede** - influenciará em diversos pontos considerados críticos, como flexibilidade, velocidade e segurança.

1.1. Topologia de Rede em Barramento (ou Linear)

Nessa topologia os computadores estão dispostos fisicamente de maneira que existe um **meio** de comunicação central por onde todos os dados da rede de computadores passam (**todas as estações compartilham um mesmo cabo)**. Esse meio é chamado de **barra** ou **bus**, sendo que todos os computadores estão ligados apenas a ele.

Lembre-se: como um único cabo pode ser conectado a vários computadores simultaneamente, essa estrutura é possível de ser montada com cabos coaxiais e conectores BNC APENAS. Então, essa topologia utiliza cabo coaxial, que deverá possuir um **terminador** resistivo de **50 ohms** em cada ponta, conforme ilustra a figura seguinte.

Figura - Topologia em Barramento (ou Linear)

O **tamanho máximo do trecho da rede está limitado ao limite do cabo**, 185 metros no caso do cabo coaxial fino. Este limite, entretanto, pode ser aumentado através de um periférico chamado repetidor, que na verdade é um amplificador de sinais.

Topologia em Barramento: modo de conexão entre computadores de uma rede, em que cada um dos computadores é conectado a um cabo principal, conhecido como **backbone** (espinha dorsal).

Para pequenas redes em escritórios ou mesmo em casa, a topologia linear usando cabo coaxial pode ser utilizada (se bem que, hoje em dia, não é tão comum encontrar mais esse tipo de rede).

Veja a seguir as principais **características da topologia de rede em barramento**:

- A rede **funciona por difusão (broadcast)**, ou seja, uma mensagem enviada por um computador acaba, eletricamente, chegando a **todos** os computadores da rede. A mensagem em si é descartada por todos os computadores, com exceção daquele que possui o endereço idêntico ao endereço existente na mensagem;
- **Baixo custo de implantação e manutenção**, devido aos equipamentos necessários (basicamente placas de rede e cabos);
- **Mesmo se uma das estações falhar, a rede continua funcionando normalmente**, pois os computadores (na verdade, as placas de rede, ou interfaces de rede) se comportam de forma **passiva**, ou seja, o sinal elétrico é APENAS RECEBIDO pela placa em cada computador, e NÃO retransmitido por esta;
- **Quanto mais computadores estiverem ligados à rede, pior será o desempenho (velocidade) da mesma** (devido à grande quantidade de colisões);
- **Como todas as estações compartilham um mesmo cabo, somente uma transação pode ser efetuada por vez, isto é, não há como mais de um micro transmitir dados por vez**. Quando mais de uma estação tenta utilizar o cabo, há uma colisão de dados. Quando isto ocorre, a placa de rede espera um período aleatório de tempo até tentar transmitir o dado novamente. Caso ocorra uma nova colisão a placa de rede espera mais um pouco, até conseguir um espaço de tempo para conseguir transmitir o seu pacote de dados para a estação receptora;
- **Sobrecarga de tráfego**: quanto mais estações forem conectadas ao cabo, mais lenta será a rede, já que haverá um maior número de colisões (lembre-se que sempre em que há uma colisão o micro tem de esperar até conseguir que o cabo esteja livre para uso), o que pode levar à diminuição ou à inviabilização da continuidade da comunicação;
- Outro grande problema na utilização da topologia linear é a **instabilidade**. Os terminadores resistivos são conectados às extremidades do cabo e são indispensáveis. **Caso o**

cabo se desconecte em algum ponto (qualquer que seja ele), a rede "sai do ar", pois o cabo perderá a sua correta impedância (não haverá mais contato com o terminador resistivo), impedindo que comunicações sejam efetuadas - em outras palavras, a rede **para de funcionar**. Como o cabo coaxial é vítima de problemas constantes de mau contato, a rede pode deixar de funcionar sem mais nem menos, principalmente em ambientes de trabalho tumultuados. Voltamos a enfatizar: basta que um dos conectores do cabo se solte para que todos os micros deixem de se comunicar com a rede;

- E, por fim, outro sério problema em relação a esse tipo de rede é a **segurança**. Na transmissão de um pacote de dados, todas as estações recebem esse pacote. No pacote, além dos dados, há um campo de identificação de endereço, contendo o número de nó[1] de destino. Desta forma, somente a placa de rede da estação de destino captura o pacote de dados do cabo, pois está a ela endereçada;
- Se na rede você tiver duas placas com o mesmo número de nó, as duas captarão os pacotes destinados àquele número de nó. É impossível você em uma rede ter mais de uma placa com o mesmo número de nó, a não ser que uma placa tenha esse número alterado propositalmente por algum hacker com a intenção de ler pacotes de dados alheios. Apesar desse tipo de "pirataria" ser rara, já que demanda de um extremo conhecimento técnico, não é impossível de acontecer. Portanto, **em redes nas quais segurança seja uma meta importante, a topologia linear NÃO deve ser utilizada**.

1.2. Topologia em Anel (Ring)

Na **topologia em anel**, **as estações de trabalho formam um laço fechado** (todos os computadores são ligados um ao outro diretamente – **ligação ponto a ponto**), conforme ilustra a figura seguinte. Os dados circulam no anel, passando de máquina em máquina, até retornar à sua origem. Todos os computadores estão ligados apenas a este anel (ring).

1Número de nó (node number) é um valor gravado na placa de rede de fábrica (é o número de série da placa). Teoricamente não existe no mundo duas placas de rede com o mesmo número de nó.

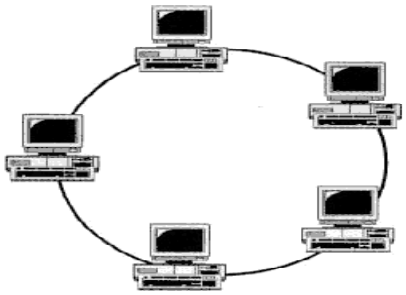


Figura - Topologia em Anel

Essa forma de ligação de computadores em rede NÃO é muito comum. **As redes Anel são normalmente implementações lógicas**, não físicas, ou seja: não é comum encontrar essas redes organizadas REALMENTE em anel, mas na sua maioria apenas funcionando assim (ou seja, é comum as redes serem, por exemplo, fisicamente estrela e logicamente anel – os micros ACHAM que estão em anel).

O padrão mais conhecido de topologia em anel é o **Token Ring (IEEE 802.5)** da IBM. No caso do Token Ring, um pacote (token) fica circulando no anel, pegando dados das máquinas e distribuindo para o destino. Somente um dado pode ser transmitido por vez neste pacote. Pelo fato de cada computador ter igual acesso a uma ficha (token), nenhum computador pode monopolizar a rede.

Quanto à **topologia em anel**, as principais características que podemos apontar são:

- **Se um dos computadores falhar, toda a rede estará sujeita a falhar porque as placas de rede dos computadores funcionam como repetidores,** ou seja, elas têm a função de receber o sinal elétrico e retransmiti-lo aos demais (possuem um comportamento ATIVO). Em outras palavras, quando uma estação (micro) recebe uma mensagem, ele verifica se ela (a mensagem) é direcionada para ele (o micro), se sim, a mensagem será assimilada (copiada para dentro do micro). Depois disso (sendo assimilada ou não) a mensagem é retransmitida para continuar circulando no Anel;
- **A mensagem enviada por um dos computadores atravessa o anel todo**, ou seja, quando um emissor envia um sinal, esse sinal passa por todos os computadores até o destinatário, que o copia e depois o reenvia, para que atravesse o restante do anel, em direção ao emissor;

- Apresenta **um desempenho estável (velocidade constante),** mesmo quando a quantidade de computadores ligados à rede é grande.

Obs.: as **redes Anel, podem, teoricamente, permitir o tráfego de dados nas duas direções, mas normalmente são unidirecionais**.

1.3. Topologia em Estrela (Star ou Hub-and-Spoke)

Esta é a topologia mais recomendada atualmente. Nela, **todas as estações são conectadas a um periférico concentrador (hub ou switch)**, como ilustra a figura seguinte. Se uma rede está funcionando realmente como estrela, dois ou mais computadores podem transmitir seus sinais ao mesmo tempo (o que não acontece nas redes barra e anel).

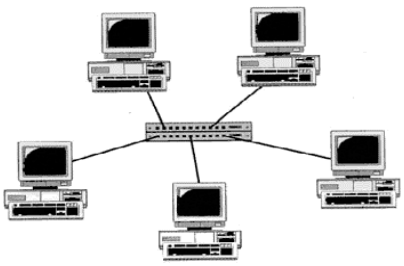


Figura - Topologia em Estrela

As principais características a respeito da topologia em estrela que devemos conhecer são:

- **Admite trabalhar em difusão**, embora esse não seja seu modo cotidiano de trabalho. Ou seja, mesmo que na maioria das vezes não atue desta forma, as redes em estrela podem enviar sinais a todas as estações (envio por broadcast - ou por difusão);
- **Todas as mensagens passam pelo Nó Central (Núcleo da rede)**;
- **Uma falha numa estação (Micro) NÃO afeta a rede**, pois as interfaces de rede também funcionam de forma PASSIVA. Ao contrário da topologia linear onde a rede inteira parava quando um trecho do cabo se rompia, na topologia em estrela apenas a estação conectada pelo cabo para;
- **Uma falha no nó central faz a rede parar de funcionar**, o que, por sinal, também é bastante óbvio! O funcionamento da topologia em estrela depende do periférico concentrador utilizado. Se o hub/switch central falhar, para toda a rede;

- **Facilidade na implantação e manutenção**: é fácil ampliar, melhorar, instalar e detectar defeitos em uma rede fisicamente em estrela;
- Neste caso, temos a grande vantagem de podermos aumentar o tamanho da rede sem a necessidade de pará-la. Na topologia linear, quando queremos aumentar o tamanho do cabo necessariamente devemos parar a rede, já que este procedimento envolve a remoção do terminador resistivo;
- A topologia em estrela é a mais fácil de todas as topologias para diagnosticar problemas de rede;
- Custa mais fazer a interconexão de cabos numa rede ligada em estrela, pois todos os cabos de rede têm de ser puxados para um ponto central, requisitando mais cabos do que outras topologias de rede;
- As redes fisicamente ligadas em estrela utilizam cabos de par trançado, conectores RJ-45 (ou fibras ópticas) e Hubs ou Switches no centro da rede. Há muitas tecnologias de redes de computadores que usam conexão física em estrela, embora funcionem como barra ou anel.

Obs.: **a grande maioria das redes atuais, mesmo as que funcionam de outras maneiras (Anel ou Barramento) são implementadas fisicamente em estrela, o que torna os processos de manutenção e expansão muito mais simplificados.**

1.4. Rede em Malha (Mesh)

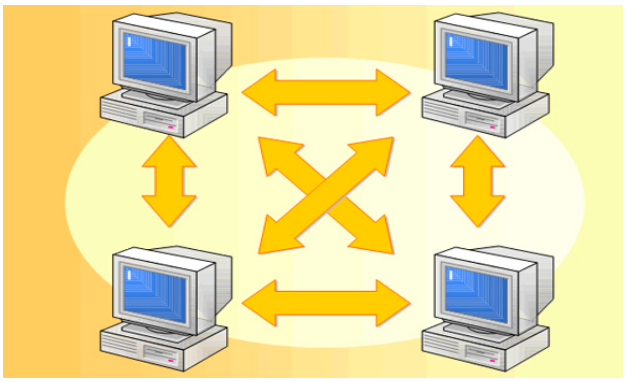
Utiliza vários segmentos de cabos.

Oferece redundância e confiabilidade.

Dispendiosa.

Geralmente utilizada em conjunto com outras topologias.

Obs.: **representa uma das topologias mais tolerantes à falha, pois geralmente há vários caminhos entre cada par de nodos.**



ATENÇÃO

Quando a rede em malha conecta todos a todos, esta especificamente é conhecida pelo termo **Full Mesh**.

1.5. Estrela Hierárquica ou Árvore (Tree)

É o tipo de topologia de rede em que existem um ou mais concentradores que ligam cada rede local e existe outro concentrador que interliga todos os outros concentradores.

Composta por vários níveis hierárquicos.

Suas ramificações tendem a convergir para uma raiz.

Isenta de loops.

Mais vulnerável.

Figura. Topologia Árvore (Tree)

1.6. Híbrida

Composição das outras.

Exemplo: Internet.

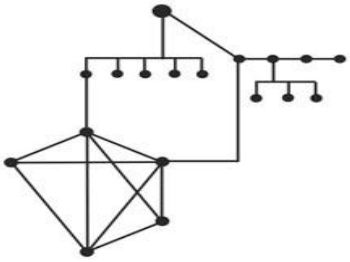


Figura. Topologia Híbrida

2. Topologia Física x Topologia Lógica

As redes de computadores podem ser divididas em duas partes principais: **parte física** e **lógica**.

A **topologia física** indica a organização e a disposição espacial do hardware da rede, organização essa conhecida como topologia física.

A **topologia lógica** abrange as regras que permitem aos componentes de hardware trabalharem adequadamente quando interligados; é a topologia lógica.

Esquematizando:

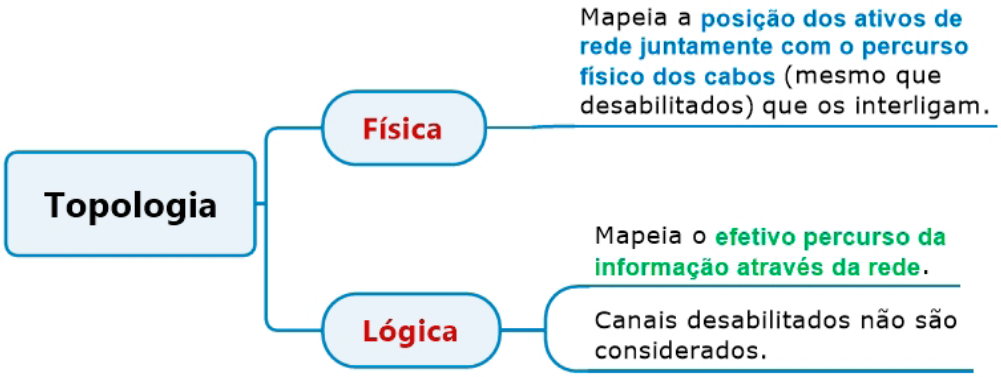


Figura. Topologia (Física e Lógica). Fonte: Quintão (2020)

Obs.: **quando o enunciado é omisso, deve-se considerar a Topologia Física!**

Nem sempre há uma coincidência das topologias físicas e lógicas num equipamento.

Obs.: como exemplo, vamos a **uma rede em estrela**, cujo elemento concentrador pode ser um **hub** ou **switch**:

No caso da utilização de um **hub, a topologia fisicamente será em estrela, porém logicamente ela continua sendo uma rede de topologia barramento (linear).**

O **hub** é um periférico que repete para todas as suas portas os pacotes que chegam, assim como ocorre na topologia linear. Em outras palavras, se a estação 1 enviar um pacote de dados para a estação 2, todas as demais estações recebem esse mesmo pacote. Portanto, continua havendo problemas de colisão e disputa para ver qual estação utilizará o meio físico.

Já no caso da utilização de um **switch, a rede será tanto fisicamente quanto logicamente em estrela.**

Este periférico tem a capacidade de analisar o cabeçalho de endereçamento dos pacotes de dados, enviando os dados **diretamente ao destino**, sem replicá-lo desnecessariamente para todas as suas portas.

Desta forma, se a estação 1 enviar um pacote de dados para a estação 2, somente esta recebe o pacote de dados. Isso faz com que a rede se torne mais segura e muito mais rápida, pois praticamente elimina problemas de colisão. Além disso, duas ou mais transmissões podem ser efetuadas simultaneamente, desde que tenham origem e destinos diferentes, o que não é possível quando utilizamos topologia linear ou topologia em estrela com hub.

Obs.: **se o controlador central for um HUB teremos uma TOPOLOGIA FÍSICA EM ESTRELA, mas uma topologia lógica em barramento.**
Já se o controlador central for um SWITCH teremos tanto a topologia física quanto lógica em ESTRELA.

3. Fundamentos da Transmissão

Para serem transmitidos, os dados têm de ser transformados em **sinais eletromagnéticos** (FOROUZAN, 2008). Os dados podem ser analógicos ou digitais. Os dados analógicos são

contínuos e assumem valores contínuos. Dados digitais têm estados discretos e assumem valores discretos.

3.1. Sinal

Em geral, entende-se que um **sinal** é **uma sequência de estados em um sistema de comunicação que codifica uma mensagem.**

3.1.1. Sinais Analógicos e Digitais

Os sinais podem ser **analógicos** ou **digitais**.

Sinal Analógico é um **tipo de sinal contínuo** que varia em função do tempo. Exemplos: velocímetro de ponteiros; termômetro de mercúrio; balança de molas. São sinais lidos de forma direta sem passar por qualquer decodificação complexa, uma vez que as variáveis são observadas diretamente.

Sinal Digital é um **sinal com valores discretos (descontínuos) na amplitude, no tempo e/ou em fase**. Isso significa que um sinal digital só é definido para determinados instantes de tempo, e que o conjunto de valores que pode assumir é finito.

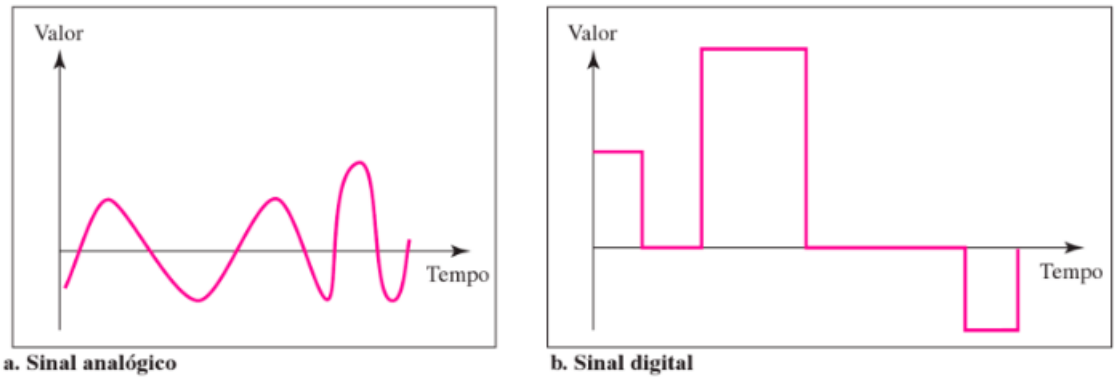


Figura. Comparação de sinais analógicos e digitais. Fonte: Forouzan (2008).

Obs.: os sinais **analógicos** podem ter um número infinito de valores em um período de tempo; os sinais **digitais** podem ter apenas um número limitado de valores.

3.1.2. Sinais Periódicos e Não Periódicos

Um **sinal periódico** completa um padrão dentro de um **período** de tempo mensurável, e esse padrão se repete, de forma idêntica, ao longo dos períodos seguintes. O término de um padrão completo é chamado **ciclo**. Um **sinal não periódico** muda sem exibir um padrão ou ciclo que se repita ao longo do tempo (FOROUZAN, 2008).

Obs.: **na comunicação de dados, usamos comumente sinais analógicos periódicos** (pois eles precisam menos largura de banda) **e sinais digitais não periódicos** (pois eles podem representar variação nos dados) (FOROUZAN,2008).

3.2. Transmissão Digital

Conforme destaca Forouzan (2008, p. 101), uma rede de computadores é construída para enviar informações de um ponto a outro. **Essas informações precisam ser convertidas em sinais digitais ou analógicos para a transmissão.**

3.2.1. Conversão Digital-Digital

Os dados podem ser digitais ou analógicos. Os sinais que representam dados também podem ser digitais ou analógicos.

Podemos representar **dados digitais** por meio de **sinais digitais** realizando uma **conversão** que envolve três técnicas: codificação de **linha**, codificação de **blocos** e **mistura de sinais**.

Obs.: **a codificação de linha é sempre necessária; a codificação de blocos e a mistura de sinais não necessariamente.**

3.2.1.1. Codificação de Linha

Conforme Forouzan (2008), a **codificação de linha** é o processo de conversão de **dados digitais** em **sinais digitais**. Partimos do pressuposto de que os dados, na forma de texto, números, imagens, áudio ou vídeo, são armazenados na memória do computador como sequências de bits. **A codificação de linha converte uma sequência de bits em um sinal digital.** No emis-

sor, os dados digitais são codificados em um sinal digital; no receptor, os dados digitais são recriados, reconvertendo-se o sinal digital. A figura a seguir ilustra o processo.

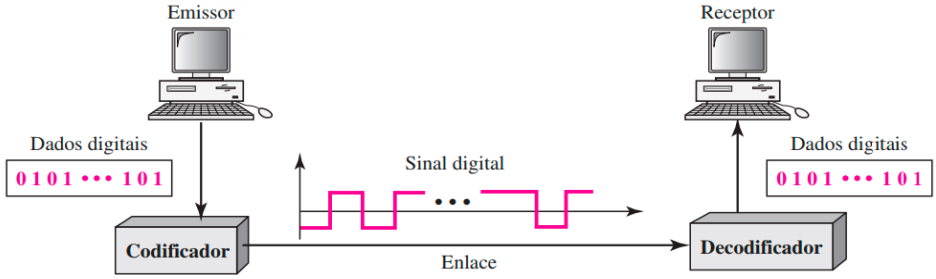


Figura. Codificação de linha e decodificação (FOROUZAN, 2008)

Taxa de Dados versus Taxa de Sinal:

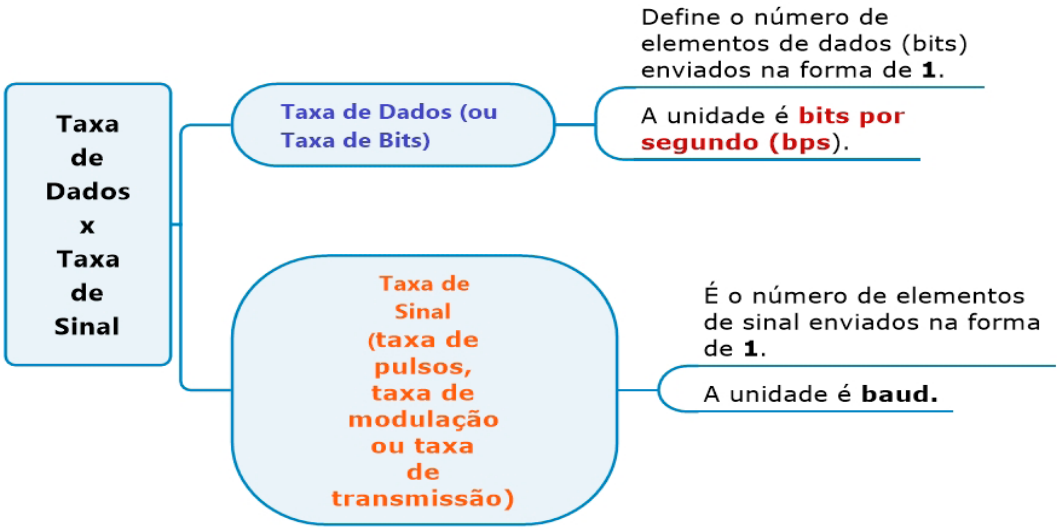


Figura. Taxa de Dados x Taxa de Sinal

Em comunicação de dados o objetivo é aumentar a taxa de dados e, ao mesmo tempo, **diminuir a taxa de sinal**. Aumentar a taxa de produção de dados eleva a velocidade de transmissão; reduzir a taxa de sinal diminui as exigências em termos de largura de banda (FOROUZAN, 2008).

Largura de Banda: uma característica que mede o desempenho das redes é a largura de banda (FOROUZAN, 2008).

Um sinal digital que transporta informações não é periódico. A largura de banda de um sinal não periódico é contínua em um intervalo infinito. Entretanto, a maioria dos sinais digitais que encontramos na vida real tem uma largura de banda com valores finitos (FOROUZAN, 2008).

Obs.: embora a largura de banda real de um **sinal digital** seja infinita, **a largura de banda efetiva é finita.**

Detecção de Erros Embutidos: é desejável possuir recursos de detecção de erros embutidos no código gerado para detectar parte ou todos os erros ocorridos durante uma transmissão (FOROUZAN, 2008).

Imunidade a Ruído e Interferência: outra característica de código desejável é um código que seja imune a ruídos e outras interferências (FOROUZAN, 2008).

Complexidade: um método complexo é mais dispendioso de implementar que um simples. Por exemplo, um método que use quatro níveis de sinal é mais difícil de interpretar que um com apenas dois níveis (FOROUZAN, 2008).

Métodos de Codificação de Linha: os métodos de codificação de linha são divididos em cinco categorias: **Unipolar, Polar, Bipolar, Multinível e Multitransição** (FOROUZAN, 2008).

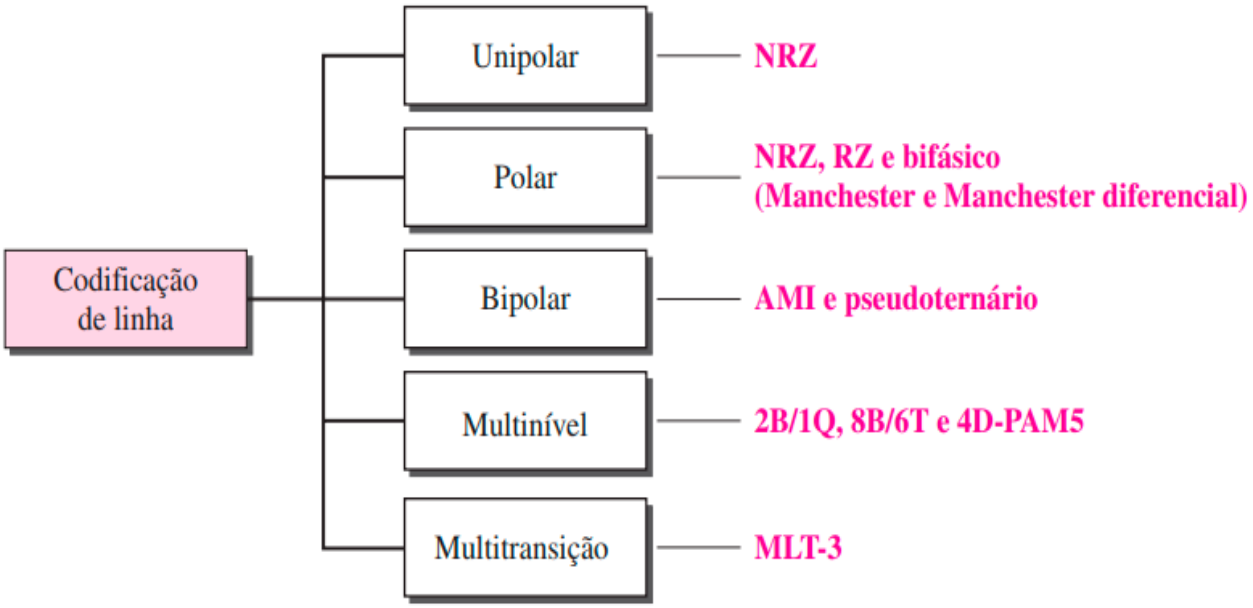
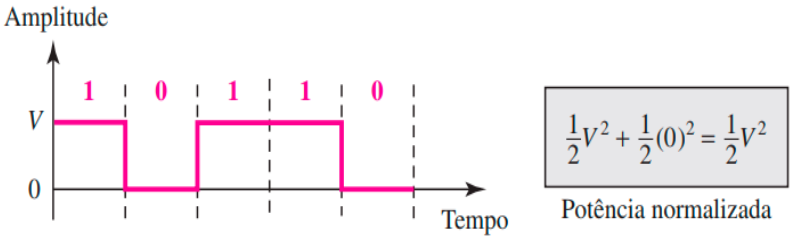


Figura. Codificação de linha, Fonte: Forouzan (2008, p. 106)

Método de Codificação	Descrição
Unipolar	Todos os níveis de sinal se encontram em um dos lados do eixo do tempo, acima ou abaixo dele. Tradicionalmente, um método unipolar foi desenvolvido como um método **NRZ** (Non-Return-to-Zero, ou seja, Sem Retorno a Zero) no qual a voltagem positiva define o bit 1 e a voltagem zero define o bit 0. **Ele é chamado NRZ porque o sinal não retorna a zero no meio do bit** (Forouzan, 2008).  Figura. Método NRZ unipolar, Fonte: Forouzan (2008) Esse método custa muito caro e, **normalmente, não é usado em comunicação de dados hoje em dia.**
Polares	**As voltagens se encontram em ambos os lados do eixo de tempo**. Por exemplo, o nível de voltagem para 0 pode ser positivo e o nível de voltagem para 1 pode ser negativo.
Bipolar (ou binária multinível)	**Existem três níveis de voltagem: positivo, negativo e zero**. O nível de voltagem para um elemento de dados se encontra em zero, ao passo que o nível de voltagem para o outro elemento fica alternando entre valores positivos e negativos. Temos **duas variações de codificação bipolar: AMI** (Inversão de Marca Alternada) e **pseudoternária**.
Multinível	Temos as seguintes variações de codificação (FOROUZAN, 2008): • **2B1Q** (usado na tecnologia DSL (Digital Subscriber Line), para oferecer uma conexão de alta velocidade para a Internet através de linhas telefônicas convencionais; • **8B6T** (oito binário, seis ternário), usado em cabos 100Base-4T; • **4D-PAM5**: modulação de amplitude de pulso com 5 níveis e quatro dimensões. O 4D indica que os dados são enviados através de 4 fios ao mesmo tempo.
Multitransição	Método de codificação diferencial com mais de duas regras de transição. O **MLT-3** (Transmissão multilinha de três níveis) é um deles.

3.2.1.2. Codificação de Blocos

Fornece redundância para garantir sincronização e detecção de erros inerente. Normalmente é conhecida como **codificação *mB/nB***; ela substitui cada grupo de *m* bits por um grupo de *n* bits (FOROUZAN, 2008).

3.2.1.3. Mistura de Sinais

Fornece sincronização sem aumentar o número de bits. Duas técnicas de mistura de sinais: B8ZS e o HDB3.

3.3. Transmissão Analógica

Segundo Forouzan (2008), a **conversão digital-analógica** é o processo de mudar uma das características de um sinal analógico com base nas informações contidas nos dados digitais.

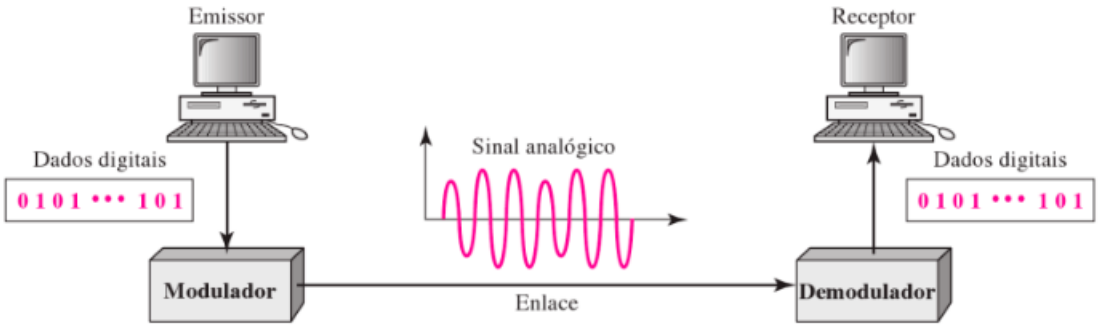


Figura. Conversão Digital-Analógica. Fonte: Forouzan (2008).

A **conversão analógica-analógica** permite a representação de informações analógicas por um sinal analógico.

4. Meios de Transmissão

Responsáveis pelo transporte dos sinais que representam os dados em uma rede. Eles transportam um fluxo bruto de bits de uma máquina para outra. Cada meio tem suas características de performance, custo, retardo e facilidade de instalação e manutenção.

Conforme destaca Forouzan (2008), os meios de transmissão estão, na verdade, localizados abaixo da camada física e são diretamente controlados por ela.

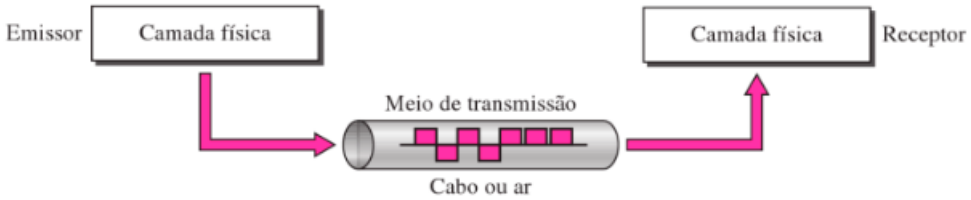


Figura. Meio de Transmissão e a Camada Física Fonte: Forouzan (2008, p. 191)+

Em telecomunicações, segundo Forouzan (2008), meios de transmissão são divididos em **duas amplas categorias**: **guiados e não guiados**.

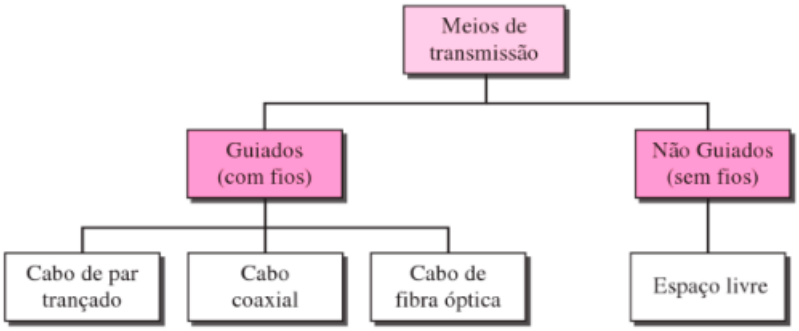


Figura. Classes de Meios de Transmissão, Fonte: Forouzan (2008, p. 192)

4.1. Meios de Transmissão Guiados

Os meios de transmissão guiados abrangem os cabos e fios.

4.1.1. Cabo Coaxial

Apresenta um **núcleo condutor central** de fio torcido ou sólido (normalmente, **cobre**) **envolto em um revestimento isolante** que, por sua vez, é revestido por um condutor externo de folha de metal, uma capa ou uma combinação de ambos (FOROUZAN, 2008).

No passado esse era o tipo de cabo mais utilizado em LANs. Atualmente, por causa de suas desvantagens, está cada vez mais caindo em desuso, sendo substituído pelo **cabo de par trançado** em LANs. Entre essas desvantagens está o **problema de mau contato nos conectores utilizados, a difícil manipulação do cabo** (como ele é rígido, dificulta a instalação em ambientes comerciais, por exemplo, passá-lo através de conduítes) e **o problema da topologia**.

Para conectar cabos coaxiais a dispositivos, precisamos de conectores coaxiais. O tipo mais comum de conector utilizado atualmente é o **conector BNC.**

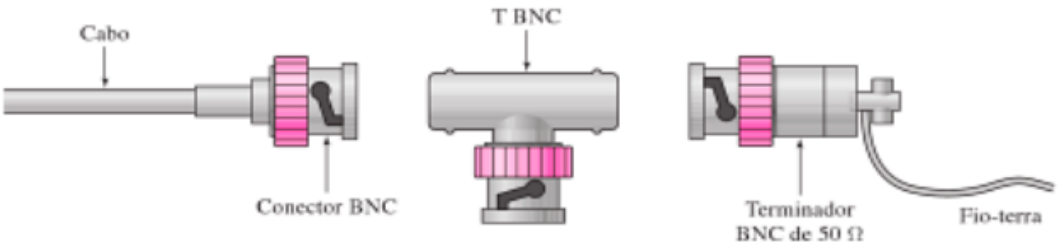


Figura. Conectores BNC - Fonte: Forouzan (2008, p. 197)

A topologia mais utilizada com esse cabo é a topologia linear (também chamada topologia em **barramento**) que **faz com que a rede inteira saia do ar caso haja o rompimento ou mau contato de algum trecho do cabeamento da rede.** Como a rede inteira cai, fica difícil determinar o ponto exato em que está o problema, muito embora existam no mercado instrumentos digitais próprios para a detecção desse tipo de problema.

Tipos de Cabo Coaxial:

- Thin –185m (Flexível) – Segmento – 10base2
- Thick – 500m (Rígido) – Backbone – 10base5

Cabo coaxial fino Cabo coaxial grosso

Cabo Coaxial FINO (10Base2 | Thin Ethernet): esse **era o tipo de cabo coaxial mais utilizado**. É chamado "fino" porque sua bitola é menor que o cabo coaxial grosso. É também chamado "Thin Ethernet" ou 10Base2. Nesta nomenclatura, "10" significa taxa de transferência de 10 Mbps e "2" a extensão máxima de cada segmento da rede, neste caso 200 m (na verdade o tamanho real é menor, 185 m).

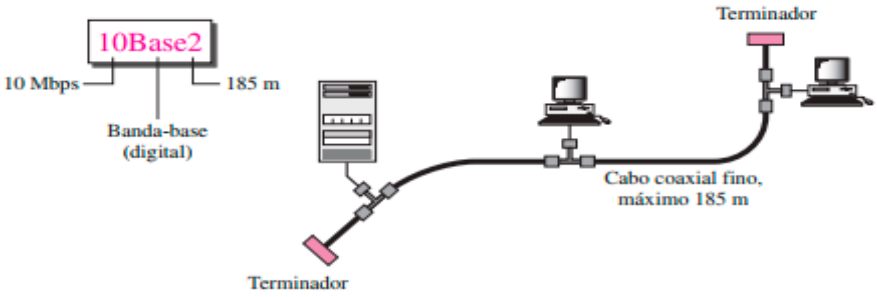


Figura. 10Base2 - Fonte: Forouzan (2008)

Cabo Coaxial GROSSO (10Base5 | Thick Ethernet): esse tipo de cabo coaxial é pouco utilizado. É também chamado "Thick Ethernet" ou 10Base5. Analogamente ao 10Base2, 10Base5 significa 10 Mbps de taxa de transferência e que cada segmento da rede pode ter até 500 metros de comprimento.

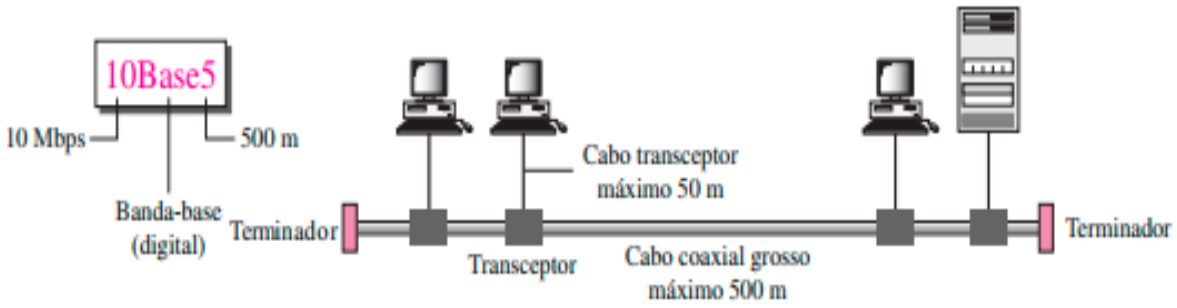


Figura. 10Base5 - Fonte: Forouzan (2008)

Padrões de Cabo Coaxial: os cabos coaxiais, segundo Forouzan (2008), são classificados em categorias de acordo com seus índices RG. Cada índice representa um conjunto exclusivo de especificações físicas.

Categoria	*Impedância*	*Uso*
RG-59	75 Ω	TV a cabo
RG-58	50 Ω	Ethernet fina
RG-11	50 Ω	Ethernet grossa

Figura. Categorias de Cabos Coaxiais - Fonte: Forouzan (2008, p. 196)

4.1.2. Cabo de Par Trançado (Twisted Pair)

É um tipo de cabo constituído por um **feixe de fios de cobre**.

Formado por pares de fios que se entrelaçam por toda a extensão do cabo, com o **objetivo de cancelar as interferências eletromagnéticas** de fontes externas e interferências mútuas (linha cruzada ou, em inglês, crosstalk) entre cabos vizinhos.

Normalmente, existem conectores apropriados para cada tipo de cabo. No caso dos cabos de par trançado, o conector utilizado é chamado de RJ-45.

Figura. Conector RJ-45

O RJ-45 é similar ao conector de linha telefônica, só que maior, com mais contatos. A propósito, o conector de linha telefônica se chama RJ-11. O RJ-45 é o conector apropriado para conectar um cabo de par trançado a placas e outros equipamentos de rede.

Tipos de Cabos de Par Trançado:

Os cabos de par trançado **sem blindagem** são chamados de **UTP** (**Unshielded Twisted Pair** - "cabo de par trançado sem blindagem"). Os **cabos blindados**, por sua vez, se dividem em três categorias:

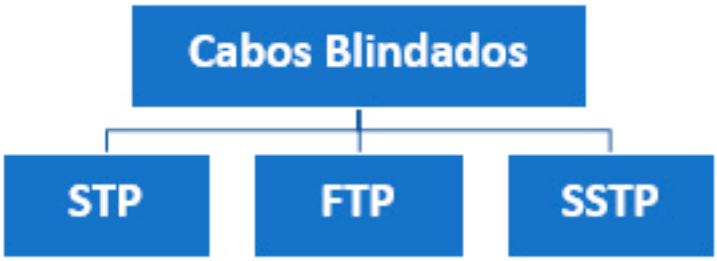
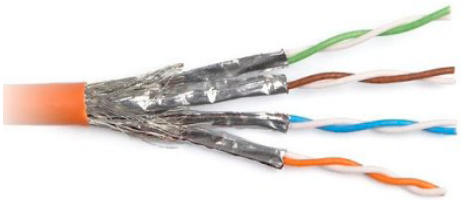


Figura. Cabos Blindados

Tipo de Cabo Blindado	Observações

FTP (Foiled Twisted Pair)	Utilizam a blindagem mais simples. Uma fina folha de aço ou de liga de alumínio envolve todos os pares do cabo, protegendo-os contra interferências externas, **mas sem fazer nada com relação ao crosstalk**, ou seja, a interferência entre os pares de cabos:  Figura. Cabo FTP
STP (Shielded Twisted Pair)	Utiliza **blindagem individual para cada par de cabos**. **Isso reduz o crosstalk** e melhora a tolerância do cabo com relação à distância, o que pode ser usado em situações em que for necessário crimpar cabos fora do padrão, com mais de 100 metros.  Figura. Cabo STP
SSTP (Screened Shielded Twisted Pair), também chamados de SFTP (Screened Foiled Twisted Pair)	Conjugam a blindagem individual dos pares a uma segunda blindagem externa, envolvendo todos os pares. **Resistentes a interferências externas**. Mais adequados a ambientes com fortes fontes de interferências.  Figura. Cabo SSTP

Fonte: https://www.hardware.com.br/livros/redes/categorias-cabos.html

Para melhores resultados, **os cabos blindados devem ser combinados com conectores RJ-45 blindados**. Eles incluem uma proteção metálica que protege a parte destrançada do cabo que vai dentro do conector, evitando que ela se torne o elo mais fraco da cadeia.

Quanto maior for o nível de interferência, mais vantajosa será a instalação de cabos blindados. Entretanto, em ambientes normais os cabos sem blindagem funcionam perfeitamente bem; justamente por isso os cabos blindados são pouco usados.

Conforme visto na figura seguinte, a diferença óbvia entre os cabos UTP e STP é a **existência de uma malha (blindagem) no cabo com blindagem**, que ajuda a diminuir a interferência eletromagnética (EMI) e/ou interferência de frequência de rádio (RFI) e, com isso, aumentar a taxa de transferência obtida na prática.

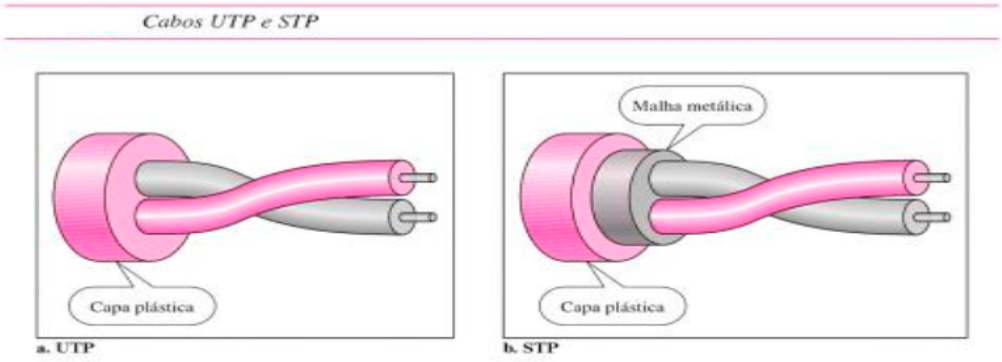


Figura. Cabos UTP (Par Trançado Sem Blindagem) e STP (Par Trançado com Blindagem).Fonte: Forouzan (2008, p. 194)

Obs.: você deve ter sempre em mente **a existência da interferência eletromagnética em cabos UTP, principalmente se o cabo tiver de passar por fortes campos eletromagnéticos,** especialmente motores e quadros de luz.

<u>É muito problemático passar cabos UTP muito próximos a geladeiras, condicionadores de ar e quadros de luz.</u> O campo eletromagnético impedirá um correto funcionamento daquele trecho da rede. Se a rede for ser instalada em um parque industrial – em que a interferência é inevitável - outro tipo de cabo deve ser escolhido para a instalação da rede, como o próprio cabo coaxial ou a fibra ótica.

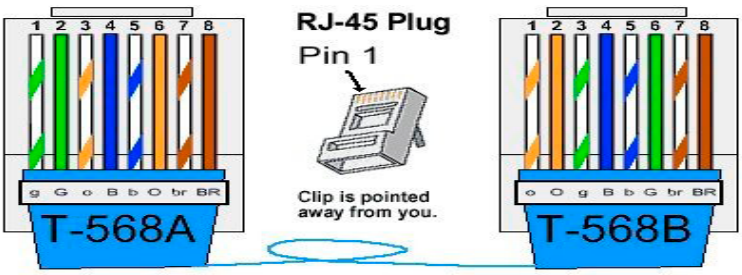
Cabo de Par Trançado Direto x Cruzado: ao utilizar o cabo de par trançado, você pode ter que utilizar um **Cabo Direto** (StraightPinning) ou um **Cabo Cruzado** (Cross-over).

O **Cabo Direto** é utilizado toda vez que você fizer a ligação de um computador para um Hub ou Switch. Neste caso você deve utilizar um cabo conectorizado pino a pino nas duas pontas, obedecendo a codificação de cores 568A ou 568B, conforme a escolhida por você (todas as conexões deverão seguir o mesmo padrão).

O **Cabo Cruzado (cross-over) é utilizado toda vez que você fizer a interligação Hub-Switch, Hub-Hub ou Switch-Switch** (deve haver apenas um cabo cruzado entre os equipamentos).

Assim, ...

Obs.: para ligar um computador a um hub ou switch, utilizamos um cabo **normal**.
Para ligar diretamente dois computadores, utilizamos um cabo de par-trançado **cross-over**.



Assim, a **única exceção** é **na conexão direta de dois micros** usando uma configuração chamada **cross-over**, utilizada para montar uma rede com apenas esses dois micros.

Aqui gostaria de destacar também o **cabo USB-USB (**também chamado de **bridged,** ou **cabo link USB)**, **utilizado também para conectar dois computadores.** Ele possui um pequeno circuito eletrônico no meio do cabo, permitindo que os dois computadores conversem entre si.

Figura. Cabo USB-USB

Note que existe ainda o **cabo USB A/A** (como o que você usa para conectar o scanner ou a impressora ao computador) que, apesar de ter os dois conectores USB padrão nas pontas, não possui o chip que permite a comunicação entre os micros e NÃO pode ser usado para conectar dois computadores.

Em redes de grande porte, os cabos UTP/STP provenientes dos diversos pontos de rede (caixas conectoras junto aos micros) são conectados a blocos de distribuição fixos em estruturas metálicas. Este conjunto é denominado **Patch Panel**.

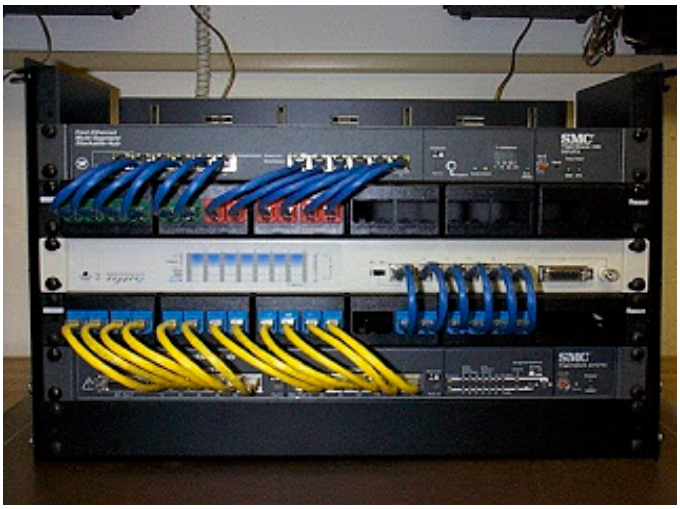


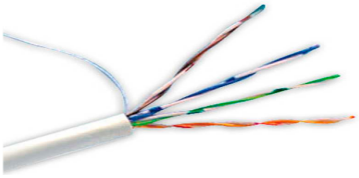
Figura. Patch Panel

A ligação dos blocos de distribuição citados aos hubs e/ou switches se dá através de **patch cords**. A utilização de patch panels confere melhor organização, maior flexibilidade e consequentemente, facilita a manutenção.

Categorias de Cabo de Par Trançado:

Ao comprar um cabo de par trançado, é importante notar qual a sua **CATEGORIA**: **cat1, cat2, cat3, cat4, cat5, cat5e, cat6, cat7, cat7a, cat 8/8.1/8.2**. Existem várias padronizações relativas aos cabos UTP, sendo comumente utilizado o padrão de categorias EIA (Electrical Industries Association).

Obs.: **via de regra, QUANTO MAIOR A CATEGORIA DO CABO, MAIOR A VELOCIDADE COM QUE ELE PODE TRANSPORTAR DADOS.**

Categoria	Frequência	Aplicações	Observações
Cat 3	16 MHz	10BASE-T / 100BASE-T4	Opera com taxa de até 16 Mbps. Utilizados em cabos de telefonia.
Cat 4	20 MHz	16 Mbps *Token Ring*	**Não** é mais utilizado.
Cat 5	**100 MHz**	100BASE-TX / **1000BASE-T**	Criados para redes **Fast Ethernet com taxa de 100 Mbps**. Suporta também *Gigabit Ethernet* com taxa de 1000 Mbps. (CAT5 não é mais recomendado pela TIA/EIA)**.** 
Cat 5e	**100 MHz**	**1000BASE-T** / 2.5GBASE-T	**Cat 5 melhorado.** Ainda muito comum nas redes. 
Cat 6	250 MHz	**5GBASE-T / 10GBASE-T**	Desenvolvido para **redes Gigabit Ethernet**. **Limitado** a 55 metros em 10GBASE-T.
Cat 6a	500 MHz	**5GBASE-T / 10GBASE-T**	Cat 6 melhorado. Atinge 100 metros em 10GBASE-T. Para que os cabos CAT 6a sofressem menos interferências os pares de fios são separados uns dos outros, o que aumentou o seu tamanho e os tornou menos flexíveis.
Cat 7	600 MHz	**5GBASE-T / 10GBASE-T**	Criado para tráfego multimídia**. Possui isolamento contra interferências**. Pode suportar até 100 Gbps.
Cat 7a	1000 MHz	**5GBASE-T / 10GBASE-T**	Semelhante ao CAT 7. Assim como o CAT 7 utiliza conector diferente do *RJ*-45.
Cat 8/8.1/8.2	2000 MHz	**25GBASE-T / 40GBASE-T**	Suportam taxas de transmissão muito altas.

Fonte: https://techenter.com.br/cabos-de-par-trancado-categorias-e-tipos/. *Acesso em: jan. 2020.*

Cabeamento – Ethernet:

- Mais popular em LANs;
- Utiliza **topologia Barramento** (com **Cabo Coaxial) ou Estrela** (com **Cabo de Par Trançado);**
- A tabela seguinte ilustra a velocidade dos adaptadores de rede, com relação aos principais padrões de arquitetura**;**
- A Ethernet evoluiu ao longo de **quatro** gerações. São elas:

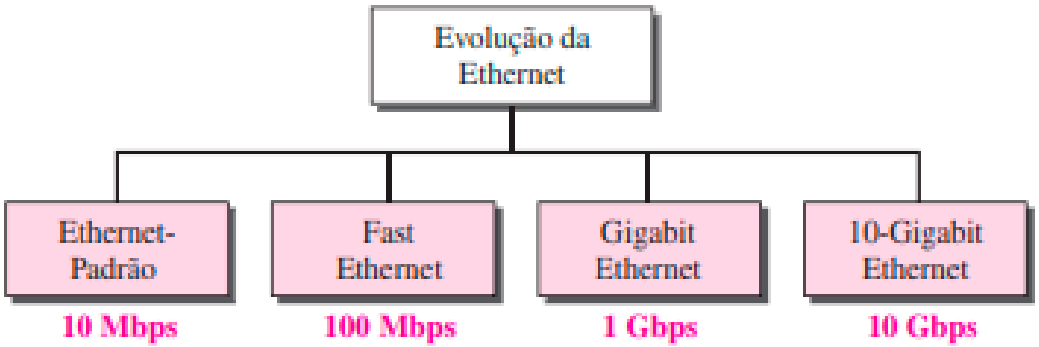


Figura. Evolução da Ethernet ao longo de quatro gerações
Fonte: Forouzan (2008, p. 398)

Padrão de Arquitetura	Velocidade do Adaptador (Placa) de Rede
Ethernet-padrão	**10 Mbps**
Fast Ethernet	**100 Mbps**
Gigabit Ethernet	**1000 Mbps = 1 Gbps**
10 Gigabit Ethernet	**10.000 Mbps = 10 Gbps**

4.1.3. Cabo de Fibra Óptica

Um cabo de fibra óptica é construído sobre uma estrutura de vidro ou plástico e **transmite sinais na forma de luz** (Forouzan, 2008), em vez de eletricidade.

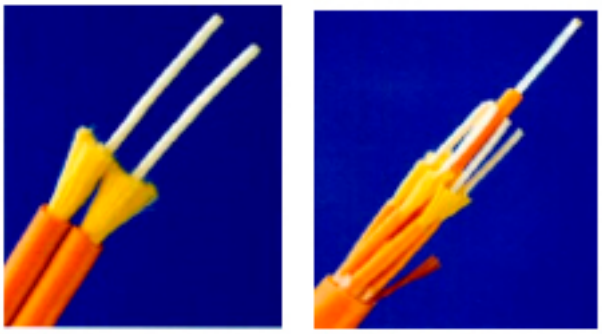


Figura - Fibra Óptica

Em uma extremidade do cabo, há um transmissor que emite pulsos de luz. Os pulsos trafegam pelo cabo até chegar ao receptor, onde são convertidos para sinais elétricos. Essas transmissões são unidirecionais. Na transmissão de pulsos de luz, um pulso indica um bit 1 e a ausência de pulso indica um bit 0.

Obs.: ao se escolher a fibra óptica como meio de transmissão do sinal de informação, o sistema **NÃO** é afetado por **interferência eletromagnética** de outros sistemas de radiofrequência que operem na região.

Os cabos de fibra óptica são **IMUNES** À INTERFERÊNCIA ELETROMAGNÉTICA, pois não possuem malha metálica.

<u>Dois TIPOS principais de fibras</u>: multimodo e modo único (ou monomodo):

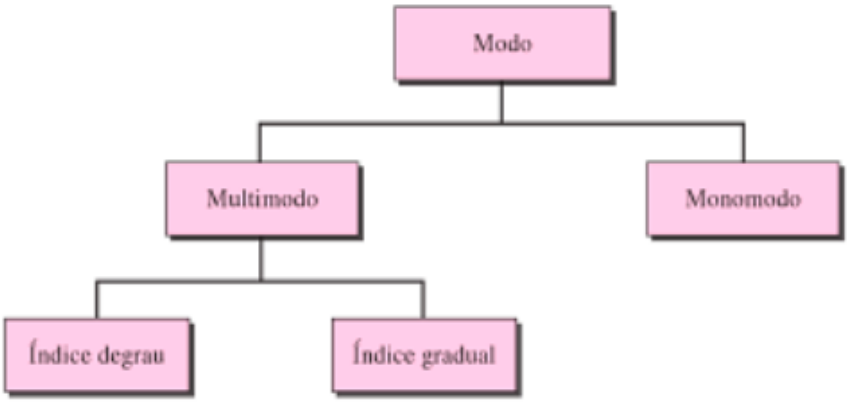


Figura. Modos de Propagação da Fibra Óptica - Fonte: Forouzan (2008, p. 199)

- A fibra **multimodo** tem o diâmetro maior permitindo o tráfego de vários pulsos, que vão ricocheteando no núcleo em ângulos diferentes;
- A fibra **modo único** (ou **monomodo**) tem o diâmetro menor permitindo a propagação do pulso somente em linha reta. Essas fibras são mais caras que as multimodo, mas são muito utilizadas em longas distâncias.

Principais características das fibras ópticas:

- Os pulsos podem se propagar por muitos quilômetros sem sofrer praticamente nenhuma perda;
- **Menor atenuação do sinal:** a distância de transmissão por fibra óptica é significativamente maior que a de qualquer outro meio de transmissão guiado. Um sinal pode percorrer 50 Km sem precisar de regeneração. No caso de cabos coaxiais ou de par trançado, precisamos de repetidores a cada 5 Km (Forouzan, 2008);
- **Imunidade a interferências eletromagnéticas:** ruídos eletromagnéticos **não** são capazes de afetar os cabos de fibra óptica, o que lhe confere alto desempenho, mas o custo de instalação e manutenção é caro. As fibras ópticas têm baixa atenuação do sinal e índice de refração baixo relativamente ao meio em que se encontrem;

- **Dimensões e peso reduzidos.** Suas dimensões reduzidas possibilitam expandir a estrutura de cabeamento sem que seja necessário aumentar os dutos de passagem dos cabos já existentes;
- A **transmissão é mais segura** por não permitir (ou dificultar muito) a interceptação, aumentando a segurança contra escutas;
- Entre as **desvantagens** no uso de fibra óptica: **sua instalação e sua manutenção exigem mão de obra especializada, que não se encontra com facilidade; a propagação da luz é unidirecional; os cabos e interfaces são relativamente mais caros** que outros meios de transmissão guiados (FOROUZAN, 2008).

4.2. Meios de Transmissão Não Guiados – Transmissão Sem Fio

Os meios de transmissão de dados não guiados são os que **envolvem o chamado espectro eletromagnético**, **permitindo o tráfego de dados sem fios.** Transportam ondas eletromagnéticas sem o uso de um condutor físico!

Obs.: **observe que os meios não guiados são os meios de transmissão sem fio, em que há a propagação de ondas eletromagnéticas através do espaço. Assim, nestes meios de transmissão a previsibilidade é muito MENOR, já que não temos controle do meio de transmissão.**

A atenuação do sinal é menos previsível em meios não guiados em comparação com os meios guiados!

Podemos dividir a transmissão sem fio em três grandes grupos:

- **ondas de rádio** (ondas que vão de 3 kHz a 1 GHz);
- **microondas** (ondas que vão de 1 a 300 GHz); e
- **ondas infravermelhas** (com frequências que vão de 300 GHz aos 400 THz).

A transmissão em uma **rede sem fio** é feita através de **ondas eletromagnéticas,** que se propagam pelo ar e podem cobrir áreas na casa das centenas de metros.

4.2.1. Classificação das Redes Sem Fio (Redes Wireless)

WPAN (Wireless Personal Area Network, Padrão IEEE 802.15):

- **Rede de computadores pessoal** - formada por nós muito próximos uns dos outros e próximos a uma pessoa;
- O termo **PAN** é bem novo, surgiu em função das novas tecnologias sem fio, como o **bluetooth**, que permitem a ligação de vários equipamentos que estejam separados por poucos metros;
- Esse tipo de rede é ideal para eliminar os cabos usualmente utilizados para interligar teclados, impressoras, telefones móveis, agendas eletrônicas, computadores de mão, câmeras fotográficas digitais, mouses e outros.

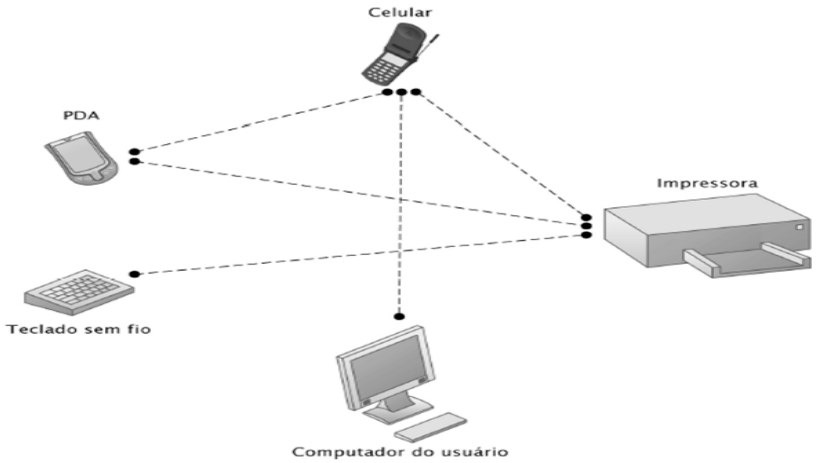


Figura – Exemplo de uma Rede WPAN

WLAN (Wireless Local Area Network), Padrão IEEE 802.11: é uma rede local sem fios com conexão à Internet, geralmente utilizada em escritórios, faculdades, aeroportos, entre outros locais.

WMAN (Wireless Metropolitan Area Network), Padrão IEEE 802.16 - WiMAX: as redes metropolitanas sem fios são utilizadas para a conexão de uma cidade, ou até mesmo em áreas um pouco menores como universidades. Um exemplo de rede que é classificada como WMAN, respeitando o padrão da norma IEEE 802.16, é o WiMAX.

WWAN (Wireless Wide Area Network), Padrão IEEE 802.20 - 3G/4G: nesta encontramos as redes sem fios de grandes extensões, ou seja, de área geográfica de dimensões maiores, como um país, ou mesmo o mundo inteiro. Os telefones celulares são os principais dispositivos utilizados nesse escopo de rede.

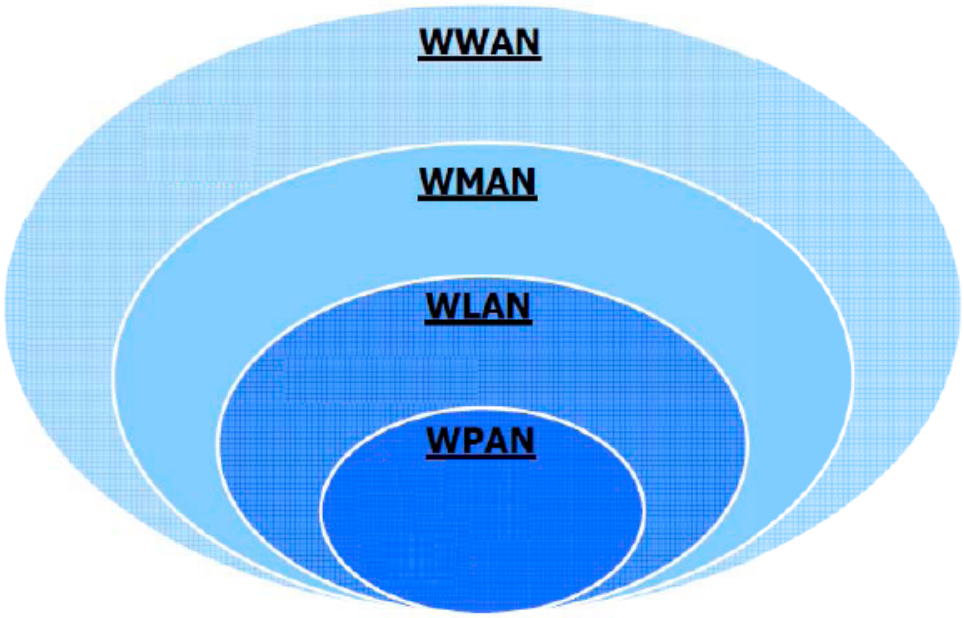


Figura. Redes Wireless

4.2.2. Nomenclatura dos Principais Componentes de uma Rede Sem Fio

STA (Wireless LAN Stations)	São os diversos clientes da rede.
AP (Access Points) – Pontos de Acesso	É o nó que **coordena** a comunicação entre as STAs dentro da BSS (conjunto de serviços básicos de uma **célula** - Área coberta por um AP). Funciona como uma ponte (bridge) de comunicação entre a rede sem fio e a rede convencional.
DS (Distribution System)	Corresponde ao backbone da WLAN, realizando a comunicação entre os APs.

4.2.3. Tipos de Dispositivos em Redes Sem Fio

Estações:

- Dispositivo compatível com interface e MAC 802.11;
- Micros, notebooks, PDAs etc.

Access Points (APs):

- Sistema de distribuição para estações associadas;
- Centraliza a comunicação;
- Também chamado de **concentrador**.

Routers: incorporam funções de switch, roteador, AP e às vezes modem ADSL.

4.2.4. Métodos de Acesso ao Meio

CSMA/CD (Collision Detection - Detecção de Colisão): nesse caso, o dispositivo monitora o meio para verificar a presença de sinal de dados. Se um sinal de dados está ausente, indicando que o meio está livre, o dispositivo transmite os dados. Se são detectados sinais que mostram que um outro dispositivo estava transmitindo ao mesmo tempo, todos os dispositivos **param** de enviar e tentam novamente mais tarde (CISCO, 2010).

Esse método é usado pelas tecnologias de rede Ethernet.

CSMA/CA (Collision Avoidance - Prevenção de Colisão): Cisco (2010) destaca que no **CSMA/CA** o dispositivo examina o meio para verificar a presença de sinal de dados. Se estiver livre, o dispositivo envia uma notificação através do meio com sua intenção de usá-lo. O dispositivo então envia os dados. **Esse método é usado pelas tecnologias de rede sem fio 802.11**.

4.2.5. Tipos de Mobilidade

A literatura destaca três tipos de mobilidade:

- **Mobilidade de terminais**: habilidade do usuário de utilizar seu terminal (i. e. dispositivo) **para se mover entre redes heterogêneas** (i. e. se mover entre diferentes sub-redes, possivelmente de diferentes domínios administrativos) enquanto continua a ter acesso ao mesmo conjunto de serviços em que está subscrito e permanece alcançável para mensagens ou requisições de outros dispositivos;
- **Mobilidade pessoal**: significa que um usuário deve poder ser globalmente alcançável através de um único identificador pessoal e ser capaz de iniciar ou aceitar sessões a partir de qualquer dispositivo;

- **Mobilidade de sessão**: refere-se à habilidade do usuário de manter uma sessão ativa enquanto muda de dispositivo.

4.2.6. Modos de Operação das Redes Wi-Fi

O **padrão 802.11 possui dois modos de operação**, que são:

- **Ad-hoc**: nesse caso, temos uma comunicação ponto-a-ponto, e cada dispositivo de rede pode se comunicar diretamente com o outro, sem a necessidade de uma estação base;

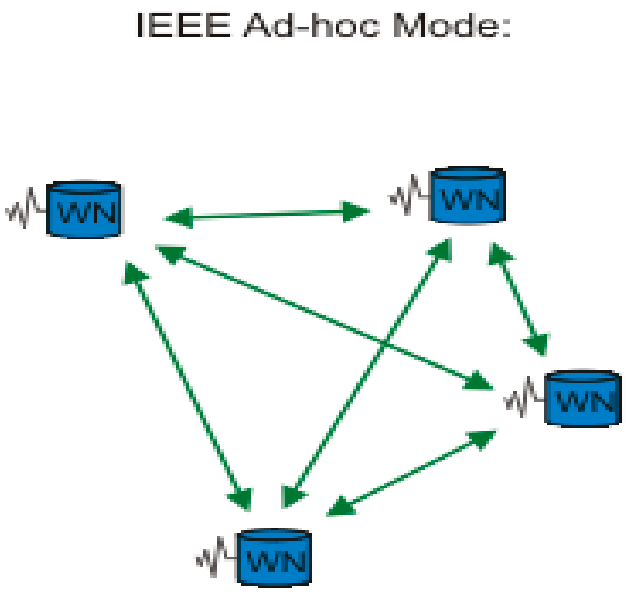


Figura. Modo Ad-Hoc

- **Infraestrutura:** os dispositivos se comunicam utilizando o conceito de **células**. As células formam um conjunto de dispositivos controlados por uma **estação base (ou ponto de acesso – Access Point).**

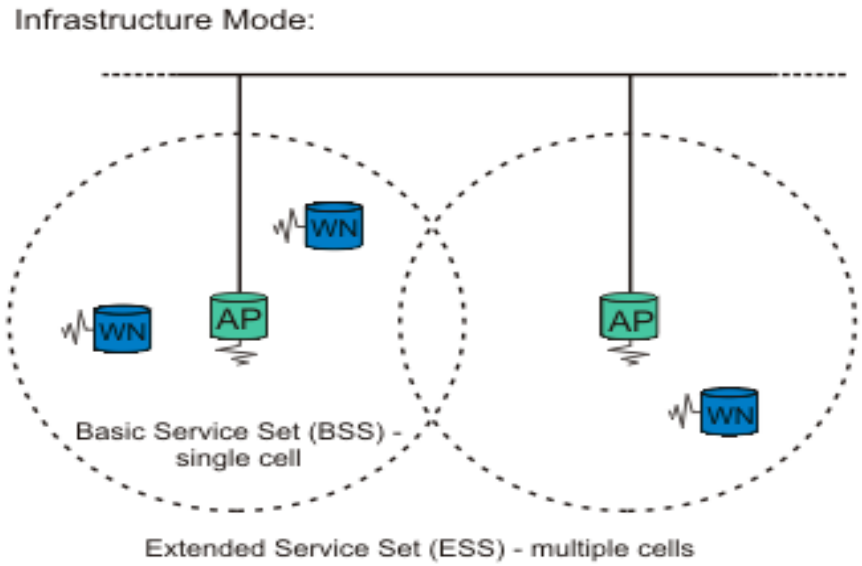


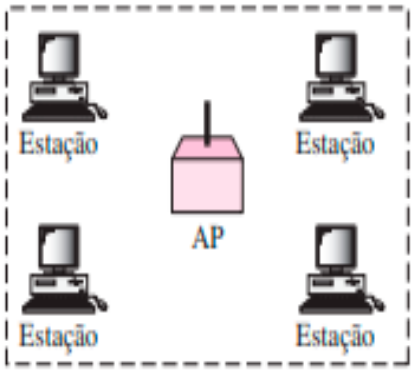
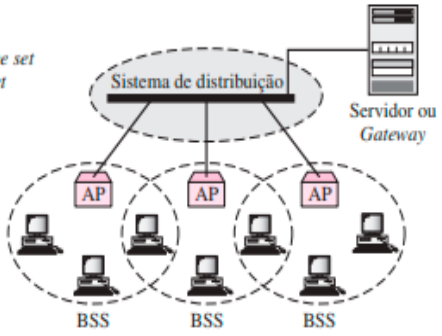
Figura. Modo de operação Infraestrutura

A banca poderá utilizar também os termos **DCF** (Distributed Coordination Function) e **PCF** (Point Coordination Function), que serão vistos em seguida.

Distributed **C**oordination **F**unction	Termos sinônimos: **sem estação base**/**ad hoc**. As estações competem entre si pelo meio. Uso de CSMA/CA. Não existe a figura de um concentrador (Ponto de Acesso). Modo obrigatório (os fabricantes sempre lançam produtos com esse modo).
Point **C**oordination **F**unction	Termos sinônimos: com estação base/**Infraestrutura**. Sem colisão. AP escuta estações em turnos para verificar se há frames. Estação-base efetua o **polling** (ato de revezar entre as estações, entregando ou recebendo alguma informação). É opcional.

4.2.7. Tipos de Serviços Básicos

Quanto aos serviços básicos providos em uma região que tem uma rede sem fio, merecem destaque:

IBSS (Independent Basic Service Set)	**– BSS sem um AP (Redes Ad-hoc).** – Uma das estações pode assumir a função de coordenação BSS: *Basic service set*  Rede *ad hoc* (BSS sem AP)
BSS (Basic Service Set)	- É o conjunto de serviços básicos de uma célula (Área coberta por **um** AP). BSS: *Basic service set* AP: *Access point*  Rede de infra-estrutura (BSS com AP)
ESS (Extended Service Set)	**– Um conjunto de BSS.** – Em uma rede ESS, é comum o acontecimento de **roaming**. ESS: *Extended service set* BSS: *Basic service set* AP: *Access point* 

Obs.: **BSA (*Basic Service Area*):** termo que designa uma área em que os dispositivos móveis podem se comunicar.

4.2.8. Principais Padrões da Família IEEE 802.11

Os principais padrões da família **IEEE 802.11 (Wi-Fi)** são:

Padrão	Faixa de Frequência	Velocidade de Transmissão	Largura de Banda	Observação
802.11**b**	2,4 GHz	11 Mbps	20 MHz	O padrão mais antigo
802.11**g**	2,4 GHz (compatível com 802.11b)	54 Mbps	20 MHz	Atualmente, é o mais usado.
802.11**a**	5 GHz	54 Mbps	20 MHz	Pouco usado no Brasil. Devido à diferença de frequência, equipamentos desse padrão não conseguem se comunicar com os outros padrões citados.
802.11**n**	Utiliza tecnologia MIMO (*Multiple Input/Multiple Output*), **frequências de 2,4 GHz e/ou 5 GHz** (compatível portanto com 802.11b e 802.11g e teoricamente com 802.11a)	Diversos fluxos de transmissão: 2x2, 2x3, 3x3,4x4. Velocidade nominal subiu de 54 para **300 Mbps** (**600 Mbps** nos APs 4x4, capazes de transmitir **4** fluxos simultâneos.	20 MHz ou 40 MHz	Padrão recente e que está fazendo grande sucesso. Este padrão pode chegar **até os 600 Mbps**, quando operando com **4 antenas** no transmissor e no receptor, e utilizando a modulação **64-QAM** (Quadrature Amplitude Modulation).

A literatura já cita um novo padrão a caminho, o **802.11ac**, prometendo velocidades em torno de 1Gbps, largura de banda de 160MHz e multi-user MIMO.

A taxa máxima de transmissão de dados no padrão IEEE 802.11b é de 11 Mbps, e o acesso ao meio é do tipo CSMA/CA.

4.2.9. Serviços

Obs.: o padrão 802.11 estabelece que cada LAN sem fio compatível deve fornecer **NOVE** tipos de serviços, divididos em duas categorias, que são: **5 (cinco) serviços de distribuição e 4 (quatro) serviços da estação.**

Os **serviços de distribuição** são fornecidos pelas **estações-base** (ou **Access Points**, ou **pontos de acesso**) e lidam com a **mobilidade** das estações à medida que elas entram e saem das células, conectando–se e desconectando–se dos pontos de acesso. São estes:

Associação	Esse serviço é usado pelas estações móveis para conectá-las às estações base. Nela, a estação móvel efetua a varredura dos 11 canais de frequência, em busca dos quadros se sinalização emitidos pela estação-base. Por meio desses quadros, a estação-base anuncia sua identidade (endereço MAC) e seus recursos (SSID – Service Set Identifier).
Desassociação	A estação móvel ou a estação base pode se desassociar, interrompendo assim o relacionamento. Uma estação deve usar esse serviço antes de se desligar ou sair.
Reassociação	Uma estação pode mudar sua estação base preferida usando esse serviço. Esse recurso é útil para estações móveis que se deslocam de uma célula para outra.
Distribuição	Esse serviço determina como rotear quadros enviados à estação base. Se o destinatário for local para o AP, os quadros poderão ser enviados diretamente pelo ar. Caso contrário, eles terão de ser encaminhados pela rede fisicamente conectada.
Integração	Se um quadro precisar ser enviado por meio de uma rede que não seja 802.11, com um esquema de endereçamento ou um formato de quadro diferente, esse serviço cuidará da conversão do formato 802.11 para o formato exigido pela rede de destino.

Os **serviços da estação** são usados geralmente depois que ocorre a associação e são intracelulares (ou seja, se relacionam a ações dentro de uma única célula):

Autenticação	O ponto de acesso envia um quadro de desafio especial à estação móvel, esta demonstra conhecimento da chave secreta (senha) criptografando o quadro de desafio e transmitindo de volta ao ponto de acesso. Se o resultado for correto, a estação móvel será completamente registrada na célula.
Desautenticação	Quando uma estação autenticada quer deixar a rede;
Privacidade	Este serviço administra a criptografia e a descriptografia, para que as informações enviadas pela rede sem fio se mantenham confidenciais. O algoritmo de criptografia utilizado é o RC4;
Entrega de Dados	Transmissão efetiva de dados, modelada com base no padrão Ethernet. Assim como em redes cabeadas, a transmissão dos dados não é totalmente confiável, então camadas mais elevadas devem assegurar a integridade das informações através de detecção e correção de erros.

4.2.10. Problemas de Segurança em Redes Sem Fio (Wireless)

Riscos maiores de invasão. Não é necessário acesso físico à rede para invadir.

Má configuração de APs. Configuração padrão geralmente é insegura – sem criptografia e com SSID de rede padrão.

Clientes/APs não autorizados. Não há autenticação e DHCP concede IP a qualquer um.

Interceptação de tráfego:

- Sniffer sem necessidade de acesso físico à rede;
- Vários protocolos com senha em texto simples (SMTP; POP; FTP).

4.2.11. Padrões Criptográficos

WEP (Wired Equivalency Privacy - sigla de "Privacidade Equivalente à de Redes com Fios") foi a primeira tentativa de se criar um protocolo eficiente de proteção de redes WI-FI em 1997. Hoje é um protocolo obsoleto no quesito segurança (muito vulnerável).

TKIP (Temporal Key Integrity Protocol): é um protocolo temporário de gerenciamento de chaves. Trata-se de um algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacote. A senha é modificada automaticamente por padrão a cada 10.000 pacotes enviados e recebidos pela sua placa de rede (Fonte: Wikipedia).

WPA (Wi-Fi Protected Access - sigla de **"Acesso Protegido a WiFi"),** também conhecido como **WEP2** é um **WEP melhorado**. Serviu como um padrão de "transição" entre o WEP e o WPA2. Surgiu com o objetivo de substituir o WEP, considerado inseguro. O **WPA utiliza o algoritmo Temporal Key Integrity Protocol (TKIP) como padrão para criptografia de chaves por pacote**. O TKIP utiliza o sistema de criptografia do WEP, mas usa no **algoritmo RC4** chaves de 128 bits. Além disso, possui um sistema mais complexo de geração de chaves, pois a chave de criptografia do frame é extraída a partir do endereço MAC do transmissor, combinado com a chave de criptografia da rede e parte do IV *(vetor de inicialização)*.

O **WPA2** segue o **padrão 802.11i** e **substitui formalmente o WEP**. Assim, é mais seguro do que o WEP!

WPA2 é o WPA + AES (ao invés do RC4).

Obs.: **o primeiro protocolo de criptografia disponível para redes Wi-Fi é baseado em um algoritmo chamado RC4, que é um codificador de fluxo.**

5. Tecnologias de Redes Locais Ethernet/Fast Ethernet/Gibabit Ethernet

Com o objetivo de facilitar a interligação e a compatibilidade dos sistemas de comunicações, foram definidos **padrões de redes de computadores**, que **envolvem a definição dos tipos de meios e os protocolos de acesso ao meio**.

As **normas IEEE 802** são subdivididas em diversos **padrões**, sendo que a seguir exemplificamos alguns deles:

802.1	**Gerência de Rede.**
802.2	**LLC (Logical Link Control).**
802.3	**-802.3 – Ethernet e especifica a sintaxe e a semântica MAC (Media Access Control).** **-802.3u - Fast Ethernet.** **-802.3z - Gigabit Ethernet.** **-802.3ae - 10 Gigabit Ethernet.**
802.4	**Token Bus.**
802.5	**Token Ring (inativo).**
802.6	**Redes Metropolitanas.**
802.7	**MANs de Banda Larga.**
802.8	**Fibra Óptica.**
802.9	**Integração de Redes Locais.**
802.10	**Segurança em Redes Locais.**
802.11 (a/b/g/n)	**Wi-fi - Redes Wireless (LANs Sem Fios).**
802.15	**Wireless Personal Area Network (Bluetooth).**
802.16	**Broadband Wireless Access (Wimax).**
802.20	**MOBILE-Fi (WWAM)**
802.22	**Wireless Regional Area Network(WRAN)**

Tabela - Padrões IEEE 802. Fonte: Quintão (2020)

6. Endereçamento TCP/IP

Em uma rede TCP/IP, cada placa de rede existente, em cada computador, é identificada por um número, chamado **endereço IP**.

Esse endereço IP consiste em conjuntos de 8 bits, chamados por isso de **octetos**.

O padrão mais utilizado atualmente é o **IPV4**, em que trabalharemos com 4 conjuntos de 8 bits (4 octetos). Os octetos, quando representados, são separados por pontos. Veja abaixo dois exemplos de endereço IP:

0 0 0 0 1 0 1 0. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 1
1 1 0 0 1 0 0 0. 1 1 1 1 1 1 1 1. 1 0 0 0 1 1 1 0. 0 0 0 0 1 0 1 0

Na verdade, a forma mais usual de representação do endereço IP é em números decimais. Essa notação divide o endereço IP em quatro grupos de 8 bits (octeto) e representa o valor decimal de cada octeto binário, separando-os por um ponto. Dessa forma, podemos transformar os endereços acima nos endereços seguintes, respectivamente:

10.0.0.1

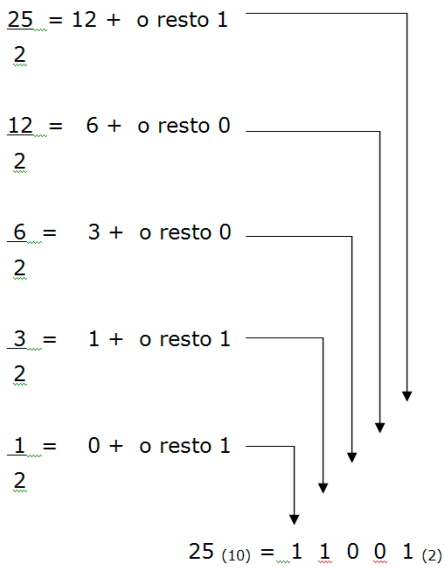
200.255.142.10

Sistemas de numeração:

- Na **notação pós-fixa**, também chamada de **n**otação **p**olonesa **r**eversa ou **RPN**, as operações são realizadas na ordem inversa àquela em que aparecem;
- Numeração Decimal (base 10): a numeração decimal é aquela em que a base de contagem é 10. Assim sendo, necessitamos de 10 símbolos (algarismos), para representar todos os números possíveis, nesta base. Os símbolos para essa base são os algarismos de 0 até 9. Essa é a base numérica em que trabalhamos normalmente e ninguém pergunta qual é a base numérica na qual trabalhamos, pois já está implícito para todos que estamos na base 10. Entretanto os computadores, não sabem trabalhar com ela. Computadores trabalham não com base 10, mas sim com **base 2** ou **notação binária**;
- **Numeração Binária (base 2):** como exemplo vamos converter o número 25 em binário. Iremos utilizar o **método das divisões sucessivas por 2 para isso**. Nesse método executa-se a divisão sucessiva pelo decimal 2 até achar um quociente 0. Achando zero no

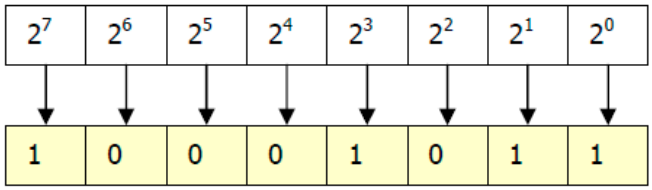
quociente, pega-se os restos dessa divisão (que sempre é 0 ou 1) pegando da direita para a esquerda (será escrito de modo inverso) onde o primeiro binário (o mais significativo, aquele que fica mais à esquerda) será o último resto.

$= (11001)_2$



Outro exemplo: passar o número binário 1 0 0 0 1 0 1 1 para o seu equivalente decimal. Veremos agora o processo inverso.

Passo 1: escreva a composição das potências de 2 e em seguida associe o número binário pertinente:



Passo 2: efetuar as multiplicações casa a casa, da composição das potências pelos dígitos do número pertinente e somar os valores:

$1 \times 2^0 + 1 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 + 0 \times 2^4 + 0 \times 2^5 + 0 \times 2^6 + 1 \times 2^7 =$

$1 \times 1 + 1 \times 2 + 0 + 1 \times 8 + 0 + 0 + 0 + 1 \times 128 =$ **139**

Se você quiser saber como ocorreu a transformação do número apresentado em nossa aula da base binária para decimal, acompanhe a descrição seguinte.

Na base binária existem os algarismos 0 e 1. E na base decimal temos os algarismos de 0 a 9.

Para o número

1 1 0 0 1 0 0 0. 1 1 1 1 1 1 1 1. 1 0 0 0 1 1 1 0. 0 0 0 0 1 0 1 0

Devemos realizar a conversão de grupo a grupo de 8 dígitos.

Uma das formas de se realizar essa conversão é a seguinte:

1 – Vamos enumerar as posições do número binário, da direita para a esquerda, e de modo que a posição mais à direita seja a posição 0; Assim para o número **11001000**, teríamos:

Número em binário	1	1	0	0	1	0	0	0
Posição	7	6	5	4	3	2	1	0

2 - Em seguida, operamos o seguinte cálculo:

Sendo:

- n, o algarismo em binário;
- p, a posição de n;

Faz-se: $n*2^p+n_1*2^{p1}+n_2*2^{p2}+n_3*2^{p3}...$

Assim, o número 110001000, ficaria assim:

$0*2^0+0*2^1+0*2^2+1*2^3+0*2^4+0*2^5+1*2^6+1*2^7=$

$= 0 + 0 + 0 + 8 + 0 + 0 + 64 + 128 = 200$

Para o número 11111111, teremos:

Listar as posições de cada algarismo:

Número em binário	1	1	1	1	1	1	1	1
Posição	7	6	5	4	3	2	1	0

(observe que a listagem das posições é sempre da direita para esquerda)

Logo o cálculo fica assim:

$1*2^0+1*2^1+1*2^2+1*2^3+1*2^4+1*2^5+1*2^6+1*2^7=$

$= 1 + 2 + 4 + 8 + 16 + 32 + 64 + 128 = 255$

Os mesmos procedimentos acima são executados para os outros dois grupos (10001110 . 00001010). E no final, temos que:

11001000 = 200 11111111 = 255 10001110 = 142 00001010 = 10

E, portanto, 11001000 . 11111111 . 10001110 . 00001010 é igual a 200.255.142.10.

Disso tudo, concluímos que o **menor octeto possível** é o **00000000**, que é igual a **0 em decimal,** e que o **maior octeto possível** é **11111111**, que é igual a **255 em decimal**. Ou seja, **cada octeto pode ir de 0 a 255**.

Endereço IP Fixo: é configurado diretamente no computador pelo usuário ou administrador da rede. Normalmente, usado em servidores ou quando se quer identificar de forma direta um computador.

Endereço IP Dinâmico: configurado para ser recebido automaticamente por um computador quando este se conecta à rede. Fornecido por um servidor que usa o protocolo **DHCP (Dynamic Host Configuration Protocol).**

Versão IPv4: versão usada atualmente, formada por 4 bytes (**4 octetos ou 32 bits**).

Versão IPv6: os endereços IPv6 são normalmente escritos como **oito grupos de 4 dígitos hexadecimais**. O padrão hexadecimal comporta as seguintes representações: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Exemplo:

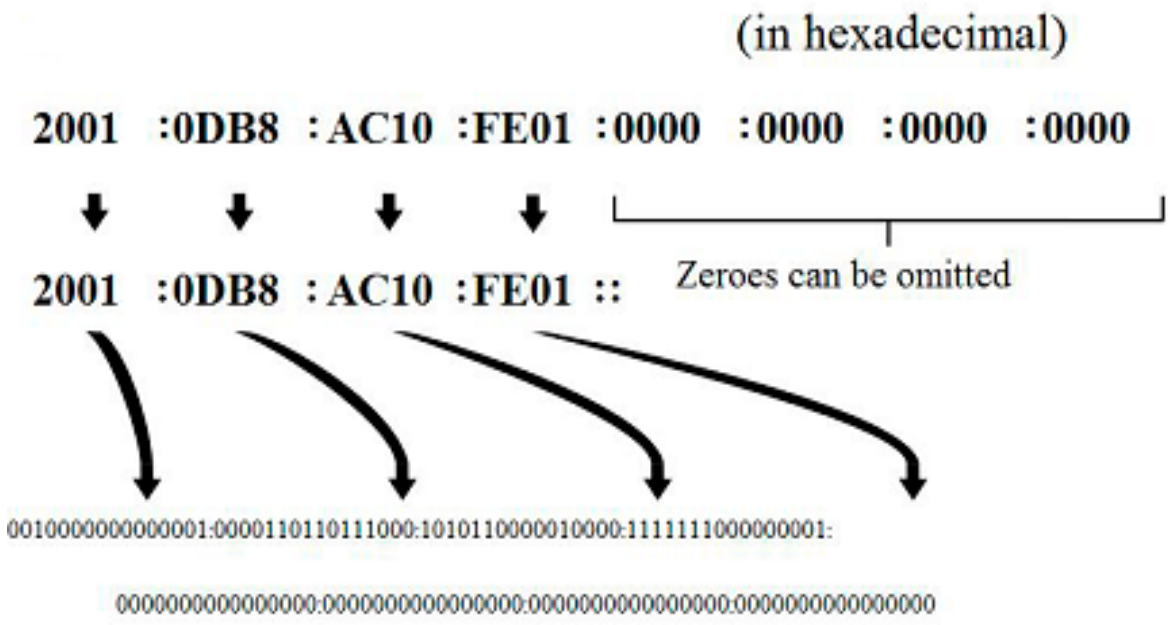


Figura. Um Endereço IPv6

Os endereços **IPs** são divididos e**m classes** como mostra o quadro a seguir:

Classe	1º octeto começa com (em binário)	1º octeto pode ser (em decimal)	Objetivo	Exemplo de Endereço IP
A	0	1 a 126	Grandes redes	**100**.1.240.28
B	10	128 a 191	Médias redes	**157**.100.5.195
C	110	192 a 223	Pequenas redes	**205**.35.4.120
D	1110	224 a 239	Multicasting.	Não usado para micros (hosts) individuais.
E	1111	240 a 254	Faixa reservada para fins futuros.	-

Tabela: Detalhes sobre o 1º octeto das classes

Máscara de Sub-rede e Sub-redes.

Máscara de sub-rede é um recurso utilizado para segmentar redes. Por que isso? Na verdade, esse é um recurso obrigatório na rede TCP/IP. Com ele, poderemos ter várias sub-redes diferentes dentro de uma rede, utilizando o mesmo cabeamento.

Dentro de uma empresa, toda a parafernália de computadores interligados denomina-se rede. As divisões lógicas desses micros, formando blocos separados denominam-se **sub-redes**. **Essa divisão lógica é feita, justamente, com base no endereço IP e na máscara de sub-rede**.

Na figura seguinte, fica bem caracterizada a diferença entre a rede **física**, representada pelos micros interligados por fios e hubs, e a rede lógica. Os círculos pontilhados representam as sub-redes (redes **lógicas**).

São três sub-redes. Note que a ideia física é totalmente diferente da ideia lógica. No círculo superior vemos máquinas que, mesmo distantes, pertencem à mesma sub-rede.

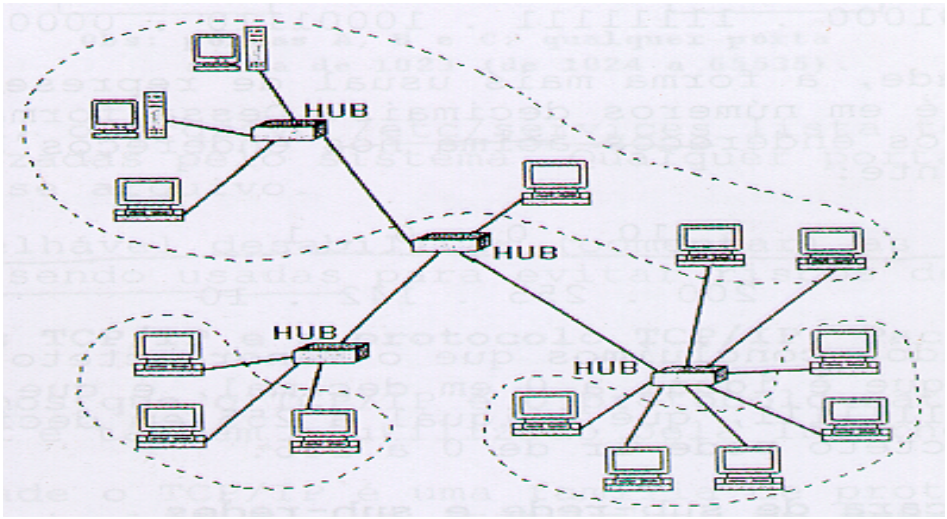


Figura. Sub-Redes

Para definirmos a **máscara de sub-rede**, utilizamos o mesmo sistema do endereço IP, ou seja, 4 octetos. Nesse esquema, tudo que for 1 representa rede e tudo que for 0 representa host. Esse artifício não admite a mistura de algarismos 0 e 1. Também não pode haver algarismo 0 antes do algarismo1.Veja a seguir dois exemplos de máscara de sub-rede:

1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0
1 1 1 1 1 1 1 1. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

Repare que não houve a mistura entre 0 e 1 ou a ocorrência de bit 0 antes de bit 1. Ou seja: a máscara de sub-rede, em relação ao endereço IP, define até onde vai a sub-rede e onde começam as máquinas.

A forma mais usual de representação de máscara de sub-rede é em números decimais. Dessa forma, podemos transformar as máscaras anteriores:

255.255.0.0
255.0.0.0

Nos casos anteriores, 0 representa host e 255 rede.

Poderá haver fragmentação do octeto. Exemplo:

11111111.11111100.00000000.00000000 = 255.252.0.0

No caso acima, no 2º octeto há uma divisão que fará com que os 6 primeiros bits do octeto do respectivo endereço IP representem rede e os 2 últimos hosts.

A identificação final da máquina será a combinação do endereço IP com a máscara de rede.

Vejamos abaixo:

Endereço IP: 200.255.142.10

Máscara de sub-rede 255.255.255.0

Octeto 200 com máscara 255- designa rede

Octeto 255 com máscara 255- designa rede

Octeto 142 com máscara 255- designa rede

Octeto 10 com máscara 0- designa host

Sendo assim, a fração 200.255.142 serve para designar a sub-rede a qual o micro (host) pertence, e a fração 10 designa o número do host dentro da sub-rede. É norma manter os 4 octetos para designar rede ou host, completando com 0 os espaços vagos. Assim, ainda no exemplo anterior, estamos falando da rede 200.255.142.0 e do host 0.0.0.10.

Apenas para fixarmos o conhecimento, vamos dar exemplos de endereços IP diversos, juntamente com sua máscara de rede e a correta interpretação:

Endereço IP 10. 10. 20. 50

Máscara de sub-rede 255. 0. 0. 0

Sub-rede 10. 0. 0. 0

Host 0. 10. 20.50

Endereço IP 14. 120. 210.150

Máscara de sub-rede 255. 0. 0. 0

Sub-rede 14. 0. 0. 0

Host 0. 120. 210.150

Endereço IP 143. 10. 20. 50

Máscara de sub-rede 255. 255. 0. 0

Sub-rede 143. 10. 0. 0

Host 0. 0. 20.50

É importante saber que sub-redes diferentes não se enxergam, a não ser que utilizemos um recurso chamado roteamento de rede.

Sendo assim, se a máscara do meu host for 255.255.255.0 e o meu endereço IP for 210.15.5.5, somente outra máquina com máscara 255.255.255.0 e endereço IP 210.15.5.x enxergará a minha máquina, por pertencerem à mesma sub-rede, a não ser que haja o roteamento.

Obs.: a **máscara de sub-rede** usa o mesmo formato de um endereço IP. A única diferença é que ela **usa o binário 1 em todos os bits que especificam o campo de rede**.
A máscara de sub-rede informa ao dispositivo quais octetos de um endereço IP devem ser observados quando da comparação com o endereço de destino do pacote.

As primeiras três classes de endereços IP têm uma máscara default ou natural, destacada a seguir.

Classe	Primeiros bits	Núm. de redes	Número de hosts	Máscara padrão
A	0	126	16.777.214	255.0.0.0
B	10	16.382	65.534	255.255.0.0
C	110	2.097.150	254	255.255.255.0
D	1110	Utilizado para tráfego Multicast.		
E	1111	Reservado para uso futuro.		

Classful adresses são aqueles que mantêm sua máscara de sub-rede natural. Ex. Rede 131.8.0.0 tem uma máscara natural de 255.255.0.0.

Outra maneira de representar a máscara 255.255.0.0 é simplesmente contar o número de bits na máscara e colocar o decimal correspondente precedido de uma barra "/".

Exemplo:

Rede 131.8.0.0 tem a máscara de sub-rede 255.255.0.0

Representação binária dessa máscara:

1111 1111.1111 1111.0000 0000. 0000 0000

Portanto, a máscara pode ser representada como /16.

Dado um endereço e uma máscara de sub-rede, pode-se determinar a rede à qual ele pertence.

Para isso faça.

Vamos escolher o primeiro host, por exemplo, que é 131.108.2.16, e transformá-lo em binário, o que gera:

1000 0011.0110 1100.0000 0010.0001 0000.

Em seguida, vamos achar a máscara em binário, 255.255.255.0, que será: **1111 1111.1111 1111.1111 1111.0000 0000**/24.

Agora, executamos um AND lógico entre o endereço e a máscara, o que nos dará a sub-rede, que é:

1000 0011.0110 1100.0000 0010.0000 00.

Convertendo III (rede) em decimal temos: 131.108.2.0.

Endereço = 131.108.2.16

Máscara de Sub-rede = 255.255.255.0

Endereço: **1000 0011.0110 1100.0000 0010.0001 0000**

Máscara Sub-Rede: **1111 1111.1111 1111.1111 1111.0000 0000**

AND lógico **1000 0011.0110 1100.0000 0010.0000 0000**

Assim, o endereço dado pertence à rede 131.108.2.0.

Faixas de Endereços Que Têm Usos Específicos e Regras Especiais:

Existem faixas de endereços que têm usos específicos e regras especiais. Vejamos.

Rota Default: a sub-rede 0.0.0.0 é conhecida como **rota default**. O endereço 0.0.0.0 especificamente é utilizado para operações de DHCP ou para indicar saída de dados para sub-redes diferentes da local. É uma sub-rede reservada e não deve ser usada para numerar máquinas.

Loopback: a sub-rede 127.0.0.0 é conhecida como loopback. Serve para testes em placas de rede. Todas as placas de rede também respondem localmente pelos endereços 127.0.0.1, 127.0.0.2, etc., sem a necessidade de numeração. É uma rede reservada e não deve ser usada para numerar máquinas.

Especiais: As **sub-redes superiores a 224.0.0.0**, inclusive, são **privadas e reservadas**, por vários motivos, e não podem numerar máquinas.

Clientes Privados: Dos mais de 4 bilhões de endereços IPs disponíveis, três faixas são reservadas para redes privadas. Essas faixas não podem ser roteadas para fora da rede privada, ou seja, não podem se comunicar diretamente com a Internet.

Dentro das classes A, B e C foram reservadas redes, definidas pela RFC 1918, que são conhecidas como **endereços de rede privados.**

São eles:

Endereço	Faixa de IP
10.0.0.0/8	(10.0.0.0 – 10.255.255.255)
172.16.0.0/12	(172.16.0.0 – 172.31.255.255)
192.168.0.0/16	(192.168.0.0 – 192.168.255.255)

O papel do NAT consiste em traduzir os endereços privados que não são válidos na Internet para um endereço válido, ou seja, que possa navegar na Internet.

Ao implantar uma intranet, utilize uma dessas faixas. Isso dará um certo grau de segurança.

Broadcast e Multicast:

- **Broadcast** é o envio de informações em massa;
- Basicamente, quando um pacote é enviado e ele passa por todos os hosts da sub-rede, esse tráfego é chamado de broadcast;
- O broadcast controlado, enviado apenas para alguns pontos da rede, é denominado **multicast;**
- O último endereço possível em uma sub-rede é denominado **endereço de broadcast,** pois o sistema sabe que ele é o limite máximo da sub-rede.

Utilização dos IPs da sub-rede: o **IP inicial de uma sub-rede**, **bem como o final**, não podem ser utilizados para numerar páginas, pois representam a sub-rede e o seu broadcast.

Exemplo:

Assim, em uma sub-rede 200.244.23.0, com máscara 255.255.255.0, notamos o seguinte:

Faixa possível: de 200.244.23.0 a 200.244.23.255

Endereço de sub-rede: 200.244.23.0

Endereço de broadcast: 200. 244.23.255

Faixa utilizável: de 200.244.23.1 a 200.244.23.254

Gateway e Default-Gateway:

- **Gateway** é um nome técnico que designa um roteador de rede. O principal roteador de uma rede é o **default gateway**;
- A sua função é procurar outras sub-redes por máquinas requisitadas mas que não pertençam a sub-rede.

Exemplo:

Sub-rede: 10.0.0.0

Default Gateway: 10.20.2.5

Máquina requisitada: 172.10.20.20

Máquina requisitante: 10.0.0.10

Como a máquina requisitada não pertence à sub-rede, a máquina requisitante contactará o **Default Gateway** da sub-rede, que tentará buscar, na sub-rede 172.10.0.0, a máquina requisitada.

É óbvio que, por ser gateway (roteador), a máquina 10.20.2.5 tem que ter ligação com a rede 172.10.0.0.

Endereçamento e Roteamento: em uma rede TCP/IP, cada computador (ou melhor, cada placa de rede, caso o computador possua mais do que uma) possui um endereço numérico formado por **4 octetos (4 bytes)**, geralmente escritos na forma **w.x.y.z**.

Além deste Endereço IP, cada computador possui uma **máscara de rede** (network mask ou subnet mask), que é um número do mesmo tipo mas com a restrição de que ele **deve começar por uma sequência contínua de bits em 1, seguida por uma sequência contínua de bits em zero**. Assim, a **máscara de rede** pode ser um número como 11111111.11111111.00000000.00000000 (255.255.0.0), mas nunca um número como 11111111.11111111.00000111.00000000 (255.255.7.0).

A **máscara de rede serve para quebrar um endereço IP em um endereço de rede e um endereço de host**. Todos os computadores em uma mesma rede local (fisicamente falando, por exemplo, um mesmo barramento Ethernet) devem ter o mesmo endereço de rede, e cada um deve ter um endereço de host diferente. Tomando-se o endereço IP como um todo, cada computador em uma rede TCP/IP (inclusive em toda a Internet) possui um endereço IP único e exclusivo.

O InterNIC controla todos os endereços IP em uso ou livres na Internet, para evitar duplicações, e reserva certas faixas de endereços chamadas de **endereços privativos** para serem usados em redes que não irão se conectar diretamente na Internet.

Quando o IP recebe um pacote para ser enviado pela rede, ele quebra o endereço destino utilizado a máscara de rede do computador e compara o endereço de rede do destino com o endereço de rede dele mesmo. **Se os endereços de rede forem iguais, isto significa que a mensagem será enviada para um outro computador na mesma rede local**, então o pacote é repassado para o protocolo de enlace apropriado (em geral o Ethernet).

Se os endereços forem diferentes, o IP envia o pacote para o default gateway, que é nada mais do que o equipamento que fornece a conexão da rede local com outras redes. Este equipamento pode ser um roteador dedicado ou pode ser um servidor com múltiplas placas de rede, e se encarrega de encaminhar o pacote para a rede local onde está o endereço IP do destino.

É importante que o endereço IP do **default gateway** esteja na mesma subnet da máquina sendo configurada, caso contrário ela não terá como enviar pacotes para o default gateway e assim só poderá se comunicar com outros hosts na mesma subnet.

Obs.: **Resumindo, um computador qualquer em uma rede TCP/IP deve ser configurado com pelo menos estes três parâmetros**:
-o seu endereço IP exclusivo;
-a sua máscara de rede (que deve ser a mesma utilizada pelos demais computadores na mesma LAN); e
-o endereço IP do default gateway.

7. Autenticação e Login

Logon: procedimento de abertura de sessão de trabalho em um computador. Normalmente, consiste em fornecer para o computador um username (também chamado de login) e uma senha, que passarão por um processo de validação.

Login/Username/ID: identificação de um usuário para um computador, ou seja, o nome pelo qual o sistema operacional irá identificar o usuário.

Senha: é a segurança utilizada para dar acesso a serviços privados pertinentes ao usuário.

User: usuários de serviços de um computador, normalmente registrado através de um login e uma password (senha).

É por meio da autenticação que se confirma a identidade da pessoa ou entidade que presta ou acessa as informações. Recursos como senhas (que, teoricamente, só o usuário conhece), biometria, assinatura digital e certificação digital são usados para essa finalidade.

8. Alguns Comandos de Redes

Ipconfig:

- Um funcionário está usando um computador com o sistema operacional Windows 8, em português, e **deseja saber o endereço IP de sua máquina;**
- Para isso, ele deve **abrir uma janela de execução do Windows utilizando o atalho Tecla do Windows + R, digitar cmd seguido de ENTER** e, na janela aberta, digitar ipconfig -all seguido de ENTER;
- O mesmo procedimento é válido no Windows 7. Observe que uma série de informações é obtida por meio desse comando, como: **endereço IP, máscara de sub-rede, endereço físico do computador (MAC Address) etc.**

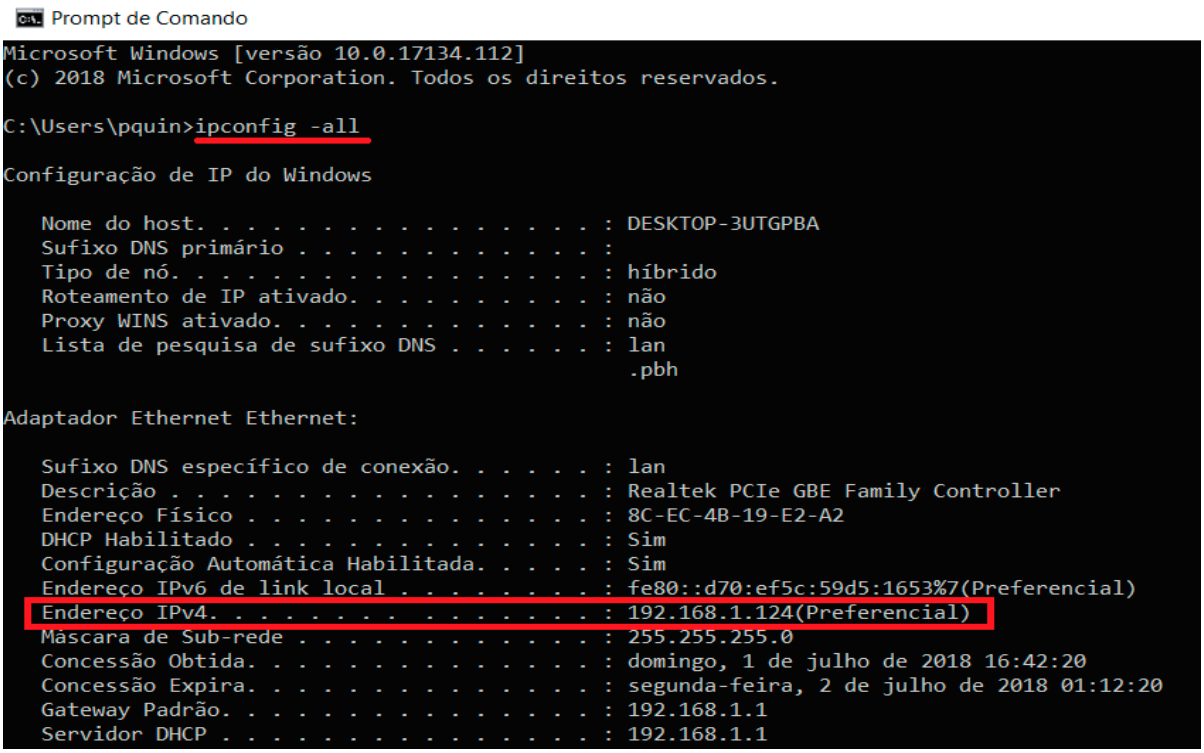
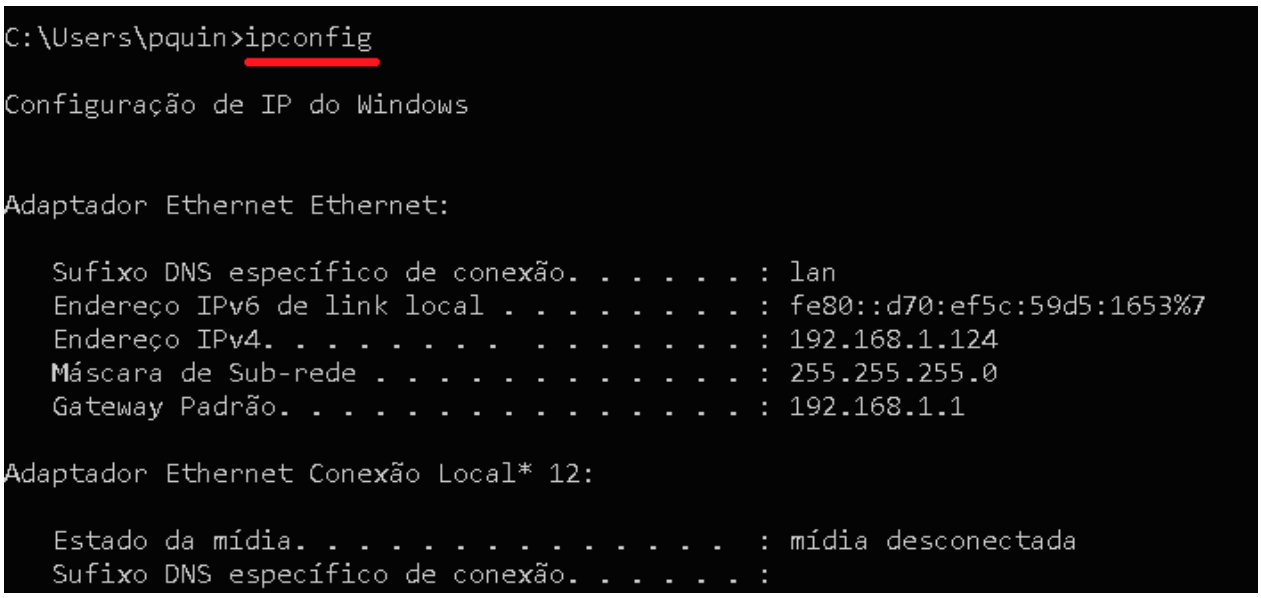


Figura. Extraída do Windows 10. Similar para Windows 8.

O comando **ipconfig** mostra os dispositivos de rede existentes no computador, bem como o respectivo endereço IP que cada dispositivo conseguiu obter, se for o caso.



ARP:

O comando do prompt do Windows que exibe e modifica as tabelas de conversão de endereços IP para endereços físicos usadas pelo protocolo de resolução de endereços é: **ARP**.

O **ARP (Address Resolution Protocol)** é responsável por mapear e converter os endereços IP (lógico) em endereços MAC (endereço físico), ou seja, passar do nível da camada de rede para a camada de enlace.

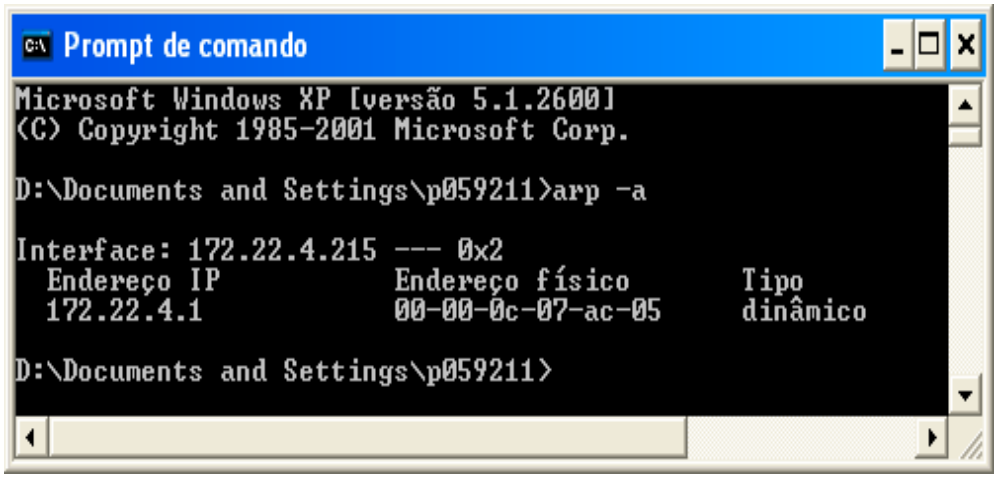
```
C:\Users\pquin>arp

Exibe e modifica as tabelas de conversão de endereços IP para endereços
físicos usadas pelo protocolo de resolução de endereços (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Exibe entradas ARP atuais interrogando os dados
                de protocolo atuais. Se inet_addr for especificado, somente
                os endereços IP e físicos do computador especificado serão
                exibidos. Se mais de uma interface de rede usar ARP, serão
                exibidas as entradas para cada tabela ARP.
  -g            O mesmo que -a.
  -v            Exibe as entradas ARP atuais no modo detalhado. Todas as
                entradas inválidas e entradas na interface de loopback
                serão mostradas.
```

Veja a ilustração seguinte que destaca o uso do comando ARP. Com o comando efetuado, verifique que é mostrado o endereço IP da máquina e seu respectivo endereço físico de placa de rede (endereço MAC).



Ping: o comando **ping** verifica se há conectividade entre os dispositivos.

Route: Route manipula as tabelas de roteamento (exibe e modifica a tabela do roteador). Busca traçar a rota e permite verificar qual o ponto, ao longo do caminho, que pode ter alguma retenção e interrupção da comunicação.

Netsh: o **netsh** ou **network shell** é um utilitário que **permite a configuração local ou remota dos parâmetros de rede**. Permite, por exemplo, exibir configuração atual de IP, exibir estado do adaptador sem fio etc.

Veja mais: https://br.ccm.net/faq/1319-comandos-ip-de-redes-no-windows

9. Velocidade de Conexão

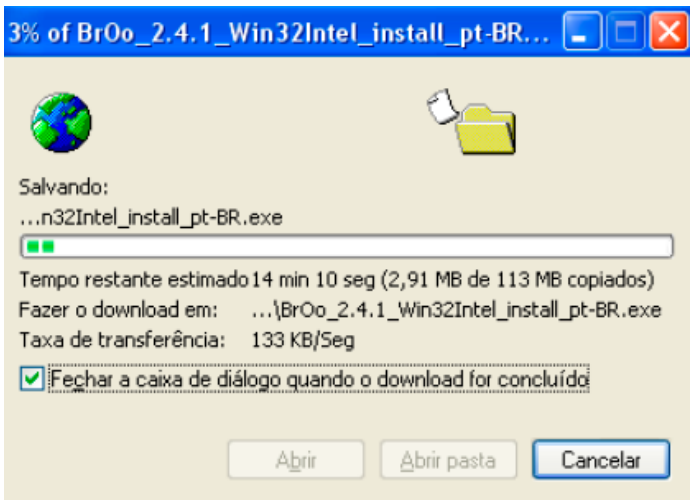
Representa a **quantidade de BITS** que trafega na rede a cada segundo, sendo medida em **bps (bits por segundo)**.

Antigamente as velocidades de conexão de dados eram muito baixas, temos como exemplo a discada, que transmitia dados na casa dos 56 Kbps ou 128 Kbps (kilobits por segundo). Hoje, podemos adquirir conexões que podem ser de 1, 2, 4, 10, 20, 200 Mbps (megabits por segundo) ou superior.

10. Taxa de Transferência

Representa a **quantidade de BYTES que é transferida a cada segundo.**

Quando estamos fazendo um download (baixando um arquivo) podemos verificar sua taxa de transferência e com base nela podemos naquele momento verificar a velocidade de conexão que temos.

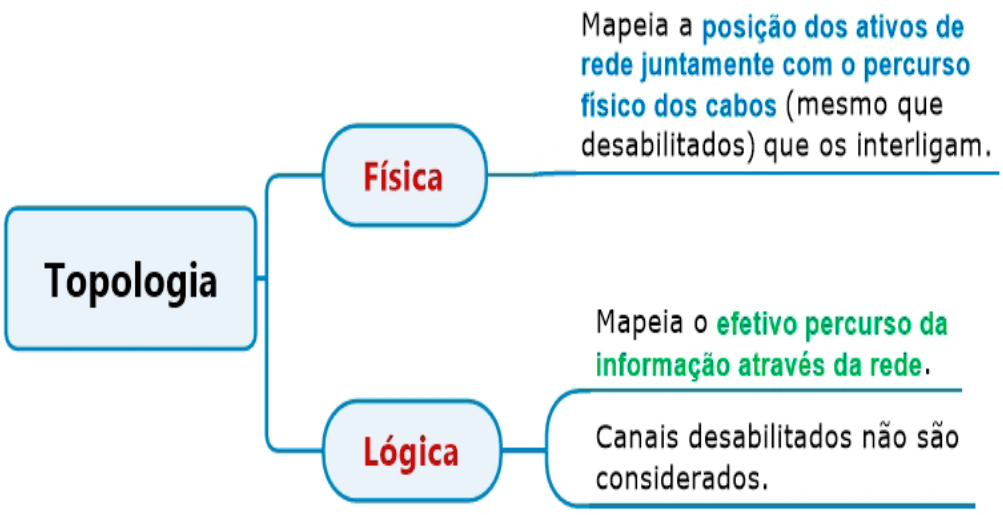


Pela figura, estou fazendo um download de um arquivo usando uma **taxa de transferência** de 133 KB/s (Kilobytes por segundo). Assim, para calcular minha **velocidade de conexão** desse momento basta pegar 133 x 8 = 1.064. Logo terei uma **velocidade de conexão** de 1.064 Kbps ou aproximadamente 1Mbps.

Para conexões a:	**O download será de:**
64Kbps (bits por segundo)	8 KBps (bytes por segundo)
128 Kbps	16 KBps
256 Kbps	32 KBps
512 Kbps	64 KBps

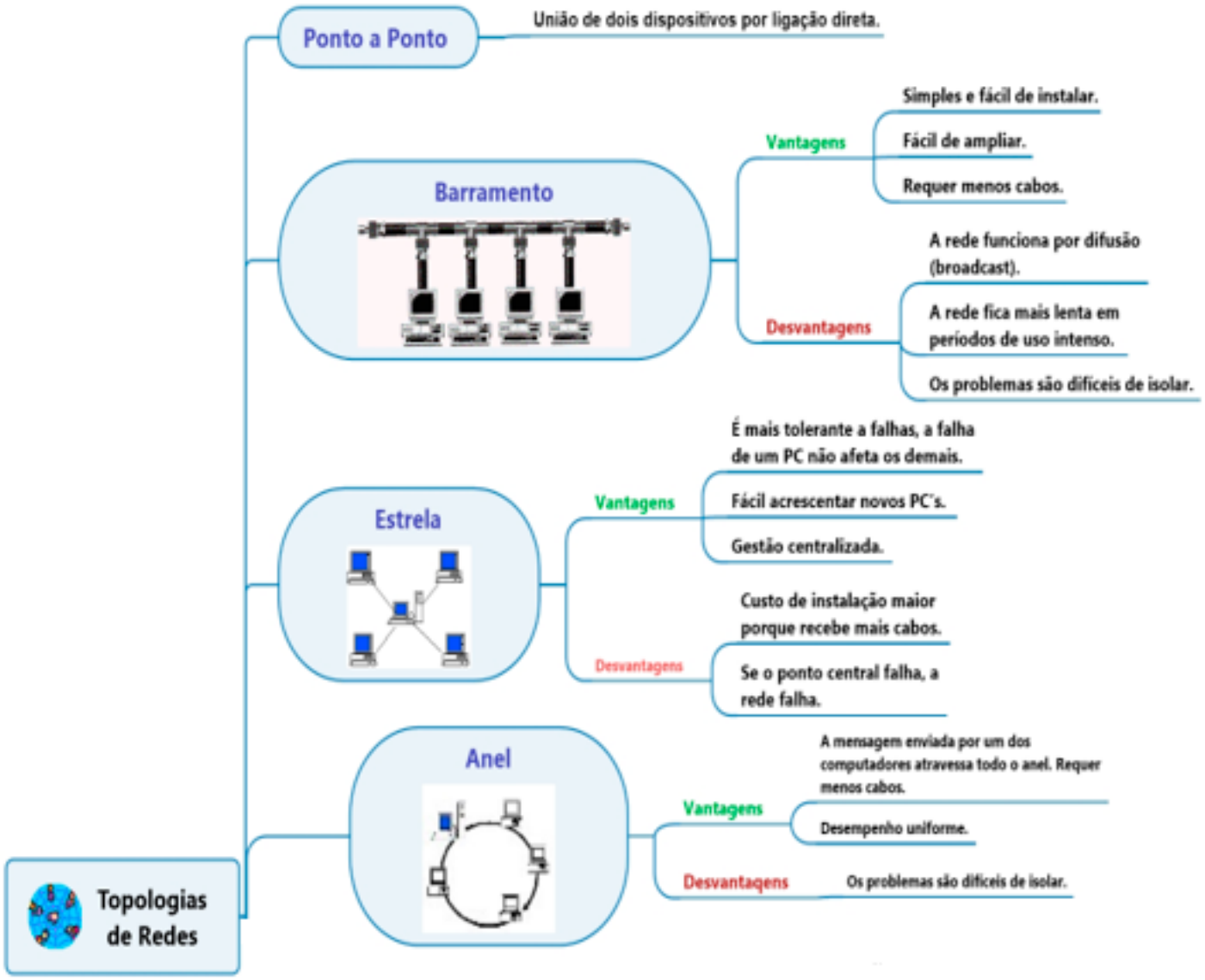
RESUMO

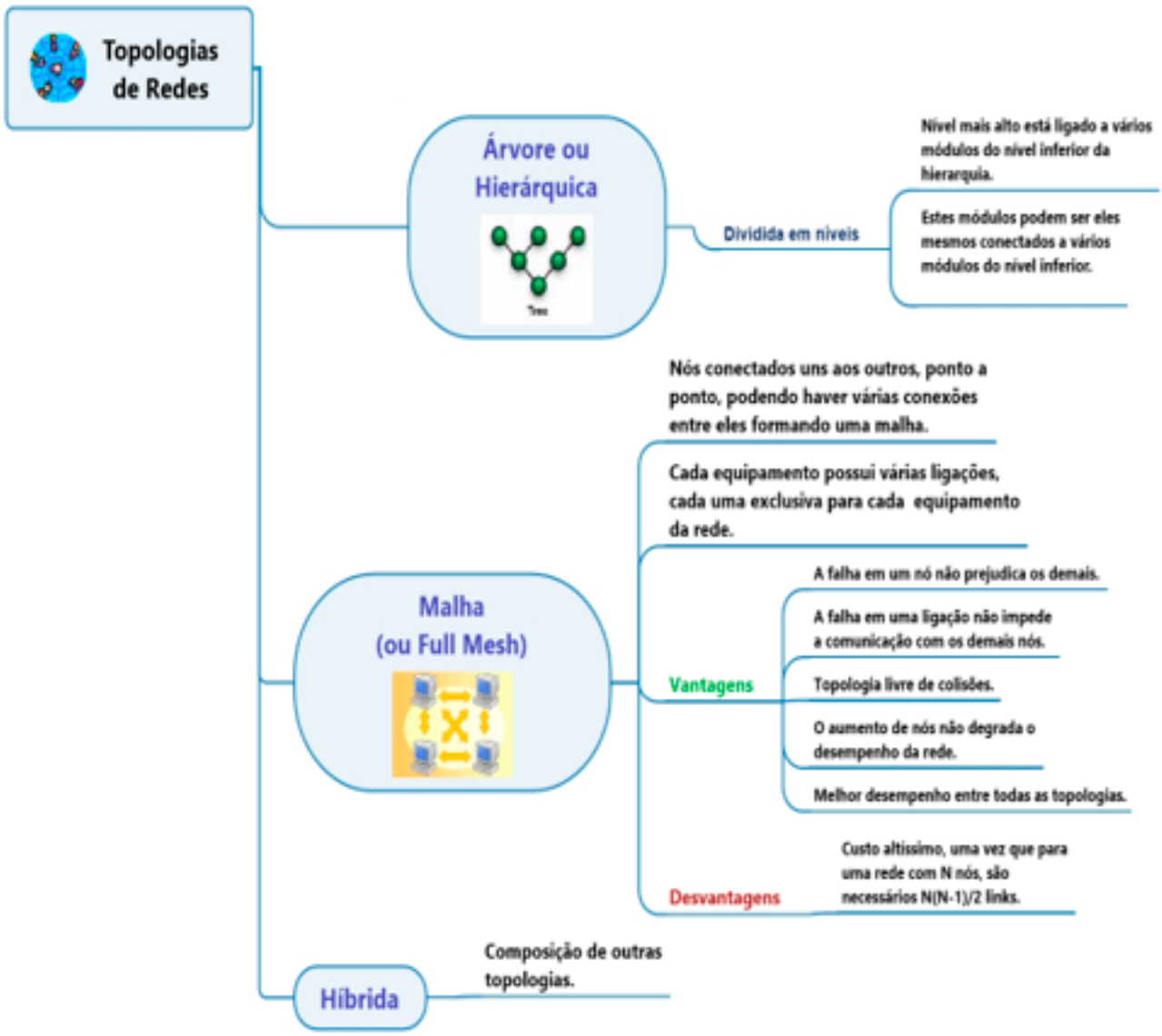
Topologias:



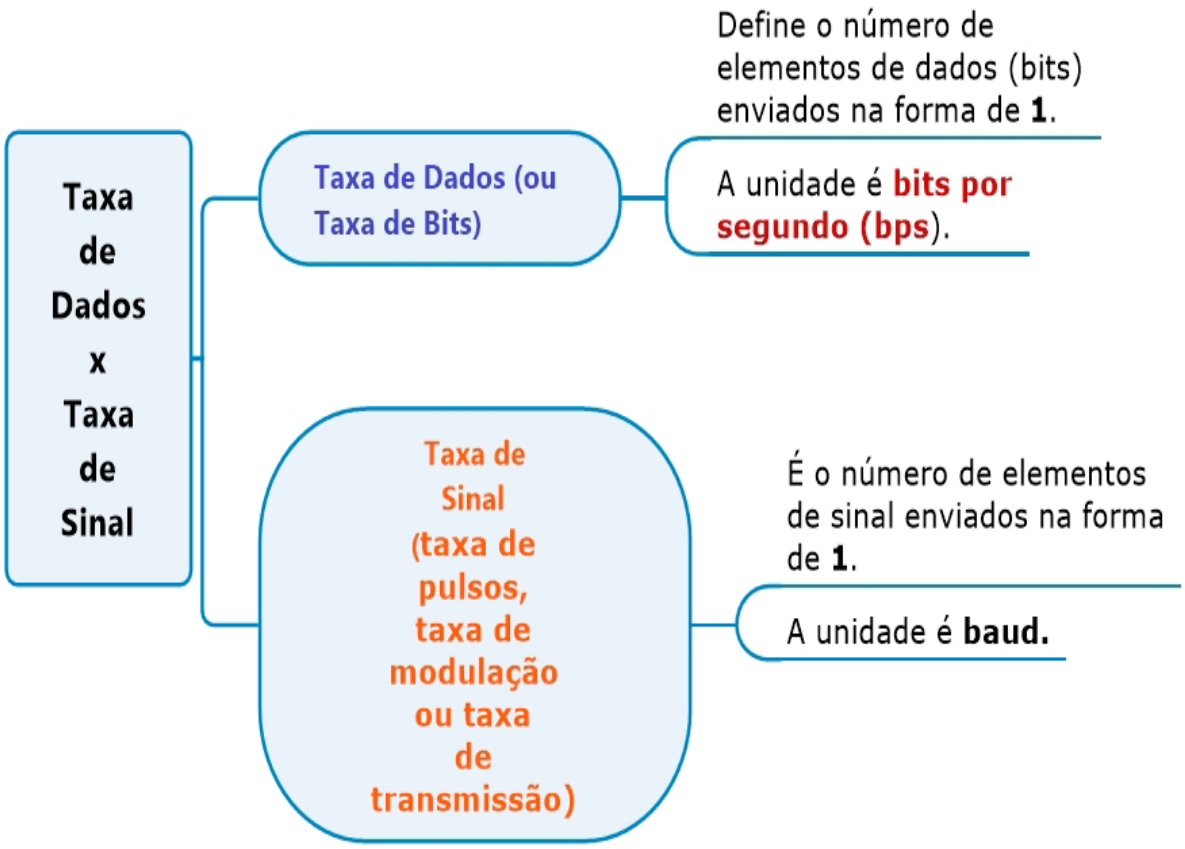
Atualmente, não se utiliza uma única topologia dentre as listadas. Utilizam-se **topologias híbridas**, ou seja, uma mistura de cada uma das topologias listadas de acordo com o custo ou a necessidade de desempenho de cada tipo.

Vamos a um quadro-resumo das topologias de redes mais comuns.





Fundamentos de Transmissão:



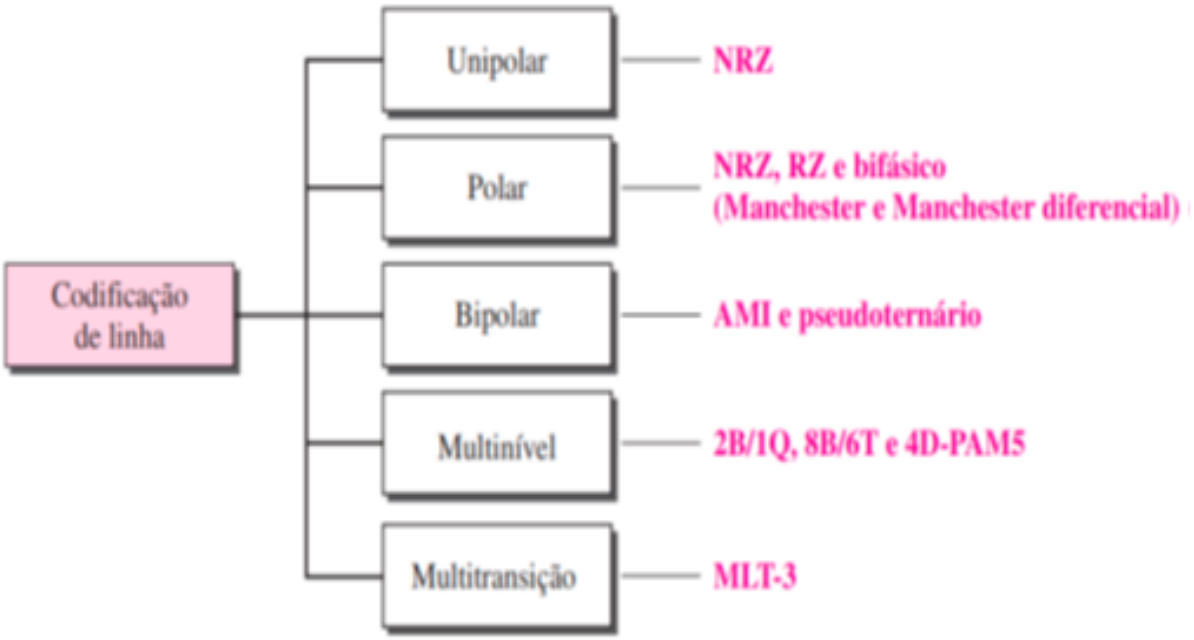
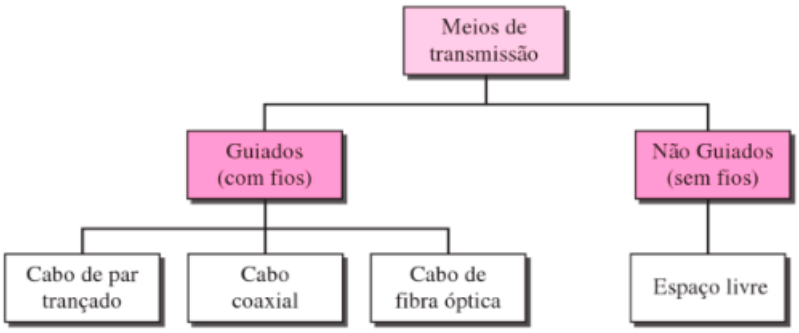


Figura. Codificação de linha, Fonte: Forouzan (2008, p. 106)

Meios de Transmissão:



Tipos de Cabo Coaxial:

- Thin –185m (Flexível) – Segmento – 10base2
- Thick – 500m (Rígido) – Backbone – 10base5

Tipos de Cabos de Par Trançado: os cabos de par trançado sem blindagem são chamados de **UTP** (Unshielded Twisted Pair - "cabo de par trançado sem blindagem").

Os **cabos blindados**, por sua vez, se dividem em três categorias:

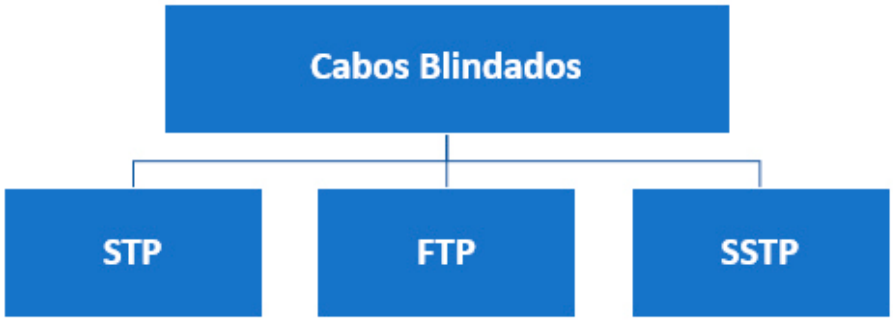
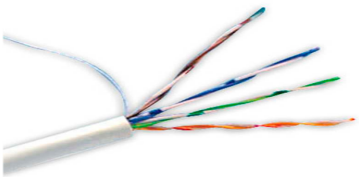


Figura. Cabos Blindados

Categorias de Cabo de Par Trançado:

Categoria	Frequência	Aplicações	Observações
Cat 3	16 MHz	10BASE-T / 100BASE-T4	Opera com taxa de até 16 Mbps. Utilizados em cabos de telefonia.
Cat 4	20 MHz	16 Mbps *Token Ring*	**Não** é mais utilizado.
Cat 5	**100 MHz**	100BASE-TX / **1000BASE-T**	Criados para redes **Fast Ethernet com taxa de 100 Mbps**. Suporta também *Gigabit Ethernet* com taxa de 1000 Mbps. (CAT5 não é mais recomendado pela TIA/EIA). 

Categoria	Frequência	Aplicações	Observações
Cat 5e	**100 MHz**	**1000BASE-T** / 2.5GBASE-T	**Cat 5 melhorado.** Ainda muito comum nas redes. 
Cat 6	250 MHz	**5GBASE-T / 10GBASE-T**	Desenvolvido para **redes Gigabit Ethernet**. **Limitado** a 55 metros em 10GBASE-T.
Cat 6a	500 MHz	**5GBASE-T / 10GBASE-T**	Cat 6 melhorado. Atinge 100 metros em 10GBASE-T. Para que os cabos CAT 6a sofressem menos interferências os pares de fios são separados uns dos outros, o que aumentou o seu tamanho e os tornou menos flexíveis.
Cat 7	600 MHz	**5GBASE-T / 10GBASE-T**	Criado para tráfego multimídia**. Possui isolamento contra interferências**. Pode suportar até 100 Gbps.
Cat 7a	1000 MHz	**5GBASE-T / 10GBASE-T**	Semelhante ao CAT 7. Assim como o CAT 7 utiliza conector diferente do *RJ*-45.
Cat 8/8.1/8.2	2000 MHz	**25GBASE-T / 40GBASE-T**	Suportam taxas de transmissão muito altas.

Fonte: https://techenter.com.br/cabos-de-par-trancado-categorias-e-tipos/.

Redes Sem Fio:

Padrão	Faixa de Frequência	Velocidade de Transmissão	Largura de Banda	Observação
802.11**b**	2,4 GHz	11 Mbps	20 MHz	O padrão mais antigo
802.11**g**	2,4 GHz (compatível com 802.11b)	54 Mbps	20 MHz	Atualmente, é o mais usado.

802.11**a**	5 GHz	54 Mbps	20 MHz	Pouco usado no Brasil. Devido à diferença de frequência, equipamentos desse padrão não conseguem se comunicar com os outros padrões citados.
802.11**n**	Utiliza tecnologia MIMO (*Multiple Input*/*Multiple Output*), frequências de 2,4 GHz e/ou 5 GHz (compatível portanto com 802.11b e 802.11g e teoricamente com 802.11a)	Diversos fluxos de transmissão: 2x2, 2x3, 3x3,4x4. Velocidade nominal subiu de 54 para **300 Mbps** (**600 Mbps** nos APs 4x4, capazes de transmitir 4 fluxos simultâneos.	20 MHz ou 40 MHz	Padrão recente e que está fazendo grande sucesso. Este padrão pode chegar **até os 600 Mbps**, quando operando com **4 antenas** no transmissor e no receptor, e utilizando a modulação **64-QAM** (Quadrature Amplitude Modulation).

A literatura já cita um novo padrão a caminho, o **802.11ac**, prometendo velocidades em torno de 1Gbps, largura de banda de 160MHz e multi-user MIMO.

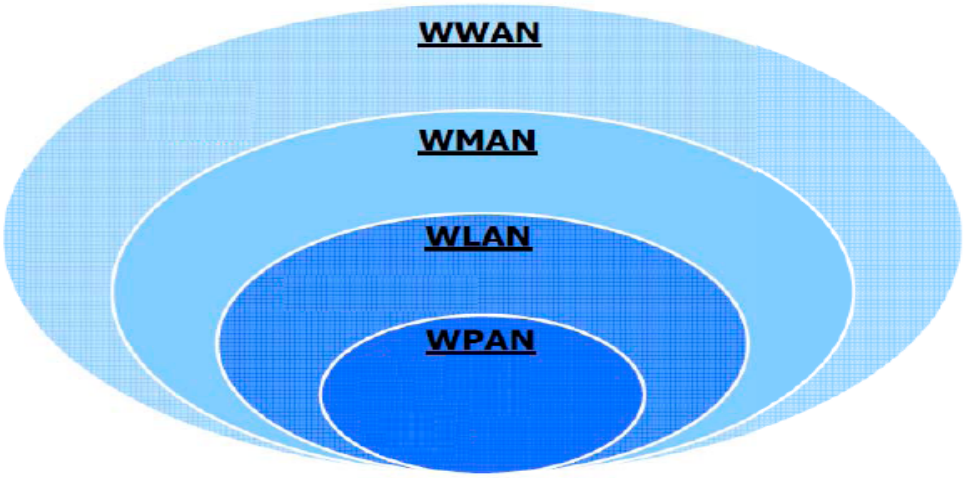


Figura. Redes Wireless

As normas IEEE 802 são subdivididas em diversos padrões:

802.2	**LLC (Logical Link Control).**	
802.3	**-802.3 – Ethernet e especifica a sintaxe e a semântica MAC (Media Access Control). -802.3u - Fast Ethernet. -802.3z - Gigabit Ethernet. -802.3ae - 10 Gigabit Ethernet.**	
IEEE 802.5	**Token Ring (inativo).**	
IEEE 802.8	**Fibra óptica.**	
IEEE 802.11 (a/b/g/n)	**Wi-fi - Redes Wireless.**	
IEEE 802.15	**Wireless Personal Area Network (Bluetooth).**	
IEEE 802.16	**Broadband Wireless Access (Wimax).**	

Padrão de Arquitetura	**Velocidade do Adaptador (Placa) de Rede**
Ethernet-padrão	**10 Mbps**
Fast Ethernet	**100 Mbps**
Gigabit Ethernet	**1000 Mbps = 1 Gbps**
10 Gigabit Ethernet	**10.000 Mbps = 10 Gbps**

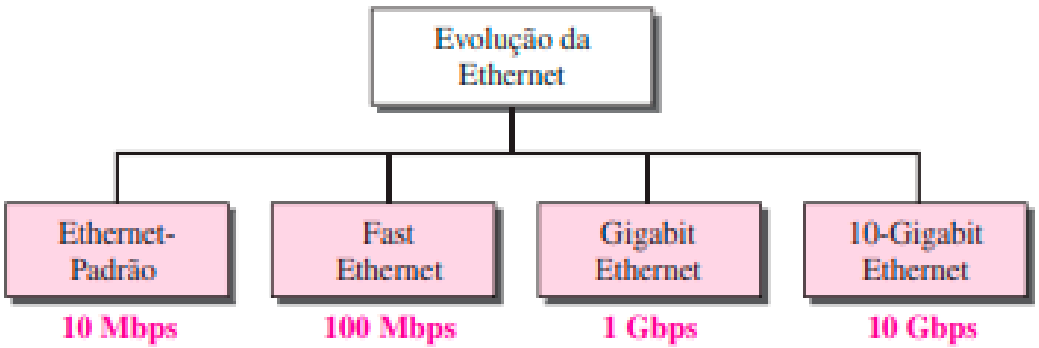
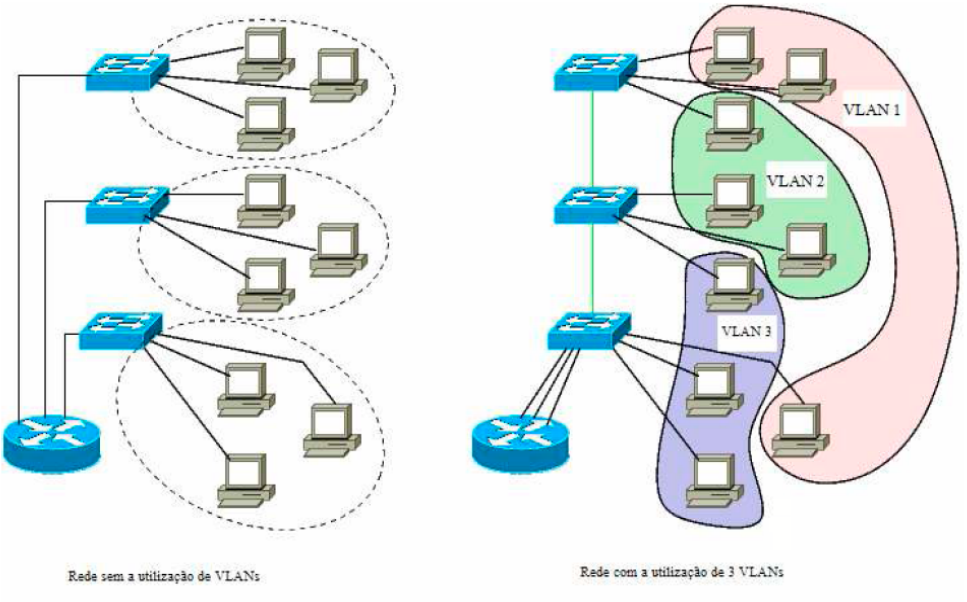


Figura. Evolução da Ethernet ao longo de quatro gerações
Fonte: Forouzan (2008, p. 398)

VLAN: a **rede local virtual (VLAN)** é uma rede de computadores que se comporta como se estivessem conectados ao mesmo segmento de rede embora possam estar fisicamente localizados em segmentos diferentes da LAN. As VLANS são configuradas por software no switch e no roteador (CISCO, 2010).

Exemplo:



Rede sem a utilização de VLANs

Rede com a utilização de 3 VLANs

Detalhes sobre o 1º octeto das classes:

Classe	*1.º octeto começa com (em binário)*	*1.º octeto pode ser (em decimal)*	*Objetivo*	*Exemplo de Endereço IP*
A	0	1 a 126	Grandes redes	**100**.1.240.28
B	10	128 a 191	Médias redes	**157**.100.5.195
C	110	192 a 223	Pequenas redes	**205**.35.4.120
D	1110	224 a 239	*Multicasting.*	Não usado para micros (*hosts*) individuais.
E	1111	240 a 254	Faixa reservada para fins futuros.	-

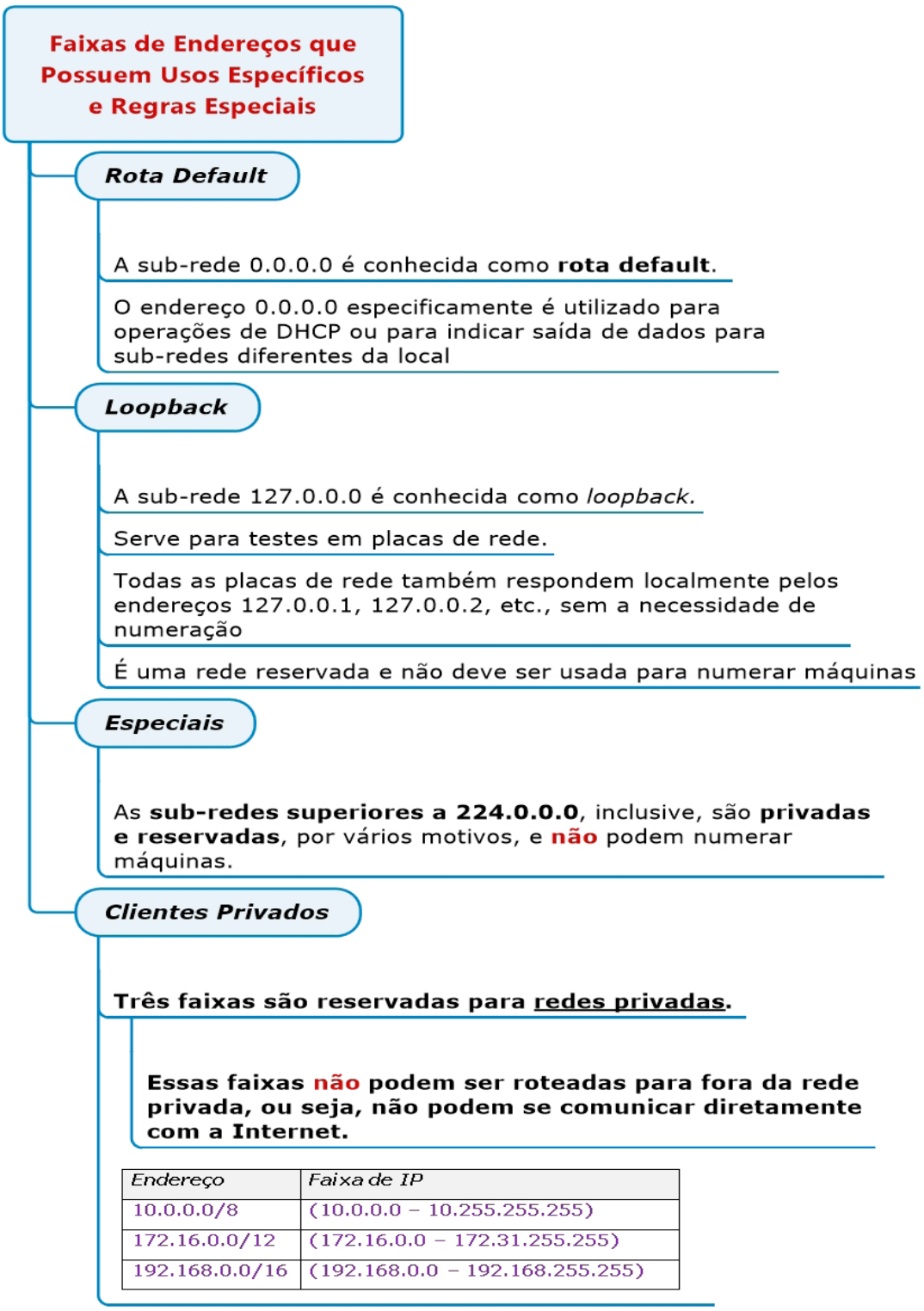


Figura. Faixas de Endereços que Possuem Usos Específicos.
Fonte: Quintão (2020)

QUESTÕES DE CONCURSO

Questão 1 (CESPE/MPC-PA/ASSISTENTE MINISTERIAL DE INFORMÁTICA/2019) Considere que quatro empresas distintas, localizadas em países e continentes diferentes, tenham de acessar e compartilhar dados entre si. Essa demanda pode ser atendida mediante a elaboração de projeto em que se conste a implementação de uma rede

a) VoIP (voice over IP).

b) PGP (Pretty Good Privacy).

c) LAN (local area network).

d) SSL (secure sockets layer).

e) WAN (wide area network).

Questão 2 (CESPE/STJ/TÉCNICO JUDICIÁRIO/ DESENVOLVIMENTO DE SISTEMAS/2018) Devido à sua estrutura, em uma rede usando a topologia estrela, o isolamento de falhas é uma tarefa complexa, o que representa uma desvantagem dessa topologia.

Questão 3 (CESPE/STJ/TÉCNICO JUDICIÁRIO/ DESENVOLVIMENTO DE SISTEMAS/2018) A rede mostrada na figura a seguir, em que as linhas representam conexões entre computadores, apresenta topologia mesh.

Questão 4 (CESPE/ABIN/OFICIAL TÉCNICO DE DE INTELIGÊNCIA/2018) Na topologia em anel, cada bite se propaga de modo independente, sem esperar pelo restante do pacote ao qual pertence, sendo possível que um bite percorra todo o anel enquanto outros bites são enviados ou, muitas vezes, até mesmo antes de o pacote ter sido inteiramente transmitido.

Questão 5 (CESPE/ABIN/OFICIAL TÉCNICO DE INTELIGÊNCIA/2018) Nas redes locais de difusão do tipo anel, há necessidade de se definir alguma regra para arbitrar os acessos simultâneos ao enlace.

Questão 6 (CESPE/POLÍCIA FEDERAL/AGENTE DE POLÍCIA FEDERAL/2018) Marta utiliza uma estação de trabalho que executa o sistema operacional Windows 10 e está conectada à rede local da empresa em que ela trabalha. Ela acessa usualmente os sítios da intranet da empresa e também sítios da Internet pública. Após navegar por vários sítios, Marta verificou o histórico de navegação e identificou que um dos sítios acessados com sucesso por meio do protocolo HTTP tinha o endereço 172.20.1.1.

Tendo como referência essa situação hipotética, julgue o item a seguir.

O endereço 172.20.1.1 identificado por Marta é o endereço IPv4 de um servidor *web* na Internet pública.

Questão 7 (CESPE/SEFAZ-RS/TÉCNICO/ADAPTADA/2018) Para a interligação dos dispositivos em uma rede de comunicação, deverá ser utilizado um cabo com blindagem de isolamento, com capacidade de tráfego de dados de até 10 Gb e que permita o menor índice possível de interferências. Nesse caso, será correto utilizar o cabo categoria

a) 1.

b) 3.

c) 5.

d) 5a.

e) 7.

Questão 8 (CESPE/ABIN/OFICIAL TÉCNICO DE INTELIGÊNCIA - ÁREA 6/2018) Com relação às tecnologias para construir um sistema de comunicação para transmitir um sinal de informação, julgue o item consecutivo.

Ainda que se escolha a fibra óptica como meio de transmissão do sinal de informação, o sistema não será robusto à interferência eletromagnética de outros sistemas de radiofrequência que operem na região.

Questão 9 (FCC/NOSSA CAIXA/ANALISTA DE SISTEMAS/2011) Em relação à topologia de redes, considere:

I – Numa sala de espera anuncia-se a senha de número 45. Todas as pessoas escutam, mas somente o portador desta senha dirige-se ao balcão de atendimento.

II – Numa sala de reunião, a lista de presença é passada de mão em mão. Cada um dos presentes preenche seus dados e a repassa ao vizinho, até que a lista seja preenchida por todos.

Analogamente, os casos I e II estão associados, respectivamente, às características de funcionamento das topologias:

a) anel e estrela;

b) estrela e árvore;

c) barramento e estrela;

d) anel e árvore;

e) barramento e anel.

Questão 10 (CESPE/EBSERH/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/2018) Acerca de infraestrutura de TI, julgue o item subsequente.

Uma rede sem fio que utiliza o padrão IEEE 802.11n tem, em ambiente sem obstáculos físicos, alta capacidade de transmissão de dados, sendo capaz de atingir até 1 Gbps, usando até 5 antenas em um único *access point*.

Questão 11 (CESPE/STJ/ TÉCNICO JUDICIÁRIO/SUPORTE TÉCNICO/2018) Acerca de topologias e equipamentos de rede, julgue o item seguinte.

Em uma rede local sem fio que utilize equipamentos de access point operando no padrão IEEE 802.11b, o tráfego de dados pode atingir velocidade de até 54 Mbps.

Questão 12 (CESPE/TELEBRAS/NÍVEL MÉDIO/CONHECIMENTOS BÁSICOS/2013) Os pacotes são unidades maiores de informação que contêm uma mensagem inteira encapsulada, que é transmitida entre computadores de uma rede, os quais alocam integralmente os recursos de transmissão enquanto as mensagens estão sendo transmitidas.

Questão 13 (CESPE/ANEEL/TODOS OS CARGOS/2010) FTP é um protocolo de comunicação que permite o envio de arquivos anexos a mensagens de correio eletrônico, sem a necessidade de compactar esses arquivos.

Questão 14 (CESPE/IPEA/ANALISTA BD/2008) Os protocolos de comunicação podem ser organizados em hierarquias compostas por camadas, em que cada camada oferece serviços para a camada acima. A um conjunto de camadas, pode ser dado o nome de pilha de protocolos. Em uma pilha, tipicamente, a camada mais inferior é a física e uma camada intermediária é a de transporte, que fornece um serviço de comunicação entre pares de portas ligadas a processos.

Questão 15 (CESPE/STF/2008) O UDP é um protocolo de transporte que não estabelece conexões antes de enviar dados, não envia mensagens de reconhecimento ao receber dados, não controla congestionamento, garante que dados sejam recebidos na ordem em que foram enviados e detecta mensagens perdidas.

Questão 16 (CESPE/SERPRO/ANALISTA/REDES DE COMPUTADORES/2005) Entre as pilhas de protocolos mais usadas na atualidade, encontra-se o TCP/IP, que tem entre os seus protocolos principais o IP, serviço de datagramas, e o TCP, serviço de transporte confiável.

Questão 17 (CESPE/MPU/TÉCNICO TI/2010) Um computador que tem conectado nele uma impressora compartilhada com a rede pode ser adequadamente configurado em um servidor DHCP como se fosse um equipamento com um endereço IP fixo.

Questão 18 (CESPE/IJSN-ES/2010) A respeito dos sistemas, das tecnologias e dos protocolos de redes sem fio, julgue os itens que se seguem.

A conexão de um cliente que usa o padrão IEEE 802.11b a um ponto de acesso que usa o padrão IEEE 802.11g pode proporcionar ao cliente um desempenho com maior velocidade].

Questão 19 (CESPE/TCE-RN/2009) A taxa máxima de transmissão de dados no padrão IEEE 802.11b é de 54 Mbps e o acesso ao meio é do tipo CSMA/CD.

Questão 20 (CESPE/IJSN-ES/2010) Considere dois hosts A e B que estejam conectados a um switch. Nessa situação, se o host A enviar um frame em broadcast e o host B não receber esse frame, então é correto inferir que os hosts A e B pertencem a VLANS diferentes.

Questão 21 (CESPE/TCU/2009) Com relação às tecnologias de redes locais, julgue os itens a seguir. [A interconexão de redes CSMA/CD, como Ethernet e IEEE 802.3, utilizando bridges ou switches, agrega os domínios de broadcast das redes, porém preserva seus domínios de colisão].

Questão 22 (CESPE/MPOG/PROCESSO SELETIVO INTERNO PARA GRATIFICAÇÕES DO GSISP – NÍVEL SUPERIOR/2009) Os roteadores atuam no nível de datagrama, levando em consideração as informações de endereço físico de destino para decidir para que interface encaminhar o pacote.

Questão 23 (CESPE/MPOG/PROCESSO SELETIVO INTERNO PARA GRATIFICAÇÕES DO GSISP/NÍVEL SUPERIOR/2009) Quanto aos elementos ativos de infraestrutura e serviços de redes de comunicação, julgue os itens subsequentes. [Roteadores são exemplos de gateways que tipicamente interconectam redes de diferentes topologias de enlace, encaminhando datagramas a partir das informações do protocolo de rede].

Questão 24 (FCC/MANAUSPREV/ANALISTA PREVIDENCIÁRIO/ TECNOLOGIA DA INFORMAÇÃO/2015) Wi-Fi é um conjunto de especificações para redes locais sem fio (Wireless Local Area Network – WLAN) que são conhecidas como redes no padrão IEEE

a) 802.2.

b) 802.11.

c) 802.8.

d) 802.16.

e) 802.15.

Questão 25 (FCC/TRE-RR/TÉCNICO DO JUDICIÁRIO/OPERAÇÃO DE COMPUTADORES/2015) A rede Wi-Fi está em conformidade com a família de protocolos 802.11 do IEEE. Dentro desta família de protocolos, o que pode atingir taxas de transmissão de até 54 Mbit/s e opera na frequência de 2.4 GHz é o padrão

a) 802.11a.

b) 802.11h.

c) 802.11g.

d) 802.11ac.

e) 802.11b.

Questão 26 (FCC/TRT-15ª/CAMPINAS/TÉCNICO JUDICIÁRIO/TI/2015) Atualmente, o mercado oferece dispositivos para acesso à rede sem fio nas diversas versões do padrão IEEE 802.11. Caso a versão 802.11g seja escolhida para implementar uma WLAN, o esquema de segurança a ser escolhido deve ser o

a) WPA2, pois utiliza o AES que é o mais seguro atualmente.

b) WEP, pois utiliza o esquema de chave dinâmica de 64 bits, sendo simples e seguro.

c) WPA, pois é mais simples e seguro que o WPA2.

d) WPA2, pois utiliza o TKIP que é o mais seguro atualmente.

e) WPA, pois utiliza o esquema de chave fixa de 128 bits que não pode ser quebrada.

Questão 27 (FCC/CNMP/ANALISTA DO CNMP/SUPORTE E INFRAESTRUTURA/2015) A escolha do tipo de proteção em uma rede sem fio é uma etapa importante na sua configuração. Uma forma de proteção muito utilizada é a chave de rede

a) que consiste na autorização de acesso à rede apenas a computadores cujos endereços MAC foram emitidos após 2005, ano após o qual um padrão seguro de acesso a redes sem fio foi incorporado.

b) sendo que a do tipo WEP é a mais indicada, pois até hoje nenhum programa conseguiu quebrá-la.

c) sendo que a do tipo WPA é muito utilizada por se basear em encriptação de 16 *bits*.

d) que consiste em uma senha que o usuário deve digitar para acessar a rede sem fio.

e) que consiste na autorização de acesso à rede apenas a computadores cujos endereços MAC foram cadastrados para realizar esse acesso.

Questão 28 (FCC/AL-PE/ANALISTA LEGISLATIVO/ INFRAESTRUTURA/2014) As redes sem fio (WiFi) apresentam características especiais de vulnerabilidade para as empresas, em função do sinal da rede poder ser capturado por dispositivos que possuam interface para redes sem fio, sendo esses equipamentos pertencentes à rede corporativa ou não. Para implantar a segurança nas redes sem fio de uma empresa, a equipe de TI deve aplicar o

a) protocolo WEP (Wired Equivalent Privacy) que possibilita a implementação de criptografia no meio WiFi, o qual não está sujeito a reinjeção de pacotes que levam à negação de serviços ou degradação do desempenho da rede.

b) protocolo WPA (Wi-Fi Protected Access) que possibilita a implementação de rede Ad-Hoc, não dependendo da centralização da comunicação em equipamentos de acesso WiFi.

c) WPA Corporativo, o qual tratará toda autenticação na rede através de um servidor de autenticação que se comunica com o AP (access point) do equipamento sem fio do usuário.

d) TKIP (Temporal Key Integrity Protocol) que é implementado no protocolo WEP e é baseado no conceito de chaves estáticas, ou seja, a chave não é substituída dinamicamente.

e) WPA2 que implementa criptografia com chave de encriptação de 64 bits.

Questão 29 (FCC/TJ-PE/ANALISTA JUDICIÁRIO/ANALISTA DE SUPORTE/2012) É um tipo de rede em que a topologia pode se alterar o tempo todo e, consequentemente, até mesmo a validade dos caminhos podem se alterar de modo espontâneo, sem qualquer aviso:

a) Ad Hoc.

b) *Full-meshed*.

c) Hub-and-spoke.

d) WWAN.

e) WMAN.

Questão 30 (FCC/TRT-23ª/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2011) Para tornar confidenciais as mensagens nas redes de comunicação sem fio, os protocolos WEP, WPA e WPA2 se baseiam, respectivamente, entre outros componentes, no algoritmo de criptografia:

a) RC4, RC4 e AES.

b) RC4, RC4 e RC4.

c) AES, AES e RC4.

d) AES, AES e AES.

e) RC4, AES e AES.

Questão 31 (FCC/INFRAERO/ANALISTA SUPERIOR III SEGURANÇA DA INFORMAÇÃO/2011) Representam fragilidades de segurança em redes sem fio, EXCETO:

a) A maioria dos concentradores vem com serviço SNMP habilitado, e isso pode ser usado por um atacante, pois revela uma vasta gama de informações sobre a rede em questão.

b) A maioria dos equipamentos saem de fábrica com senhas de administração e endereço IP padrão. Caso estes não sejam trocados, poderão permitir a um atacante que se utilize delas em uma rede-alvo.

c) A alta potência dos equipamentos pode permitir que um atacante munido de uma interface de maior potência receba o sinal a uma distância não prevista pelos testes.

d) O posicionamento de determinados componentes de rede pode comprometer o bom funcionamento da rede e facilitar o acesso não autorizado e outros tipos de ataque.

e) Os métodos de segurança WEP são completamente vulneráveis por possuírem chaves WEP pré-configuradas que não podem ser modificadas.

Questão 32 (FCC/TRT-9/ANALISTA JUDICIÁRIO/TI/2010) O primeiro protocolo de criptografia disponível para redes Wi-Fi é baseado em um algoritmo chamado

a) RC4, que é um codificador de fluxo.

b) RSA, que é um decodificador de chave pública.

c) WAP, que é um protetor de arquivos transmitidos.

d) NAT, que é um decodificador de fluxos.

e) WPA, que é um protetor de arquivos transmitidos.

Questão 33 (FCC/AL-SP/AGENTE TÉCNICO LEGISLATIVO/SEGURANÇA DE REDES/2010) Com relação à robustez do método criptográfico utilizado, a ordem do protocolo mais vulnerável para o menos vulnerável é

a) TKIP, WPA e WEP.

b) WPA, TKIP e WEP.

c) TKIP, WEP e WPA.

d) WEP, TKIP e WPA.

e) WEP, WPA e TKIP.

Questão 34 (IADES/CONAB/TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO/NÍVEL MÉDIO/2014) Qual padrão IEE 802 é responsável pela tecnologia sem fio para comunicação pessoal (WPAN) e possibilita comunicações com distâncias de 1, 10 e até 100 metros, dependendo da potência de transmissão?

a) Bluetooth (802.15).

b) Wi-Fi (802.11).

c) WiMax (802.16)

d) Wireless (802.18).

e) WiMobily (802.20).

Questão 35 (IADES/EBSERH/ANALISTA DE TI/SUPORTE E REDES/SUPERIOR/2014) Assinale a alternativa que indica o padrão IEEE que regulamenta o uso de redes wireless com largura de banda de no máximo 54 Mbps operando na frequência de 5 GHz.

a) 802.11

b) 802.11a

c) 802.11b

d) 802.11g

e) 802.15

Questão 36 (FCC/TRT-16ª REGIÃO/MA/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2014) Atenção: Para responder às questões de números 51 a 53, considere o texto abaixo.

Um Analista de Redes de Computadores deve planejar a instalação física e a configuração lógica de uma rede local de computadores do ambiente de escritório do Tribunal Regional do Trabalho da 16ªRegião. Dentre as especificações recebidas, estão: a área total do escritório é de 200 m^2, a rede deve interligar 30 computadores, o uso dos computadores é para aplicativos típicos de escritório e TRT da 16ª Região contratou o serviço de acesso (provedor) para 100 Mbps.

A partir dessa especificação, o Analista escolheu o cabo de pares trançados para realizar as conexões na rede local. Face à variedade de categorias atualmente existentes para esse tipo de cabo, para essa instalação o Analista deve escolher o cabo

a) CAT3 que permite uma taxa de dados de até 100 Mbps e alcança 50 m.

b) CAT5 que permite uma taxa de dados de até 100 Mbps e alcança até 100m.

c) CAT5 que permite uma taxa de dados de até 100 Mbps e alcança até 200 m.

d) CAT6 que permite uma taxa de dados de até 200 Mbps e alcança 1.000 m.

e) CAT6 que permite uma taxa de dados de até 10.000 Mbps e alcança 1.000 m.

Questão 37 (FCC/SABESP/TÉCNICO EM SISTEMAS DE SANEAMENTO 01/ELETRÔNICA/2018) Com relação ao protocolo IP, é correto afirmar:

a) Todos os computadores de uma determinada rede têm o mesmo número de IP.

b) O número IPv4 é formado por 128 bits.

c) Geralmente os dois primeiros bytes do IP representam o número da rede e os dois últimos o número da placa de rede.

d) Para formação do endereço de IPv4 todas combinações são possíveis, não havendo números de IP inválidos.

e) Se o valor do primeiro byte for um número entre 128 e 191, então temos um endereço de IP classe B para o IPv4.

Questão 38 (FCC/TRT-16ª REGIÃO/MA/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2014) Atenção: Para responder às questões de números 51 a 53, considere o texto seguinte.

Um Analista de Redes de Computadores deve planejar a instalação física e a configuração lógica de uma rede local de computadores do ambiente de escritório do Tribunal Regional do Trabalho da 16ªRegião. Dentre as especificações recebidas, estão: a área total do escritório é de 200 m^2, a rede deve interligar 30 computadores, o uso dos computadores é para aplicativos típicos de escritório e TRT da 16ª Região contratou o serviço de acesso (provedor) para 100 Mbps.

Após a finalização das escolhas do cabeamento e dos equipamentos, o Analista decidiu configurar logicamente a rede utilizando o conceito de sub-rede na rede local e otimizar o seu desempenho. Para que a sub-rede criada acomode todos os 30 computadores, a máscara de sub-rede utilizada deve ser:

a) 255.255.255.252

b) 255.255.255.240

c) 255.255.255.224

d) 255.255.255.192

e) 255.255.255.255

Questão 39 (FCC/AL-PE/ANALISTA LEGISLATIVO/INFRAESTRUTURA/2014) Uma indústria está mudando a sua sede para um novo local com 360.000 m2. No novo local, planeja-se que o data center seja instalado em um prédio diferente daquele onde estarão os usuários. O data center estará a 540 metros de distância do escritório da empresa, onde estarão as estações dos usuários (desktops e notebooks). Todos os equipamentos servidores, estações e periféricos que serão conectados na rede terão interface física de rede com conector RJ45 e capacidade de transmissão com negociação automática 10/100 Mbps. Os switches e roteadores da rede que tratarão a comunicação entre os nós da LAN poderão ser ligados ao backbone da rede com portas físicas com conector ST e capacidade de transmissão de 1 Gbps. A rede não contará com repetidores. Nesse projeto, deve ser adotado cabeamento

a) coaxial entre os roteadores do data center e os roteadores do escritório e cabeamento em fibra ótica entre os switches e as estações.

b) com par trançado CAT5 entre os roteadores do data center e os roteadores do escritório e cabeamento em fibra ótica entre os switches e as estações.

c) em fibra ótica entre os roteadores do data center e os roteadores do escritório e cabeamento coaxial entre os switches e as estações.

d) em fibra ótica entre os roteadores do data center e os roteadores do escritório e cabeamento em par trançado CAT5 entre os switches e as estações.

e) em par trançado CAT 5 entre os roteadores do data center e os roteadores do escritório e cabeamento em par trançado CAT 1 entre os switches e as estações.

Questão 40 (FCC/TRT-1R/ANALISTA JUDICIÁRIO/ÁREA JUDICIÁRIA/2013) A placa de rede do computador de Paulo tem velocidade de transmissão de 10/100. Isso significa que a transmissão de dados pela rede entre o computador de Paulo e um computador servidor com placa de rede de mesma velocidade pode ser de até

a)10 megabytes por segundo.

b)100 megabits por minuto.

c)1000 megabits por segundo.

d)100 megabits por segundo.

e)100 megabytes por segundo.

Questão 41 (FCC/TRE-RN/TÉCNICO JUDICIÁRIO/OPERAÇÃO DE COMPUTADOR/2005) No TCP/IP, o endereço IP 172.20.35.36 enquadra-se na classe:

a) A;

b) B;

c) C;

d) D;

e) E.

Questão 42 (FCC/CEAL/ANALISTA DE SISTEMAS/2005) Na arquitetura TCP/IP:

a) o IP 127.0.0.1 é utilizado para representar máquinas de toda a rede;

b) o IP 10.0.0.1 enquadra-se no padrão classe B;

c) a máscara de rede FFFFFF00 é típica do padrão classe C;

d) o serviço UDP é orientado à conexão;

e) a aplicação FTP também é conhecida pelo nome de Terminal Virtual Remoto.

Questão 43 (FCC/SABESP/ANALISTA DE GESTÃO/ADMINISTRAÇÃO/2018) Um funcionário está usando um computador com o sistema operacional Windows 8, em português, e deseja saber o endereço IP de sua máquina. Para isso, ele deve abrir uma janela de execução do Windows:

a) clicando no botão Iniciar, digitar run seguido de ENTER e, na janela aberta, digitar ipshow seguido de ENTER. O mesmo procedimento é válido no Windows 10

b) clicando no botão Iniciar, digitar cmd seguido de ENTER e, na janela aberta, digitar ipconfig seguido de ENTER. O mesmo procedimento não é válido no Windows 7.

c) pressionando a Tecla do Windows, digitar ipshow -all seguido de ENTER. O mesmo procedimento é válido no Windows 10.

d) utilizando o atalho Tecla do Windows + R, digitar cmd seguido de ENTER e, na janela aberta, digitar ipconfig -all seguido de ENTER. O mesmo procedimento é válido no Windows 7.

e) utilizando o atalho Tecla do Windows + E, digitar run seguido de ENTER e, na janela aberta, digitar ipconfig -all seguido de ENTER. O mesmo procedimento não é válido no Windows 7.

Questão 44 (FCC/SABESP/TÉCNICO EM SISTEMAS DE SANEAMENTO 01 – ELETRÔNICA/2018)

O comando do prompt do windows que exibe e modifica as tabelas de conversão de endereços IP para endereços físicos usadas pelo protocolo de resolução de endereços é:

a) Ping

b) Ipconfig

c) Route

d) Arp

e) Netsh

Questão 45 (FCC/SABESP/TÉCNICO EM SISTEMAS DE SANEAMENTO 01/ELETRÔNICA/2018) O cabo UTP para redes 100BASE-TX e 1000BASE-T que suportam frequências de até 100 MHz é classificado como categoria

a) 3.

b) 1.

c) 2.

d) 4.

e) 5e.

Questão 46 (FCC/CÂMARA DOS DEPUTADOS/ANALISTA DE INFORMÁTICA LEGISLATIVA/2007) O padrão de velocidade e cabeamento 1000Base-T caracteriza uma tecnologia de interconexão para redes locais denominada

a) 10Mbit/s Ethernet.

b) 10-Gigabit Ethernet.

c) Gigabit Ethernet.

d) Wireless Ethernet.

e) Fast Ethernet.

Questão 47 (FCC/TRT-9ª REGIÃO/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2010) O cabo par trançado tradicional de categoria 5 é composto de

a) um par de fios.

b) dois pares de fios.

c) três pares de fios.

d) quatro pares de fios.

e) cinco pares de fios.

Questão 48 (FCC/TRT-9ª REGIÃO/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2010) Quanto ao tipo de rede, considere:

I – Ethernet Padrão (10 Mbps).

II – Gigabit Ethernet (1 Gbps).

III – Fast Ethernet (100 Mbps).

IV – 10G Ethernet (10 Gbps).

Com referência ao cabo par trançado, considere:

1) um par de fios.
2) dois pares de fios.
3) três pares de fios.
4) quatro pares de fios.
5) cinco pares de fios.

Quanto ao uso da quantidade de par de fios do cabo na rede, é correta a associação

a) I-1, II-2, III-3 e IV-4.

b) I-2, II-3, III-4 e IV-5.

c) I-2, II-4, III-2 e IV-4.

d) I-3, II-3, III-4 e IV-4.

e) I-3, II-4, III-4 e IV-5.

Questão 49 (FCC/TRT-MG/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2005)

Em relação ao padrão ETHERNET, considere os Itens abaixo:

I – Cabo Coaxial Fino
II – Fast Ethernet
III – Gigabit Ethernet
IV – 10 Gigabit Ethernet

I, II, III e IV referem-se, respectivamente:

a) 10Base5, 100BaseT, IEEE802.3g, IEEE702.3ae

b) 10Base5, 100BaseX, IEEE802.3g, IEEE802.3gg

c) 10Base5, 10BaseX, IEEE802.3ae, IEEE802.3z

d) 10Base2, 100BaseT, IEEE802.3z, IEEE802.3ae

e) 10Base2, 100BaseG, IEEE802.3ae, IEEE802.3z

Questão 50 (FCC/DETRAN-MA/ASSISTENTE DE TRÂNSITO/2018) Atualmente, o acesso à internet é realizado por meio de uma estrutura composta tipicamente por um provedor de acesso à internet, um Modem/roteador de acesso ao provedor, um Access Point/roteador sem

fio Wi-Fi (802.11g) e um computador portátil. Com relação à comunicação Wi-Fi, é correto afirmar que

a) utilizar o WEP é mais seguro que a comunicação por cabo de par trançado.

b) permite o acesso à internet, mas não à intranet.

c) possui velocidade de transmissão maior que um cabo de par trançado Categoria 5.

d) opera na frequência de 2,4 GHz, ou seja, micro-ondas.

e) opera na mesma frequência dos telefones sem fio, ou seja, 900 MHz.

GABARITO

1. e
2. E
3. E
4. C
5. C
6. E
7. e
8. E
9. e
10. E
11. E
12. E
13. E
14. C
15. E
16. C
17. C
18. E
19. E
20. C
21. C
22. E
23. C
24. b
25. c
26. a
27. d
28. c
29. a
30. a
31. e
32. a
33. d
34. a
35. b
36. b
37. e
38. c
39. d
40. d
41. b
42. c
43. d
44. d
45. e
46. c
47. d
48. c
49. d
50. d

GABARITO COMENTADO

Questão 1 (CESPE/MPC-PA/ASSISTENTE MINISTERIAL DE INFORMÁTICA/2019) Considere que quatro empresas distintas, localizadas em países e continentes diferentes, tenham de acessar e compartilhar dados entre si. Essa demanda pode ser atendida mediante a elaboração de projeto em que se conste a implementação de uma rede

a) VoIP (voice over IP).

b) PGP (Pretty Good Privacy).

c) LAN (local area network).

d) SSL (secure sockets layer).

e) WAN (wide area network).

Letra e.

a) Errada. VoIP (Voice over Internet Protocol) é a tecnologia que torna possível a comunicação de voz sobre a rede IP permitindo, assim, a realização de chamadas telefônicas pela Internet.

b) Errada. PGP (Pretty Good Privacy) é um pacote que fornece recursos de compactação, privacidade e assinaturas digitais, além de poder criptografar mensagens de correio eletrônico. A tecnologia PGP consiste de um **sistema híbrido de criptografia** que usa tanto encriptação simétrica como assimétrica para atingir altos níveis de segurança e privacidade.

c) Errada. As redes podem ser classificadas de acordo com a distância e a disposição física entre seus computadores. Nesse contexto, a **LAN (Local Area Network)** é uma rede local, que permite a conexão de equipamentos em uma pequena área geográfica (como uma residência, um escritório, um prédio ou um grupo de prédios vizinhos), onde os computadores estão próximos uns dos outros.

d) Errada. SSL (Secure sockets layer) é um protocolo utilizado para prover segurança em redes de computadores. Por meio de criptografia fornece confidencialidade e integridade nas comunicações entre um cliente e um servidor, podendo também ser usado para prover autenticação.

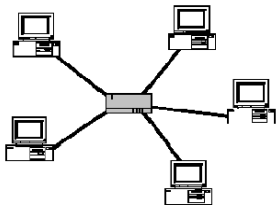
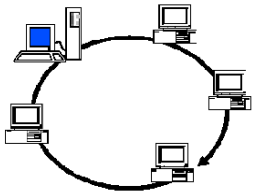
e) Certa. O **termo WAN (Wide Area Network, ou Rede de longa distância)** designa **uma rede geograficamente distribuída, que abrange uma grande área geográfica, conectando cidades e países.** Surgiu da necessidade de compartilhar recursos especializados por uma maior comu-

nidade de usuários geograficamente dispersos (localizados a grandes distâncias – até milhares de quilômetros – uns dos outros). Esse é o cenário destacado na questão em que quatro empresas distintas, localizadas em países e continentes diferentes, precisam acessar e compartilhar dados entre si.

Questão 2 (CESPE/STJ/TÉCNICO JUDICIÁRIO/ DESENVOLVIMENTO DE SISTEMAS/2018) Devido à sua estrutura, em uma rede usando a topologia estrela, o isolamento de falhas é uma tarefa complexa, o que representa uma desvantagem dessa topologia.

Errado.

A **topologia** refere-se ao layout, forma como as máquinas/cabos estão dispostos na rede e como as informações trafegam nesse ambiente.

Topologia	Pontos Positivos	Pontos Negativos
Estrela 	É mais tolerante a falhas, a falha de um PC não afeta os demais. Fácil acrescentar novos PC's. Gestão centralizada.	Custo de instalação maior porque recebe mais cabos. Se o ponto central falha, a rede falha.
Anel 	A mensagem enviada por um dos computadores atravessa todo o anel. Requer menos cabos. Desempenho uniforme.	Os problemas são difíceis de isolar.
Barramento (Barra ou **linear)** 	Simples e fácil de instalar. Fácil de ampliar. Requer menos cabos.	. A rede funciona por difusão (broadcast). A rede fica mais lenta em períodos de uso intenso. Os problemas são difíceis de isolar.

A **topologia de rede em estrela** possui características importantes que permitem isolar falhas. Neste tipo de topologia um elemento central controla o fluxo de dados da rede, ficando ligado ponto-a-ponto a cada nó. É esta característica que permite isolar um nodo em falha, evitando assim que o resto da rede seja afetada, permitindo assim a continuação de um bom funcionamento da rede. No entanto, esta topologia tem a **desvantagem** de requerer maiores comprimentos de cabo para a implementar do que numa rede baseada em barramentos por exemplo. Uma outra desvantagem se o nodo central por algum problema parar de funcionar compromete toda a rede.

Vantagens da Topologia em Estrela:

- Facilidade de inserir novos dispositivos na rede;
- Toda a comunicação é supervisionada por um nó central;
- Se o cabo da conexão de dispositivo possuir qualquer falha, não afeta a integridade da rede toda;
- A unidade central determina a velocidade de transmissão entre o transmissor e o receptor, e converte sinais transmitidos por protocolos diferentes.

Questão 3 (CESPE/STJ/TÉCNICO JUDICIÁRIO/ DESENVOLVIMENTO DE SISTEMAS/2018) A rede mostrada na figura a seguir, em que as linhas representam conexões entre computadores, apresenta topologia mesh.

Errado.

Numa **topologia Mesh**, **os computadores e redes locais interligam-se entre si, ponto a ponto, através de cabos e dispositivos de interligação adequados**. Assim, **existem diversos caminhos para se chegar ao mesmo destino.**

O papel fundamental, cabe, neste caso, aos dispositivos de interligação – por exemplo, os routers – que se encarregam do encaminhamento das mensagens através dos vários nós da

malha constituída. Uma **vantagem** é que existem vários caminhos possíveis para a comunicação. Por exemplo, quando enviamos um e-mail, ele pode seguir diversos caminhos. Caso haja problema em um caminho, a mensagem segue por outro caminho, aumentando assim a probabilidade de chegar ao destino.

A figura apresentada mostra uma topologia em barramento, em que todos os computadores são ligados em um mesmo barramento físico de dados. Quando um computador estiver a transmitir um sinal, toda a rede fica ocupada e se outro computador tentar enviar outro sinal ao mesmo tempo, ocorre uma colisão e é preciso reiniciar a transmissão.

Questão 4 (CESPE/ABIN/OFICIAL TÉCNICO DE INTELIGÊNCIA/2018) Na topologia em anel, cada bite se propaga de modo independente, sem esperar pelo restante do pacote ao qual pertence, sendo possível que um bite percorra todo o anel enquanto outros bites são enviados ou, muitas vezes, até mesmo antes de o pacote ter sido inteiramente transmitido.

Certo.

Conforme consta no livro de A. S. Tanenbaum, nas redes de **topologia em anel** cada bit se propaga de modo independente, sem esperar pelo restante do pacote ao qual pertence. Em geral, cada bit percorre todo o anel no intervalo de tempo em que alguns bits são enviados, muitas vezes até mesmo antes de o pacote ter sido inteiramente transmitido.

Um bit viaja partir de um sistema através de uma série de links e roteadores até atingir o sistema de destino. Nesse caminho, o bit é transmitido diversas vezes. O sistema de origem transmite o bit, o primeiro roteador recebe o bit e o transmite e assim por diante. Enquanto viaja da origem para o destino, o bit passa por uma série de transmissores e receptores. Cada bit é enviado pela propagação de ondas eletromagnéticas ou pulsos ópticos através de um meio físico. Os meios físicos podem ter formas distintas e não precisam ser do mesmo tipo em todo o caminho. Cada bit se propaga de modo independente não importando a topologia ou protocolo.

Questão 5 (CESPE/ABIN/OFICIAL TÉCNICO DE INTELIGÊNCIA/2018) Nas redes locais de difusão do tipo anel, há necessidade de se definir alguma regra para arbitrar os acessos simultâneos ao enlace.

Certo.

São caracterizadas pelo compartilhamento, por todas as estações, de uma linha única de transmissão. Neste caso, as mensagens enviadas por uma estação são recebidas por todas as outras conectadas à rede, sendo que um campo de endereço contido na mensagem permite identificar o destinatário.

Assim como ocorre em todos os outros sistemas de difusão, existe a necessidade de se definir alguma regra ou protocolo para arbitrar ou gerenciar os acessos simultâneos ao anel. Por exemplo: O IEEE 802.5 (a rede Token Ring da IBM) é uma rede local baseada em anel que opera a 4 e 16 Mbps. O FDDI é um outro exemplo de rede em anel.

Questão 6 (CESPE/POLÍCIA FEDERAL/AGENTE DE POLÍCIA FEDERAL/2018) Marta utiliza uma estação de trabalho que executa o sistema operacional Windows 10 e está conectada à rede local da empresa em que ela trabalha. Ela acessa usualmente os sítios da intranet da empresa e também sítios da Internet pública. Após navegar por vários sítios, Marta verificou o histórico de navegação e identificou que um dos sítios acessados com sucesso por meio do protocolo HTTP tinha o endereço 172.20.1.1.

Tendo como referência essa situação hipotética, julgue o item a seguir.

O endereço 172.20.1.1 identificado por Marta é o endereço IPv4 de um servidor *web* na Internet pública.

Errado.

Dos mais de 4 bilhões de endereços IPs disponíveis, três faixas são reservadas para redes privadas. Essas faixas não podem ser roteadas para fora da rede privada, ou seja, não podem se comunicar diretamente com a Internet.

Dentro das classes A, B e C foram reservadas redes, definidas pela RFC 1918, que são conhecidas como **endereços de rede privados.** São eles:

Endereço	***Faixa de IP***
Classe A - **10.0.0.0/8**	(10.0.0.0 – 10.255.255.255)
Classe B - **172.16.0.0/12**	(172.16.0.0 – 172.31.255.255) (O endereço IPv4 172.20.1.1 está incluído nessa faixa).

Classe C - **192.168.0.0/16**	(192.168.0.0 – 192.168.255.255)

Assim, conforme visto na tabela anterior, o endereço **IPv4 172.20.1.1 está incluído na faixa de endereços reservados** especificamente para uso em redes locais, não podendo ser utilizado como endereço IPv4 de um servidor web na Internet pública.

O papel do **NAT** consiste em **traduzir os endereços privados que não são válidos na Internet para um endereço válido**, ou seja, que possa navegar na Internet.

Questão 7 (CESPE/SEFAZ-RS/TÉCNICO/ADAPTADA/2018) Para a interligação dos dispositivos em uma rede de comunicação, deverá ser utilizado um cabo com blindagem de isolamento, com capacidade de tráfego de dados de até 10 Gb e que permita o menor índice possível de interferências. Nesse caso, será correto utilizar o cabo categoria

a) 1.

b) 3.

c) 5.

d) 5a.

e) 7.

Letra e.

Os cabos das categorias 6a e 7 podem ser utilizados, pois permitem capacidade de tráfego de dados de até 10 Gb. Dentre as assertivas, só nos resta marcar a letra "e".

Categoria	Frequência	Aplicações	Observações
Cat 5	**100 MHz**	100BASE-TX / **1000BASE-T**	Criados para redes **Fast Ethernet com taxa de 100 Mbps**. Suporta também *Gigabit Ethernet* com taxa de 1000 Mbps. (CAT5 não é mais recomendado pela TIA/EIA).
Cat 5e	**100 MHz**	**1000BASE-T** / 2.5GBASE-T	**Cat 5 melhorado.** Ainda muito comum nas redes.

Categoria	Frequência	Aplicações	Observações
Cat 6a	500 MHz	**5GBASE-T / 10GBASE-T**	Cat 6 melhorado. Atinge 100 metros em 10GBASE-T. Para que os cabos CAT 6a sofressem menos interferências os pares de fios são separados uns dos outros, o que aumentou o seu tamanho e os tornou menos flexíveis.
Cat 7	600 MHz	**5GBASE-T / 10GBASE-T**	Criado para tráfego multimídia. **Possui isolamento contra interferências**.
Cat 7a	1000 MHz	**5GBASE-T / 10GBASE-T**	Semelhante ao CAT 7. Assim como o CAT 7 utiliza conector diferente do *RJ*-45.

Fonte: https://techenter.com.br/cabos-de-par-trancado-categorias-e-tipos/. *Acesso em: jan. 2020*

Questão 8 (CESPE/ABIN/OFICIAL TÉCNICO DE INTELIGÊNCIA/ÁREA 6/2018) Com relação às tecnologias para construir um sistema de comunicação para transmitir um sinal de informação, julgue o item consecutivo.

Ainda que se escolha a fibra óptica como meio de transmissão do sinal de informação, o sistema não será robusto à interferência eletromagnética de outros sistemas de radiofrequência que operem na região.

Errado.

Ao se escolher a fibra óptica como meio de transmissão do sinal de informação, o sistema **NÃO** é afetado por **interferência eletromagnética** de outros sistemas de radiofrequência que operem na região.

Os cabos de fibra óptica são **IMUNES** À INTERFERÊNCIA ELETROMAGNÉTICA, pois não possuem malha metálica.

Questão 9 (FCC/NOSSA CAIXA/ANALISTA DE SISTEMAS/2011) Em relação à topologia de redes, considere:

I – Numa sala de espera anuncia-se a senha de número 45. Todas as pessoas escutam, mas somente o portador desta senha dirige-se ao balcão de atendimento.

II – Numa sala de reunião, a lista de presença é passada de mão em mão. Cada um dos presentes preenche seus dados e a repassa ao vizinho, até que a lista seja preenchida por todos.

Analogamente, os casos I e II estão associados, respectivamente, às características de funcionamento das topologias:

a) anel e estrela;

b) estrela e árvore;

c) barramento e estrela;

d) anel e árvore;

e) barramento e anel.

Letra e.

Item I. Analogamente essa assertiva faz referência à **Topologia em Barramento**. Principais características:

- computadores compartilham cabo único;
- dados são recebidos por todos, mas só a máquina de destino aceita;
- somente 1 computador por vez pode transmitir dados;
- se houver ruptura no cabo, toda rede é afetada.

Item II. Analogamente essa assertiva faz referência à **Topologia em Anel**. Principais características:

- estações conectadas por um único cabo, em forma de círculo;
- conceito de Token para transmissão;
- falha em um computador impacta toda rede.

Diante do exposto, a letra “e” é a resposta da questão.

Questão 10 (CESPE/EBSERH/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/2018) Acerca de infraestrutura de TI, julgue o item subsequente.

Uma rede sem fio que utiliza o padrão IEEE 802.11n tem, em ambiente sem obstáculos físicos, alta capacidade de transmissão de dados, sendo capaz de atingir até 1 Gbps, usando até 5 antenas em um único *access point*.

Errado.

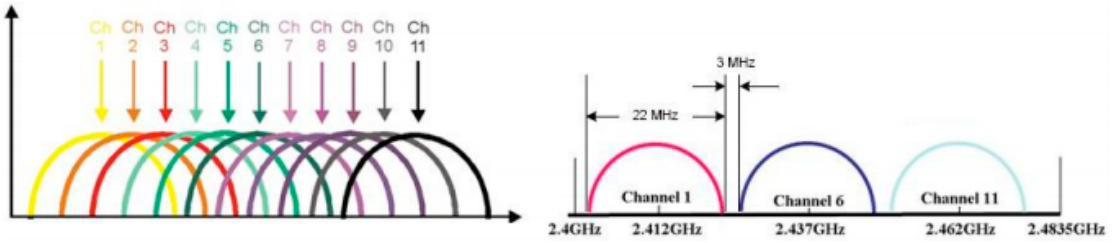
Uma rede sem fio que utiliza o padrão IEEE 802.11n tem, em ambiente sem obstáculos físicos, alta capacidade de transmissão de dados, sendo capaz de atingir até **600 Mbps**, quando operando com **4 antenas** no transmissor e no receptor, e utilizando a modulação **64-QAM** (Quadrature Amplitude Modulation).

Questão 11 (CESPE/STJ/ TÉCNICO JUDICIÁRIO - SUPORTE TÉCNICO/2018) Acerca de topologias e equipamentos de rede, julgue o item seguinte. Em uma rede local sem fio que utilize equipamentos de access point operando no padrão IEEE 802.11b, o tráfego de dados pode atingir velocidade de até 54 Mbps.

Errado.

Conforme visto na tabela seguinte, o padrão 802.11b permitirá velocidade máxima de11 Mbps.

Padrão	Frequência	Velocidade	OBS.
802.11**b**	2,4 GHz	11 Mbps	O padrão mais antigo



Canais de operação de uma WLAN no Brasil – IEEE 802.11b

Questão 12 (CESPE/TELEBRAS/NÍVEL MÉDIO/CONHECIMENTOS BÁSICOS/2013) Os pacotes são unidades maiores de informação que contêm uma mensagem inteira encapsulada, que é transmitida entre computadores de uma rede, os quais alocam integralmente os recursos de transmissão enquanto as mensagens estão sendo transmitidas.

Errado.

Em teoria, uma única comunicação, tal como um vídeo ou uma mensagem de email, poderia ser enviada por uma rede de uma origem a um destino como um fluxo de bits massivo e contínuo. Se as mensagens fossem realmente transmitidas dessa maneira, isso significaria que nenhum outro dispositivo seria capaz de enviar mensagens na mesma rede enquanto essa transferência de dados estivesse em progresso. Esses grandes fluxos de dados resultariam em atrasos consideráveis. Além disso, se um link na infraestrutura de rede falhar durante a transmissão, toda a mensagem seria perdida e teria de ser retransmitida por completo.

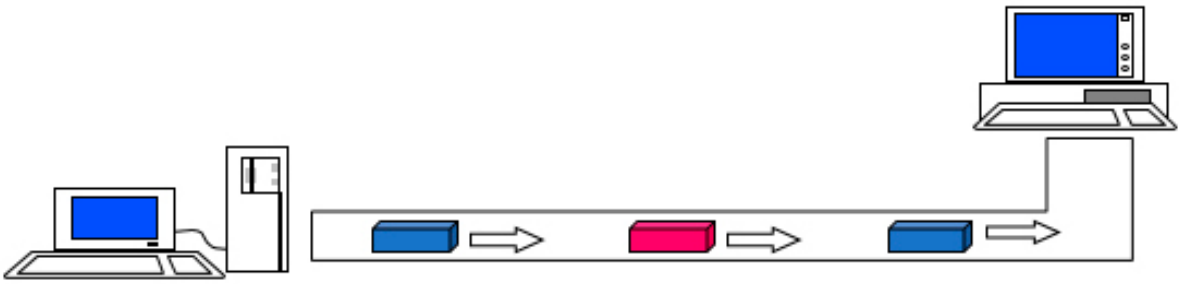
Uma melhor abordagem seria **dividir os dados em pedaços menores** e mais gerenciáveis para o envio através da rede. Essa divisão do fluxo de dados em pedaços menores é chamada de **segmentação**. Segmentar mensagens gera dois benefícios primários.

Primeiro, ao se enviar pedaços ou partes individuais menores da origem ao destino, várias conversas diferentes podem ser intercaladas na rede. O processo utilizado para intercalar os pedaços de conversas separadas na rede é chamado de **multiplexação**.

Segundo, a segmentação pode aumentar a confiabilidade das comunicações de rede. Os pedaços separados de cada mensagem não precisam viajar o mesmo caminho pela rede da origem ao destino. Se um caminho específico se tornar congestionado com tráfego de dados ou falhar, pedaços individuais da mensagem ainda podem ser direcionados ao destino usando caminhos alternativos. Se uma parte da mensagem falhar ao ser enviada ao destino, somente as partes perdidas precisam ser retransmitidas.

Assim, os pacotes são unidades **menores** de informação, que contém **um pedaço de uma mensagem** encapsulada (no pacote de dados). Quando enviados, alocam **somente os recursos para envio daquele pacote de dados**, podendo compartilhar o meio de comunicação com outras mensagens de outros dispositivos (técnica de multiplexação).

Na maioria das redes, as informações enviadas são quebradas em partes menores chamadas "**pacotes**".



Cada pacote deve conter dados de endereçamento para que possam chegar ao seu destino e serem recompostos.

Questão 13 (CESPE/ANEEL/TODOS OS CARGOS/2010) FTP é um protocolo de comunicação que permite o envio de arquivos anexos a mensagens de correio eletrônico, sem a necessidade de compactar esses arquivos.

Errado.

O **FTP (File Transfer Protocol - Protocolo de Transferência de arquivos)** não é usado para envio de mensagens de texto contendo anexos, e sim para a troca de arquivos e pastas entre cliente e servidor.

Questão 14 (CESPE/IPEA/ANALISTA BD/2008) Os protocolos de comunicação podem ser organizados em hierarquias compostas por camadas, em que cada camada oferece serviços para a camada acima. A um conjunto de camadas, pode ser dado o nome de pilha de protocolos. Em uma pilha, tipicamente, a camada mais inferior é a física e uma camada intermediária é a de transporte, que fornece um serviço de comunicação entre pares de portas ligadas a processos.

Certo.

A maioria dos protocolos, especialmente no contexto da comunicação em rede de computadores, são agrupados em **pilhas de protocolos**, nas quais as diferentes tarefas que perfazem uma comunicação são executadas por níveis especializados da pilha. Enquanto uma pilha de protocolos denota uma combinação específica de protocolos que trabalham conjuntamente, um modelo de referência é uma arquitetura de software que lista cada um dos níveis e os serviços que cada um deve oferecer. O modelo clássico OSI, em sete níveis é utilizado para conceitualizar pilhas de protocolo.

Para que você memorize os nomes das camadas do modelo OSI, aqui vai uma dica: lembre-se da palavra **FERTSAA**, com as iniciais de cada camada, que são: **F**->Física, **E**->Enlace, **R-**>Rede, **T**->Transporte, **S**->Sessão, **A**->Apresentação. Fácil, não é mesmo?

Questão 15 (CESPE/STF/2008) O UDP é um protocolo de transporte que não estabelece conexões antes de enviar dados, não envia mensagens de reconhecimento ao receber dados, não controla congestionamento, garante que dados sejam recebidos na ordem em que foram enviados e detecta mensagens perdidas.

Errado.

O **UDP (User Datagram Protocol – Protocolo de Datagrama de Usuário)** é um protocolo de transporte que não estabelece conexões antes de enviar dados (é não orientado à conexão). Ele fornece uma entrega rápida mas não confiável dos pacotes. O UDP não fornece o controle de fluxo necessário, nem tampouco exige uma confirmação do receptor, o que pode fazer com que a perda de um pacote aconteça SEM a devida correção.

Portanto, com a utilização do UDP os datagramas podem chegar fora de ordem, e também ele não detecta mensagens perdidas. Demais itens da questão estão ok.

Questão 16 (CESPE/SERPRO/ANALISTA/REDES DE COMPUTADORES/2005) Entre as pilhas de protocolos mais usadas na atualidade, encontra-se o TCP/IP, que tem entre os seus protocolos principais o IP, serviço de datagramas, e o TCP, serviço de transporte confiável.

Certo.

Para que os computadores de uma rede possam trocar informações entre si é necessário que todos estejam utilizando o mesmo **protocolo** - conjunto de regras necessárias para que o computador de destino "entenda" as informações no formato que foram enviadas pelo computador de origem.

Antes da popularização da Internet existiam diferentes protocolos sendo utilizados nas redes das organizações, alguns roteáveis - que permitiam o acesso das redes à Internet (como o TCP/IP) e outros não (como o NETBEUI, por exemplo). Na atualidade, o protocolo TCP/IP passou a tornar-se um padrão de fato, em virtude da necessidade de as redes atuais terem acesso à Internet. O **TCP/IP na verdade é uma pilha de protocolos**, sendo que os 2 protocolos mais importantes dessa pilha são o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo Internet), destacados a seguir:

TCP: é um protocolo de transporte, que executa importantes funções para garantir que os dados sejam entregues de uma maneira **confiável**, ou seja, sem que sejam corrompidos ou alterados. O TCP, portanto, fornece um serviço orientado à conexão confiável, com controle de erros na transmissão dos pacotes!

Para memorizar!

O TCP (Protocolo de Controle de Transmissão) => é confiável, orientado à conexão e faz controle de fluxo.

IP: esse protocolo encapsula ou empacota o segmento ou datagrama da camada de transporte para que a rede possa entregá-lo ao host de destino.

Questão 17 (CESPE/MPU/TÉCNICO TI/2010) Um computador que tem conectado nele uma impressora compartilhada com a rede pode ser adequadamente configurado em um servidor DHCP como se fosse um equipamento com um endereço IP fixo.

Certo.

Nesse caso, como o computador estará compartilhando um recurso (impressora) na rede, é até mesmo aconselhável que façamos a configuração de um endereço IP fixo para o computador no servidor DHCP.

Questão 18 (CESPE/IJSN-ES/2010) A respeito dos sistemas, das tecnologias e dos protocolos de redes sem fio, julgue os itens que se seguem.

A conexão de um cliente que usa o padrão IEEE 802.11b a um ponto de acesso que usa o padrão IEEE 802.11g pode proporcionar ao cliente um desempenho com maior velocidade].

Errado.

A transmissão em uma rede no padrão IEEE 802.11 é feita através de ondas eletromagnéticas, que se propagam pelo ar e podem cobrir áreas na casa das centenas de metros.

Quanto aos padrões mencionados na questão temos:

Padrão	Frequência	Velocidade	Observação
802.11b	2,4 GHz	11 Mbps	O padrão mais antigo
802.11g	2,4 GHz (compatível com 802.11b)	54 Mbps	Atualmente, é o mais usado.

Conforme visto na tabela, 802.11b =11 Mbps e o 802.11g = 54 Mbps. Portanto, o usuário estará limitado à capacidade do seu equipamento, compatível com IEEE 802.11b, e não terá ganho de velocidade.

Questão 19 (CESPE/TCE-RN/2009) A taxa máxima de transmissão de dados no padrão IEEE 802.11b é de 54 Mbps e o acesso ao meio é do tipo CSMA/CD.

Errado.

A taxa máxima de transmissão de dados no padrão IEEE 802.11b é de 11 Mbps, e o acesso ao meio é do tipo **CSMA/CA**.

Cisco (2010) destaca que no **CSMA/CA (Collision Avoidance - Prevenção de Colisão)** o dispositivo examina o meio para verificar a presença de sinal de dados. Se estiver livre, o dispositivo envia uma notificação através do meio com sua intenção de usá-lo. O dispositivo então envia os dados. Esse método é usado pelas tecnologias de rede sem fio 802.11.

Complementando, no CSMA/CD (*Collision Detection* - Detecção de Colisão) o dispositivo monitora o meio para verificar a presença de sinal de dados. Se um sinal de dados está ausente,

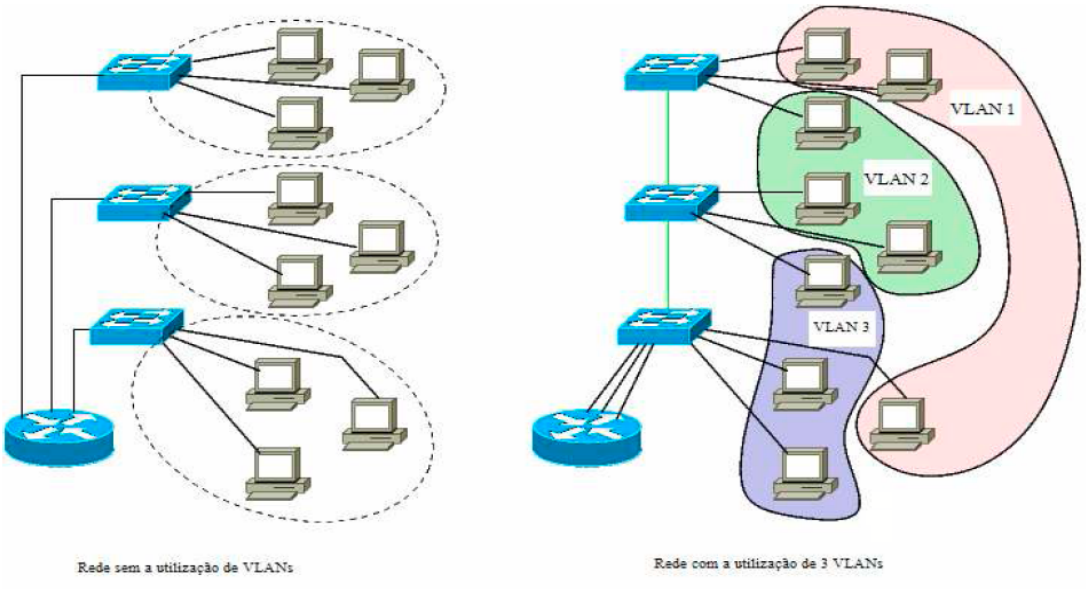
indicando que o meio está livre, o dispositivo transmite os dados. Se são detectados sinais que mostram que um outro dispositivo estava transmitindo ao mesmo tempo, todos os dispositivos param de enviar e tentam novamente mais tarde.

Questão 20 (CESPE/IJSN-ES/2010) Considere dois hosts A e B que estejam conectados a um switch. Nessa situação, se o host A enviar um frame em broadcast e o host B não receber esse frame, então é correto inferir que os hosts A e B pertencem a VLANS diferentes.

Certo.

A **rede local virtual (VLAN)** é uma rede de computadores que se comporta como se estivessem conectados ao mesmo segmento de rede embora possam estar fisicamente localizados em segmentos diferentes da LAN. As VLANS são configuradas por software no switch e no roteador (CISCO, 2010).

Exemplo:



Questão 21 (CESPE/TCU/2009) Com relação às tecnologias de redes locais, julgue os itens a seguir. [A interconexão de redes CSMA/CD, como Ethernet e IEEE 802.3, utilizando bridges ou switches, agrega os domínios de broadcast das redes, porém preserva seus domínios de colisão].

Certo.

Um maior número de hosts conectados a uma única rede pode produzir volumes de tráfego de dados que podem forçar, quando não sobrecarregar, os recursos de rede como a largura de banda e a capacidade de roteamento.

A divisão de grandes redes de modo que os hosts que precisam se comunicar sejam reunidos reduz o tráfego nas conexões de redes.

Além das próprias comunicações de dados entre hosts, o gerenciamento da rede e o tráfego de controle (overhead) também aumentam com o número de hosts. Um contribuinte significativo para este overhead pode ser os broadcasts.

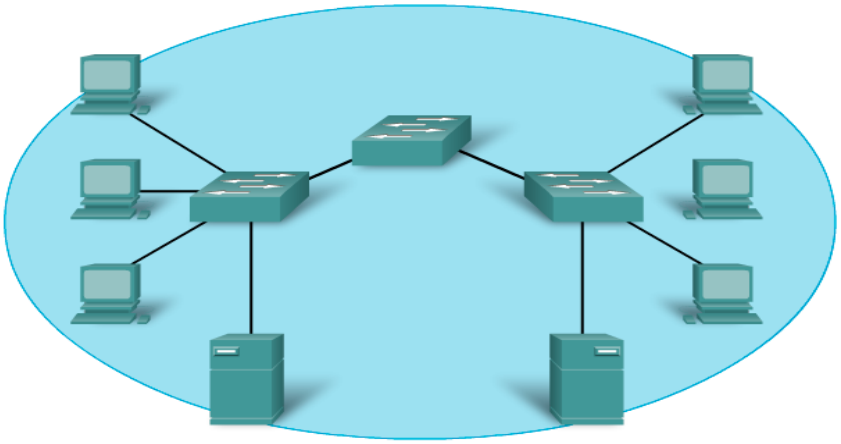
Um broadcast é uma mensagem enviada de um host para todos os outros hosts da rede.

Normalmente, um host inicia um broadcast quando as informações sobre um outro host desconhecido são necessárias. O broadcast é uma ferramenta necessária e útil usada pelos protocolos para habilitar a comunicação de dados nas redes. Porém, grandes números de hosts geram grandes números de broadcast que consomem a largura de banda. E em razão de alguns hosts precisarem processar o pacote de broadcast, as outras funções produtivas que o host está executando também são interrompidas ou deterioradas.

Os **broadcasts** ficam contidos dentro de uma rede. Neste contexto, uma rede também é conhecida como um **domínio de broadcast**. Gerenciar o tamanho dos domínios de broadcast pela divisão de uma rede em sub-redes garante que o desempenho da rede e dos hosts não seja deteriorado em níveis inaceitáveis.

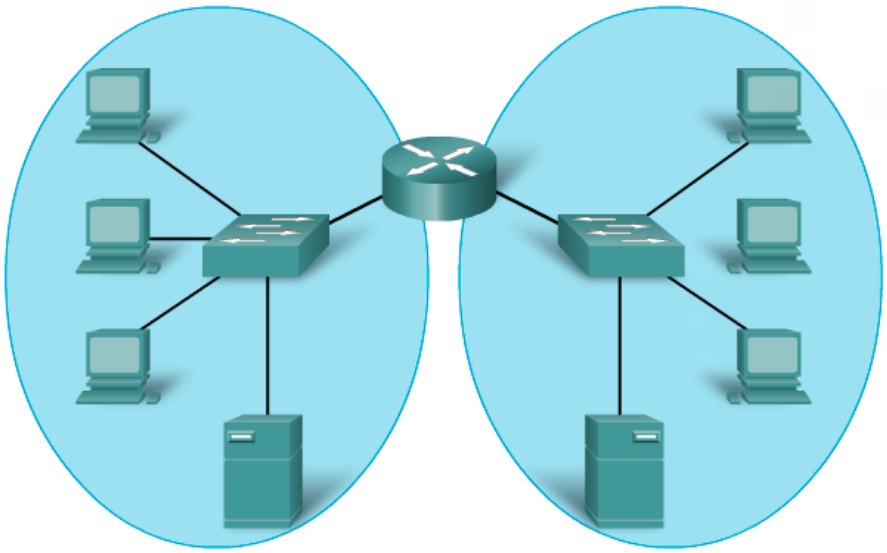
Domínio de broadcast

Computadores pertencentes a uma mesma rede IP, que se comunicam sem o auxílio de um roteador.



Todos os dispositivos nesta rede estão conectados em um domínio de broadcast quando o switch é configurado para as configurações padrão de fábrica. Uma vez que os switches encaminham broadcasts por padrão, os broadcasts são processadas por todos os dispositivos nesta rede.

Figura 1. Um domínio de broadcast (CISCO, 2010)



Substituir o switch por um roteador cria 2 sub-redes IP, portanto, 2 domínios distintos de broadcast. Todos os dispositivos são conectados, mas broadcasts locais são incluídas.

Figura 2. Dois domínios distintos de broadcast (CISCO, 2010)

Observe na Figura 2 que a substituição de um switch por um roteador separa um grande domínio de broadcast em dois domínios mais gerenciáveis.

Domínio de colisão

Dois ou mais computadores conectados a um mesmo barramento (físico ou lógico).

Hub

Amplia os domínios de broadcast e colisão a todos os computadores a ele conectados.

Switch/Bridge

Amplia **apenas** o domínio de broadcast.

Cada porta do switch (incluindo aqui o uplink) é um domínio de colisão distinto.

Questão 22 (CESPE/MPOG/PROCESSO SELETIVO INTERNO PARA GRATIFICAÇÕES DO GSISP/NÍVEL SUPERIOR/2009) Os roteadores atuam no nível de datagrama, levando em consideração as informações de endereço físico de destino para decidir para que interface encaminhar o pacote.

Errado.

Os roteadores levam em consideração as informações do endereço lógico (IP) do destino para decidir para onde devem encaminhar o pacote.

Questão 23 (CESPE/MPOG/PROCESSO SELETIVO INTERNO PARA GRATIFICAÇÕES DO GSISP/NÍVEL SUPERIOR/2009) Quanto aos elementos ativos de infraestrutura e serviços de redes de comunicação, julgue os itens subsequentes. [Roteadores são exemplos de gateways que tipicamente interconectam redes de diferentes topologias de enlace, encaminhando datagramas a partir das informações do protocolo de rede].

Certo.

Roteador é um equipamento que pode ser usado para a **comunicação entre redes distintas**, permitindo a comunicação de computadores distantes entre si.

Os roteadores são dispositivos que operam na Camada de Rede do modelo OSI e têm como principal função: selecionar a rota mais apropriada para encaminhar os datagramas recebidos, ou seja, escolher o melhor caminho disponível na rede para um determinado destino.

Questão 24 (FCC/MANAUSPREV/ANALISTA PREVIDENCIÁRIO/ TECNOLOGIA DA INFORMAÇÃO/2015) Wi-Fi é um conjunto de especificações para redes locais sem fio (Wireless Local Area Network – WLAN) que são conhecidas como redes no padrão IEEE

a) 802.2.

b) 802.11.

c) 802.8.

d) 802.16.
e) 802.15.

Letra b.

Wi-Fi é um conjunto de especificações para redes locais sem fio (Wireless Local Area Network – WLAN) que são conhecidas como redes no padrão IEEE 802.11.

Padrão	**802.11b**	**802.11g**	**802.11a**	**802.11n**
Faixa de frequência	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz e/ou 5 GHz
Largura de banda	20 MHz	20 MHz	20 MHz	20 MHz ou 40 MHz
Velocidade de transmissão	11 Mbps	54 Mbps	54 Mbps	Até 600 Mbps

QUESTÃO 25 (FCC/TRE-RR/TÉCNICO DO JUDICIÁRIO/OPERAÇÃO DE COMPUTADORES/2015) A rede Wi-Fi está em conformidade com a família de protocolos 802.11 do IEEE. Dentro desta família de protocolos, o que pode atingir taxas de transmissão de até 54 Mbit/s e opera na frequência de 2.4 GHz é o padrão

a) 802.11a.
b) 802.11h.
c) 802.11g.
d) 802.11ac.
e) 802.11b.

Letra c.

A questão destaca o padrão 802.11g, aprovado em 2003. Esse padrão veio para trabalhar na frequência de **2,4GHz,** permitindo atingir taxas de transmissão de até **54Mbps**.

QUESTÃO 26 (FCC/TRT-15ª/CAMPINAS/TÉCNICO JUDICIÁRIO/TI/2015) Atualmente, o mercado oferece dispositivos para acesso à rede sem fio nas diversas versões do padrão IEEE

802.11. Caso a versão 802.11g seja escolhida para implementar uma WLAN, o esquema de segurança a ser escolhido deve ser o

a) WPA2, pois utiliza o AES que é o mais seguro atualmente.

b) WEP, pois utiliza o esquema de chave dinâmica de 64 bits, sendo simples e seguro.

c) WPA, pois é mais simples e seguro que o WPA2.

d) WPA2, pois utiliza o TKIP que é o mais seguro atualmente.

e) WPA, pois utiliza o esquema de chave fixa de 128 bits que não pode ser quebrada.

Letra a.

O esquema de segurança a ser escolhido deve ser o **WPA2**, que segue o padrão 802.11i e substitui formalmente o WEP. O **WPA2 utiliza o AES** (*Advanced Encryptation Standard*). O AES permite ser utilizada chave de 128, 192 e 256 bits (**o padrão no WPA2 é 256 bits)**, sendo assim, uma ferramenta muito poderosa de criptografia.

WPA2 = WPA + AES.

Questão 27 (FCC/CNMP/ANALISTA DO CNMP/SUPORTE E INFRAESTRUTURA/2015) A escolha do tipo de proteção em uma rede sem fio é uma etapa importante na sua configuração. Uma forma de proteção muito utilizada é a chave de rede

a) que consiste na autorização de acesso à rede apenas a computadores cujos endereços MAC foram emitidos após 2005, ano após o qual um padrão seguro de acesso a redes sem fio foi incorporado.

b) sendo que a do tipo WEP é a mais indicada, pois até hoje nenhum programa conseguiu quebrá-la.

c) sendo que a do tipo WPA é muito utilizada por se basear em encriptação de 16 *bits*.

d) que consiste em uma senha que o usuário deve digitar para acessar a rede sem fio.

e) que consiste na autorização de acesso à rede apenas a computadores cujos endereços MAC foram cadastrados para realizar esse acesso.

Letra d.

Uma forma de proteção muito utilizada é a chave de rede que consiste em uma senha que o usuário deve digitar para acessar a rede sem fio.

O esquema de segurança **WPA2**, segue o padrão 802.11i e substitui formalmente o WEP.

WPA utiliza encriptação de 128 bits e serviu como um padrão de "transição" entre o WEP e o WPA2.

Questão 28 (FCC/AL-PE/ANALISTA LEGISLATIVO/ INFRAESTRUTURA/2014) As redes sem fio (WiFi) apresentam características especiais de vulnerabilidade para as empresas, em função do sinal da rede poder ser capturado por dispositivos que possuam interface para redes sem fio, sendo esses equipamentos pertencentes à rede corporativa ou não. Para implantar a segurança nas redes sem fio de uma empresa, a equipe de TI deve aplicar o

a) protocolo WEP (Wired Equivalent Privacy) que possibilita a implementação de criptografia no meio WiFi, o qual não está sujeito a reinjeção de pacotes que levam à negação de serviços ou degradação do desempenho da rede.

b) protocolo WPA (Wi-Fi Protected Access) que possibilita a implementação de rede Ad-Hoc, não dependendo da centralização da comunicação em equipamentos de acesso WiFi.

c) WPA Corporativo, o qual tratará toda autenticação na rede através de um servidor de autenticação que se comunica com o AP (access point) do equipamento sem fio do usuário.

d) TKIP (Temporal Key Integrity Protocol) que é implementado no protocolo WEP e é baseado no conceito de chaves estáticas, ou seja, a chave não é substituída dinamicamente.

e) WPA2 que implementa criptografia com chave de encriptação de 64 bits.

Letra c.

Para implantar a segurança nas redes sem fio de uma empresa, a equipe de TI deve aplicar o **WPA Corporativo**, que tratará toda autenticação na rede através de um **servidor de autenticação** que se comunica com o AP (access point) do equipamento sem fio do usuário.

Questão 29 (FCC/TJ-PE/ANALISTA JUDICIÁRIO/ANALISTA DE SUPORTE/2012) É um tipo de rede em que a topologia pode se alterar o tempo todo e, consequentemente, até mesmo a validade dos caminhos podem se alterar de modo espontâneo, sem qualquer aviso:

a) Ad Hoc.

b) *Full-meshed*.

c) Hub-and-spoke.

d) WWAN.

e) WMAN.

Letra a.

Trata-se de **redes Ad Hoc**, que são **redes sem fio que dispensam o uso de um ponto de acesso comum aos computadores conectados a ela**, de modo que TODOS os dispositivos da rede funcionam como se fossem um roteador, encaminhando comunitariamente informações que vêm de dispositivos vizinhos.

Geralmente, numa rede ad hoc não há topologia predeterminada, nem controle centralizado, e a validade dos caminhos podem se alterar de modo espontâneo no tempo, sem necessidade de aviso.

Fonte: http://www.tecmundo.com.br/internet/2792-o-que-sao-redes-ad-hoc-.htm

---

Questão 30 (FCC/TRT-23ª/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2011) Para tornar confidenciais as mensagens nas redes de comunicação sem fio, os protocolos WEP, WPA e WPA2 se baseiam, respectivamente, entre outros componentes, no algoritmo de criptografia:

a) RC4, RC4 e AES.

b) RC4, RC4 e RC4.

c) AES, AES e RC4.

d) AES, AES e AES.

e) RC4, AES e AES.

Letra a.

A banca destacou algoritmos que controlam o sigilo. Assim, os protocolos WEP e WPA baseiam-se no RC4 e o WPA2 no AES.

Questão 31 (FCC/INFRAERO/ANALISTA SUPERIOR III SEGURANÇA DA INFORMAÇÃO/2011) Representam fragilidades de segurança em redes sem fio, EXCETO:

a) A maioria dos concentradores vem com serviço SNMP habilitado, e isso pode ser usado por um atacante, pois revela uma vasta gama de informações sobre a rede em questão.

b) A maioria dos equipamentos saem de fábrica com senhas de administração e endereço IP padrão. Caso estes não sejam trocados, poderão permitir a um atacante que se utilize delas em uma rede-alvo.

c) A alta potência dos equipamentos pode permitir que um atacante munido de uma interface de maior potência receba o sinal a uma distância não prevista pelos testes.

d) O posicionamento de determinados componentes de rede pode comprometer o bom funcionamento da rede e facilitar o acesso não autorizado e outros tipos de ataque.

e) Os métodos de segurança WEP são completamente vulneráveis por possuírem chaves WEP pré-configuradas que não podem ser modificadas.

Letra e.

a) Certa. Esse serviço habilitado por padrão facilita a gerência remota, e contribui para revelação de informações sobre a rede, por possuir senha e usuário padrão.

b) Certa. Isso acontece bastante, uma vez que é comum achar uma rede aberta ao nosso redor, sem troca de usuário/senha padrão.

a) Certa. Não conseguimos conter o avanço do sinal, assim, a alta potência dos equipamentos pode permitir que um atacante munido de uma interface de maior potência receba o sinal a uma distância não prevista pelos testes. A proteção nesse caso seria a criptografia.

d) Certa. Deixar equipamentos próximos a redes sem fio poderá comprometer o funcionamento da rede e facilitar o acesso não autorizado e outros tipos de ataque.

e) Errada. Essa opção não é uma vulnerabilidade. Essas chaves podem ser modificadas. Existem outras vulnerabilidades que poderiam ser relatadas.

Questão 32 (FCC/TRT-9ª/ANALISTA JUDICIÁRIO/TI/2010) O primeiro protocolo de criptografia disponível para redes Wi-Fi é baseado em um algoritmo chamado

a) RC4, que é um codificador de fluxo.
b) RSA, que é um decodificador de chave pública.
c) WAP, que é um protetor de arquivos transmitidos.
d) NAT, que é um decodificador de fluxos.
e) WPA, que é um protetor de arquivos transmitidos.

Letra a.

Dentre as assertivas, o algoritmo criptográfico a ser utilizado é **RC4**, que é um codificador de fluxo.

Questão 33 (FCC/AL-SP/AGENTE TÉCNICO LEGISLATIVO/SEGURANÇA DE REDES/2010) Com relação à robustez do método criptográfico utilizado, a ordem do protocolo mais vulnerável para o menos vulnerável é

a) TKIP, WPA e WEP.
b) WPA, TKIP e WEP.
c) TKIP, WEP e WPA.
d) WEP, TKIP e WPA.
e) WEP, WPA e TKIP.

Letra d.

WEP (Wired Equivalent Privacy) foi a primeira tentativa de se criar um protocolo eficiente de proteção de redes Wi-Fi. Dessa forma, é o mais vulnerável, e já eliminamos as assertivas (A), (B) e (C).

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) é um protocolo temporário de gerenciamento de chaves. Trata-se de um algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacote. A senha é modificada automaticamente por padrão a cada 10.000 pacotes enviados e recebidos pela sua placa de rede (Fonte: Wikipedia).

WPA (Wi-Fi Protected Access), também conhecido como WEP2 é um WEP melhorado. Surgiu com o objetivo de substituir o WEP, considerado inseguro. O WPA utiliza o algoritmo Temporal Key Integrity Protocol (TKIP) como padrão para criptografia de chaves por pacote. O TKIP utiliza o sistema de criptografia do WEP, mas usa no algoritmo RC4 chaves de 128 bits. Além disso, possui um sistema mais complexo de geração de chaves, pois a chave de criptografia do frame é extraída a partir do endereço MAC do transmissor, combinado com a chave de criptografia da rede e parte do IV *(vetor de inicialização)*.

WPA2 é o WPA + AES (ao invés do RC4).

Assim, a ordem correta é **WEP->TKIP ->WPA**.

Questão 34 (IADES/CONAB/TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO/NÍVEL MÉDIO/2014) Qual padrão IEE 802 é responsável pela tecnologia sem fio para comunicação pessoal (WPAN) e possibilita comunicações com distâncias de 1, 10 e até 100 metros, dependendo da potência de transmissão?

a) Bluetooth (802.15).

b) Wi-Fi (802.11).

c) WiMax (802.16)

d) Wireless (802.18).

e) WiMobily (802.20).

Letra a.

Veja a seguir a **classificação das redes sem fio (Redes Wireless):**

WPAN (Wireless Personal Area Network, Padrão IEEE 802.15 - Bluetooth)

Trata-se de uma **rede de computadores pessoal** - formada por nós (dispositivos conectados à rede, como computadores, telefones e PDAs) muito próximos uns dos outros e próximos a uma pessoa.

O termo **PAN** é bem novo, surgiu em função das novas tecnologias sem fio, como o **bluetooth**, que permite a ligação de vários equipamentos que estejam separados por distâncias de 1, 10 e até 100 metros, dependendo da potência de transmissão.

Esse tipo de rede é ideal para eliminar os cabos usualmente utilizados para interligar teclados, impressoras, telefones móveis, agendas eletrônicas, computadores de mão, câmeras fotográficas digitais, mouses e outros.

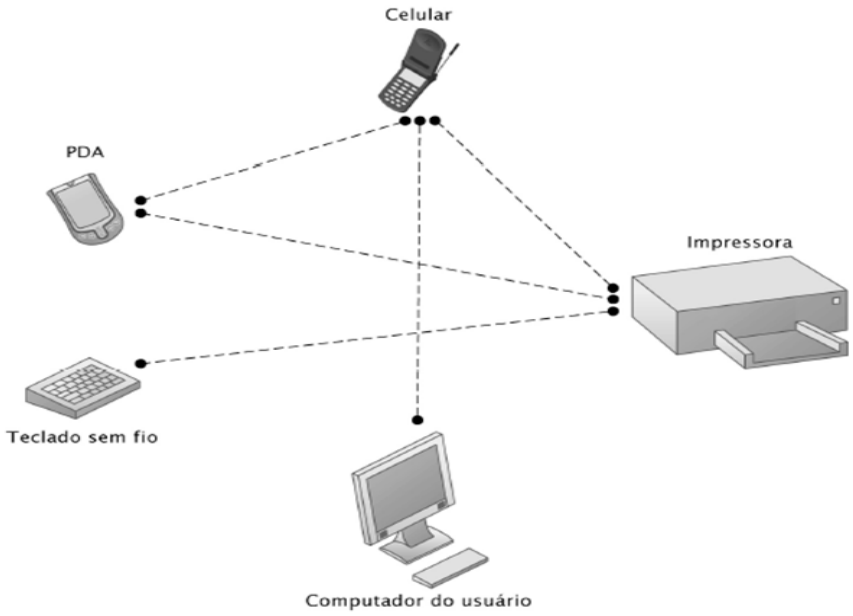


Figura – Exemplo de uma Rede WPAN

WLAN (Wireless Local Area Network), Padrão IEEE 802.11

É uma rede local sem fios com conexão à Internet, geralmente utilizada em escritórios, faculdades, aeroportos, entre outros locais.

WMAN (Wireless Metropolitan Area Network), Padrão IEEE 802.16 - WiMAX

As redes metropolitanas sem fios são utilizadas para a conexão de uma cidade, ou até mesmo em áreas um pouco menores como universidades. Um exemplo de rede que é classificada como WMAN, respeitando o padrão da norma IEEE 802.16, é o WiMAX.

WWAN (Wireless Wide Area Network), Padrão IEEE 802.20 - 3G/4G

Nesta encontramos as redes sem fios de grandes extensões, ou seja, de área geográfica de dimensões maiores, como um país, ou mesmo o mundo inteiro. Os telefones celulares são os principais dispositivos utilizados nesse escopo de rede.

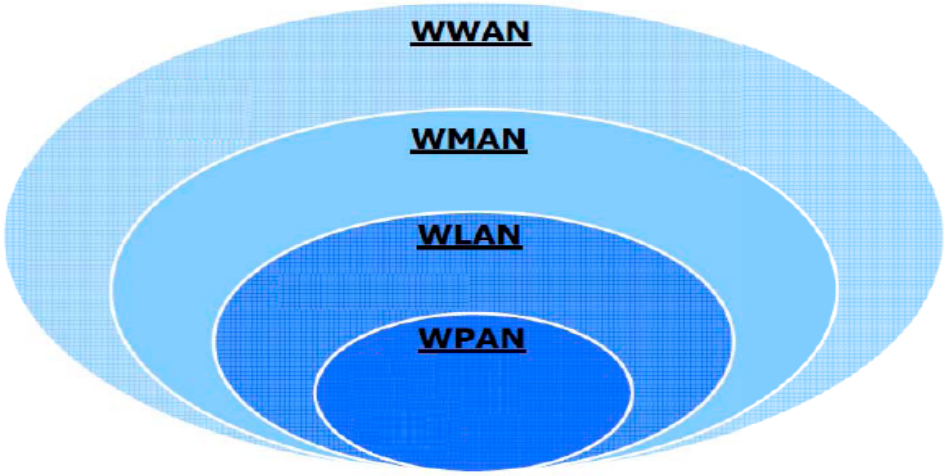


Figura. Redes Wireless

Questão 35 (IADES/EBSERH/ANALISTA DE TI/SUPORTE E REDES/SUPERIOR/2014) Assinale a alternativa que indica o padrão IEEE que regulamenta o uso de redes wireless com largura de banda de no máximo 54 Mbps operando na frequência de 5 GHz.

a) 802.11

b) 802.11a

c) 802.11b

d) 802.11g

e) 802.15

Letra b.

Os principais padrões da família **IEEE 802.11 (Wi-Fi)** são:

Padrão	Faixa de Frequência	Velocidade de Transmissão	Largura de Banda	Observação
802.11**b**	2,4 GHz	11 Mbps	20 MHz	O padrão mais antigo
802.11**g**	2,4 GHz (compatível com 802.11b)	54 Mbps	20 MHz	Atualmente, é o mais usado.
802.11a	**5 GHz**	**54 Mbps**	20 MHz	Pouco usado no Brasil. Devido à diferença de frequência, equipamentos desse padrão não conseguem se comunicar com os outros padrões citados.
802.11**n**	Utiliza tecnologia MIMO (Multiple Input/ Multiple Output), frequências de 2,4 GHz e/ou 5 GHz (compatível portanto com 802.11b e 802.11g e teoricamente com 802.11a)	Diversos fluxos de transmissão: 2x2, 2x3, 3x3,4x4. Velocidade nominal subiu de 54 para **300 Mbps** (**600 Mbps** nos APs 4x4, capazes de transmitir 4 fluxos simultâneos.	20 MHz ou 40 MHz	Padrão recente e que está fazendo grande sucesso.

A literatura já cita um novo padrão a caminho, o **802.11ac**, prometendo velocidades em torno de 1Gbps, largura de banda de 160MHz e multi-user MIMO.

Conforme visto, o padrão que regulamenta o uso de redes wireless com largura de banda de no máximo 54 Mbps operando na frequência de 5 GHz é o IEEE 802.11a.

Questão 36 (FCC/TRT-16ª REGIÃO/MA/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2014) Atenção: Para responder às questões de números 51 a 53, considere o texto abaixo.

Um Analista de Redes de Computadores deve planejar a instalação física e a configuração lógica de uma rede local de computadores do ambiente de escritório do Tribunal Regional do Trabalho da 16ªRegião. Dentre as especificações recebidas, estão: a área total do escritório é

de 200 m², a rede deve interligar 30 computadores, o uso dos computadores é para aplicativos típicos de escritório e TRT da 16ª Região contratou o serviço de acesso (provedor) para 100 Mbps.

A partir dessa especificação, o Analista escolheu o cabo de pares trançados para realizar as conexões na rede local. Face à variedade de categorias atualmente existentes para esse tipo de cabo, para essa instalação o Analista deve escolher o cabo

a) CAT3 que permite uma taxa de dados de até 100 Mbps e alcança 50 m.

b) CAT5 que permite uma taxa de dados de até 100 Mbps e alcança até 100m.

c) CAT5 que permite uma taxa de dados de até 100 Mbps e alcança até 200 m.

d) CAT6 que permite uma taxa de dados de até 200 Mbps e alcança 1.000 m.

e) CAT6 que permite uma taxa de dados de até 10.000 Mbps e alcança 1.000 m.

Letra b.

Para essa instalação o Analista deve escolher o cabo CAT5 que permite uma taxa de dados de até **100 Mbps** e alcança até **100 m**.

Quadro Resumo. Categorias de Fios de Par Trançado (*Twisted Pair*)

EIA/TIA	Utilização
CAT3	Dados até 16 MHz, incluindo 10Base-T e 100Base-T.
CAT4	Dados até 16 MHz, incluindo 10Base-T e 100Base-T.
CAT5	Dados até 100MHz, incluindo 100Base-T4 e 100Base-TX (extinto).

Quanto às distâncias, veja o exemplo seguinte:

Cable Name	Cable Type	Speed	Max Seg. Length
Ethernet			
10Base2	Coaxial RG-58 - Thinnet	10 Mbps	185 m
10Base5	Coaxial RG-8 - Thicknet	10 Mbps	500 m
10BaseT	UTP - CAT 3	10 Mbps	100 m
10BaseT	UTP - CAT 5	100 Mbps	100 m
10BaseF	Fiber Optic	10 Mbps	2 Km
Fast Ethernet			
100BaseT4	UTP - 4 pair (CAT 3,4 & 5)	100 Mbps	100 m
100BaseTX	UTP/STP - 2 pair (CAT 5)	100 Mbps	100 m
100BaseFX	Fiber Optic - 2 Strand	100 Mbps	2 Km
Gigabit Ethernet			
1000Base SX	Fiber - Multimode	1000 Mbps	550 m
1000Base LX	Fiber - Multimode	1000 Mbps	550 m
1000Base LX	Fiber - Singlemode	1000 Mbps	5 Km
1000Base CX	UTP	1000 Mbps	25 m
1000BaseT	UTP - CAT 5	1000 Mbps	100 m

Conforme visto, 100m é o tamanho máximo para configuração de T (Twisted pair), e a alternativa que se enquadra é a letra “b”.

Questão 37 (FCC/SABESP/TÉCNICO EM SISTEMAS DE SANEAMENTO 01/ELETRÔNICA/2018) Com relação ao protocolo IP, é correto afirmar:

a) Todos os computadores de uma determinada rede têm o mesmo número de IP.

b) O número IPv4 é formado por 128 bits.

c) Geralmente os dois primeiros bytes do IP representam o número da rede e os dois últimos o número da placa de rede.

d) Para formação do endereço de IPv4 todas combinações são possíveis, não havendo números de IP inválidos.

e) Se o valor do primeiro byte for um número entre 128 e 191, então temos um endereço de IP classe B para o IPv4.

Letra e.

a) Errada. Em uma rede TCP/IP, cada placa de rede existente, em cada computador, é identificada por um número, chamado **endereço IP**. Exemplo de endereço IP: 200.251.137.2.

Esse endereço IP precisa ser único **na rede**, ou seja, não podem existir números duplicados.

Para evitar esta duplicidade na Internet, a distribuição de números IP é **centralizada**.

Na verdade, **o número IP não está associado a cada computador, e sim a cada interface de rede que o computador possui**.

Portanto, se uma máquina possui várias conexões a diversas redes físicas, ela pode ser referenciada por quaisquer desses endereços.

b) Errada. Os endereços IPv6 têm um tamanho de **128 bits.** O número IPv4 é formado por **32 bits**, em que trabalharemos com 4 conjuntos de 8 bits (4 octetos). Os octetos, quando representados, são separados por pontos. Veja abaixo dois exemplos de endereço IP:

0 0 0 0 1 0 1 0. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 1

1 1 0 0 1 0 0 0. 1 1 1 1 1 1 1 1. 1 0 0 0 1 1 1 0. 0 0 0 0 1 0 1 0

Na verdade, a forma mais usual de representação do endereço IP é em números decimais. Essa notação divide o endereço IP em quatro grupos de 8 bits (octeto) e representa o valor decimal de cada octeto binário, separando-os por um ponto. Dessa forma, podemos transformar os endereços acima nos endereços seguintes, respectivamente:

10.0.0.1

200.255.142.10

c) Errada. O **endereço IP é dividido logicamente em duas partes:**

- Parte de **rede**, identificando a rede dentro da Internet.
- Parte do **nó**, identificando uma interface dentro de uma dada rede.

- Classe A: N.H.H.H
  - usa o primeiro octecto como endereço de rede
- Classe B: N.N.H.H
  - usa os dois primeiros octectos como endereço de rede
- Classe C: N.N.N.H
  - usa os três primeiros octectos como endereço de rede

N = Endereço de Rede

H = Endereço de Host

Todos os computadores em uma mesma rede local (fisicamente falando, por exemplo, um mesmo barramento Ethernet) devem ter o mesmo endereço de rede, e cada um deve ter um endereço de host (nó) diferente. Em uma rede doméstica, por exemplo, você poderia utilizar os endereços “192.168.1.1”, “192.168.1.2” e “192.168.1.3”, em que o “192.168.1.” é o endereço da rede (e por isso não muda) e o último número (1, 2 e 3) identifica os três micros que fazem parte dela.

d) Errada. O InterNIC controla todos os endereços IP em uso ou livres na Internet, para evitar duplicações, e reserva certas faixas de endereços chamadas de **endereços privativos** para serem usados em redes que não irão se conectar diretamente na Internet.

e) Certa. Os endereços IPs são divididos em classes como mostra o quadro a seguir:

Classe	1º octeto começa com (em binário)	1º octeto pode ser (em decimal)	Objetivo	Exemplo de Endereço IP
A	0	1 a 126	Grandes redes	**100**.1.240.28
B	10	**128 a 191**	Médias redes	**157**.100.5.195
C	110	192 a 223	Pequenas redes	**205**.35.4.120
D	1110	224 a 239	Multicasting.	Não usado para micros (hosts) individuais.
E	1111	240 a 254	Faixa reservada para fins futuros.	-

Tabela: Detalhes sobre o 1º octeto das classes

Conforme visto, se o valor do primeiro byte for um número entre 128 e 191, então temos um endereço de IP classe B para o IPv4.

Questão 38 (FCC/TRT-16ª REGIÃO/MA/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2014) Atenção: Para responder às questões de números 51 a 53, considere o texto seguinte.

Um Analista de Redes de Computadores deve planejar a instalação física e a configuração lógica de uma rede local de computadores do ambiente de escritório do Tribunal Regional do Trabalho da 16ªRegião. Dentre as especificações recebidas, estão: a área total do escritório é de 200 m^2, a rede deve interligar 30 computadores, o uso dos computadores é para aplicativos típicos de escritório e TRT da 16ª Região contratou o serviço de acesso (provedor) para 100 Mbps.

Após a finalização das escolhas do cabeamento e dos equipamentos, o Analista decidiu configurar logicamente a rede utilizando o conceito de sub-rede na rede local e otimizar o seu

desempenho. Para que a sub-rede criada acomode todos os 30 computadores, a máscara de sub-rede utilizada deve ser:

a) 255.255.255.252

b) 255.255.255.240

c) 255.255.255.224

d) 255.255.255.192

e) 255.255.255.255

Letra c.

Cálculo de sub-rede:

Primeiramente, para acomodar um número de 30 máquinas é necessário gastar 5 bits. **($2^5 = 32$)**

O número máximo possível da máscara é de 256 bits (de 0 a 255). Dessa forma, basta subtrair o número máximo da sub rede ao número de bits necessários: 256 - 32 = 224.

Máscara: 255.255.255.224

Outra maneira de calcular a resposta, vide a seguir:

A fórmula para cálculo de sub-redes é (2^n) - 2, aqui se lê: **dois elevado a n menos dois**. **O menos dois é por causa dos endereços reservados, que não poderão ser utilizados para endereçar hosts.** São eles: o endereço de rede e outro o endereço de broadcast, e **n=bits zero da máscara**.

Se considerarmos n=5, representando 5 bits para endereçar hosts, teremos o cálculo listado a seguir.

Calculando o número total de hosts que podem ser ligados na rede teremos $2^5 – 2 = 32 -2 = 30$. Esse total já resolve o nosso problema, já que o enunciado diz que é necessário ligar 30 máquinas na rede. Assim, para que a sub-rede criada acomode todos os 30 computadores, a máscara de sub-rede utilizada deve ser 11111111.11111111.11111111.11100000, que é 255.255.255.224.

Questão 39 (FCC/AL-PE/ANALISTA LEGISLATIVO/INFRAESTRUTURA/2014) Uma indústria está mudando a sua sede para um novo local com 360.000 m2. No novo local, planeja-se que o data center seja instalado em um prédio diferente daquele onde estarão os usuários.

O data center estará a 540 metros de distância do escritório da empresa, onde estarão as estações dos usuários (desktops e notebooks). Todos os equipamentos servidores, estações e periféricos que serão conectados na rede terão interface física de rede com conector RJ45 e capacidade de transmissão com negociação automática 10/100 Mbps. Os switches e roteadores da rede que tratarão a comunicação entre os nós da LAN poderão ser ligados ao backbone da rede com portas físicas com conector ST e capacidade de transmissão de 1 Gbps. A rede não contará com repetidores. Nesse projeto, deve ser adotado cabeamento

a) coaxial entre os roteadores do data center e os roteadores do escritório e cabeamento em fibra ótica entre os switches e as estações.

b) com par trançado CAT5 entre os roteadores do data center e os roteadores do escritório e cabeamento em fibra ótica entre os switches e as estações.

c) em fibra ótica entre os roteadores do data center e os roteadores do escritório e cabeamento coaxial entre os switches e as estações.

d) em fibra ótica entre os roteadores do data center e os roteadores do escritório e cabeamento em par trançado CAT5 entre os switches e as estações.

e) em par trançado CAT 5 entre os roteadores do data center e os roteadores do escritório e cabeamento em par trançado CAT 1 entre os switches e as estações.

Letra d.

Dentre as assertivas, a que melhor se adequa é a letra D. Deve ser adotado cabeamento em fibra ótica entre os roteadores do data center e os roteadores do escritório e cabeamento em par trançado CAT5 entre os switches e as estações.

Questão 40 (FCC/TRT-1ª/ANALISTA JUDICIÁRIO/ÁREA JUDICIÁRIA/2013) A placa de rede do computador de Paulo tem velocidade de transmissão de 10/100. Isso significa que a transmissão de dados pela rede entre o computador de Paulo e um computador servidor com placa de rede de mesma velocidade pode ser de até

a) 10 megabytes por segundo.

b) 100 megabits por minuto.

c) 1000 megabits por segundo.

d) 100 megabits por segundo.

e) 100 megabytes por segundo.

Letra d.

O 100 megabytes por segundo informa que a velocidade de transmissão é de **10/100**, em que a possibilidade de tráfego máxima é de **100 megabits por segundo**, sendo a opção correta a letra "d".

Questão 41 (FCC/TRE-RN/TÉCNICO JUDICIÁRIO/OPERAÇÃO DE COMPUTADOR/2005) No TCP/IP, o endereço IP 172.20.35.36 enquadra-se na classe:

a) A;

b) B;

c) C;

d) D;

e) E.

Letra b.

Conforme ilustrado no quadro a seguir, a classe B possui um valor decimal no primeiro octeto que irá variar de 128 a 191.

Classe	1º octeto começa com (em binário)	1º octeto pode ser (em decimal)	Objetivo	Exemplo de Endereço IP
A	0	1 a 126	Grandes redes	**100**.1.240.28
B	10	128 a 191	Médias redes	**157**.100.5.195
C	110	192 a 223	Pequenas redes	**205**.35.4.120
D	1110	224 a 239	Multicasting.	Não usado para micros (hosts) individuais.
E	1111	240 a 254	Faixa reservada para fins futuros.	-

Tabela: Detalhes sobre o 1º octeto das classes
Fonte: Quintão (2011)

Explicando em detalhes, se o primeiro octeto (que é um número binário de 8 bits) começar com 0, é sinal de que ele pode ser 00000000 até 01111111 (ou seja, em decimal seria 0 até 127).

No entanto, alguns endereços são reservados pela IANA, instituição responsável pela atribuição dos endereços para cada computador na Internet e não poderão ser utilizados em micros na Internet (nem em redes locais). No contexto dado, temos que o primeiro octeto não pode ser 0 (zero) nem 127 na Internet, portanto iremos excluir os decimais 0 e 127 da relação.

Endereço IP que inicia o primeiro byte com valor decimal **127** é considerado inválido para identificar micros já que esse endereço identifica a própria máquina em si. Assim, uma mensagem de dados destinada a um servidor 127.x.x.x deverá retornar para o emitente.

O endereço **0.0.0.0** é reservado para uso como a rota-padrão do computador.

De acordo com o quadro anterior, o endereço IP 172.20.35.36 enquadrase na classe B.

Nota!

Vamos às dicas para conversão de binário para decimal.

Aqui tem-se a conversão de números da base binária para decimal. Na base binária existem os algarismos 0 e 1. E na base decimal temos os algarismos de 0 a 9. Para o número 11001000. 11111111. 10001110. 00001010 nós devemos realizar a conversão de grupo a grupo de 8 dígitos.

Uma das formas de se realizar essa conversão é a seguinte:

1 – Vamos enumerar as posições do número binário, da direita para a esquerda, e de modo que a posição mais à direita seja a posição 0.

Assim para o número **11001000**, teríamos:

Número em binário	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**
Posição	7	6	5	4	3	2	1	0

2 - Em seguida, operamos o seguinte cálculo:

Sendo:

n, o algarismo em binário;

p, a posição de n;

Faz-se: $n*2^{p}+n_{1*}2^{p1}+n_{2}*2^{p2}+n_{3}*2^{p3}$.

Assim, o número 110001000, ficaria assim:

$0*2^0+0*2^1+0*2^2+1*2^3+0*2^4+0*2^5+1*2^6+1*2^7=$

$= 0 + 0 + 0 + 8 + 0 + 0 + 64 + 128= 200$

Para o número 11111111, teremos:

Listar as posições de cada algarismo:

Número em binário	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
Posição	7	6	5	4	3	2	1	0

(observe que a listagem das posições é sempre da direita para esquerda)

Logo o cálculo fica assim:

$1*2^0+1*2^1+1*2^2+1*2^3+1*2^4+1*2^5+1*2^6+1*2^7=$

$= 1 + 2 + 4 + 8 + 16 + 32 + 64 + 128= 255$

Os mesmos procedimentos acima são executados para os outros dois grupos (10001110. 00001010). E no final, temos que:

11001000 = 200 11111111 = 255 10001110 = 142 00001010 = 10

E, portanto, 11001000. 11111111. 10001110. 00001010 é igual a 200.255.142.10.

Questão 42 (FCC/CEAL/ANALISTA DE SISTEMAS/2005) Na arquitetura TCP/IP:

a) o IP 127.0.0.1 é utilizado para representar máquinas de toda a rede;

b) o IP 10.0.0.1 enquadra-se no padrão classe B;

c) a máscara de rede FFFFFF00 é típica do padrão classe C;

d) o serviço UDP é orientado à conexão;

e) a aplicação FTP também é conhecida pelo nome de Terminal Virtual Remoto.

Letra c.

a) Errada. O endereço de IP 127.0.0.1 é o endereço da própria máquina, também conhecido como endereço de **loopback**.

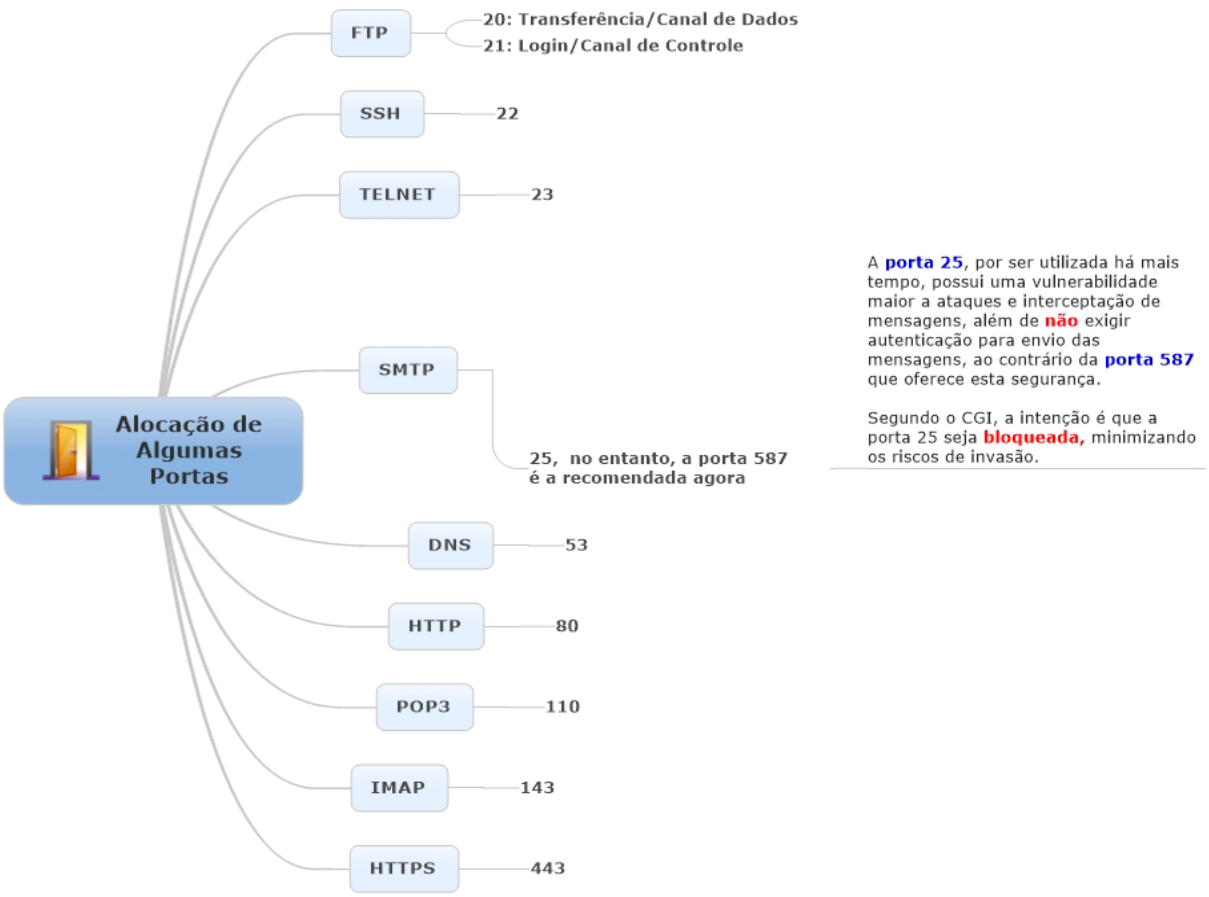
b) Errada. O IP 10.0.0.1 é da classe A.

c) Certa. O endereço FFFFFF00 é a máscara 255.255.255.0 em sistema hexadecimal, que corresponde à classe C.

d) Errada. O protocolo **UDP** (User Datagram Protocol – Protocolo de Datagrama de Usuário) é um protocolo sem conexão, que não verifica a recepção correta das mensagens. Por essa razão, o UDP é mais rápido que o TCP, sendo bastante utilizado, por exemplo, em aplicações multimídias (videoconferência) em que a perda de um quadro não chega a causar sérios problemas.

e) Errada. O protocolo **FTP** (File Transfer Protocol – Protocolo de Transferência de Arquivos) é utilizado na transferência de arquivos entre computadores. Permite recebimento e envio de arquivos, bem como criação e gerenciamento de diretórios no computador remoto. O FTP utiliza 2 portas no protocolo TCP:

- a porta **20** para a efetiva transferência dos dados, e
- a porta **21** para transferência das informações de autenticação (como login, estabelecimento da conexão, senha) e comandos (cópia, exclusão, movimentação de arquivos etc.).



Conforme visto, não está relacionado a terminais virtuais remotos. A resposta à questão é a alternativa “c”!

Questão 43 (FCC/SABESP/ANALISTA DE GESTÃO/ADMINISTRAÇÃO/2018) Um funcionário está usando um computador com o sistema operacional Windows 8, em português, e deseja saber o endereço IP de sua máquina. Para isso, ele deve abrir uma janela de execução do Windows:

a) clicando no botão Iniciar, digitar run seguido de ENTER e, na janela aberta, digitar ipshow seguido de ENTER. O mesmo procedimento é válido no Windows 10

b) clicando no botão Iniciar, digitar cmd seguido de ENTER e, na janela aberta, digitar ipconfig seguido de ENTER. O mesmo procedimento não é válido no Windows 7.

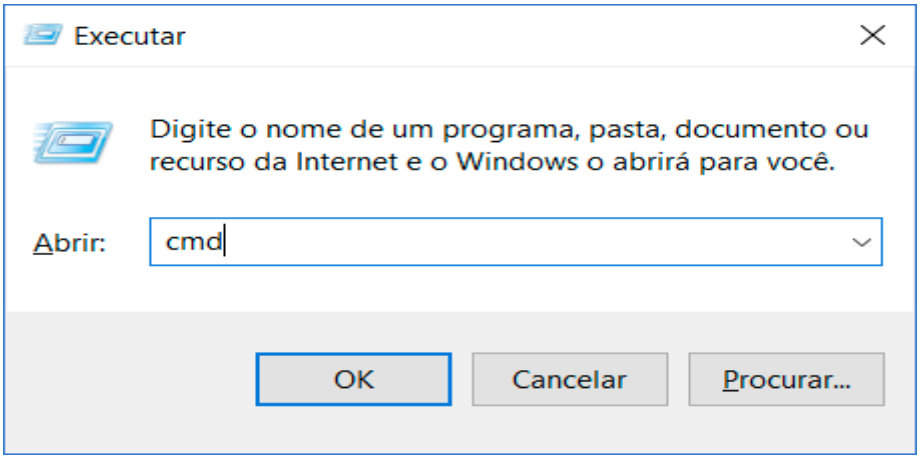
c) pressionando a Tecla do Windows, digitar ipshow -all seguido de ENTER. O mesmo procedimento é válido no Windows 10.

d) utilizando o atalho Tecla do Windows + R, digitar cmd seguido de ENTER e, na janela aberta, digitar ipconfig -all seguido de ENTER. O mesmo procedimento é válido no Windows 7.

e) utilizando o atalho Tecla do Windows + E, digitar run seguido de ENTER e, na janela aberta, digitar ipconfig -all seguido de ENTER. O mesmo procedimento não é válido no Windows 7.

Letra d.

Inicialmente, abra uma janela de execução do **Windows**, com atalho “Tecla do **Windows + R**”. Digite **cmd** e clique no botão **OK** para confirmar a operação.



Veja que uma tela de comando é aberta. Digite **ipconfig –all** e observe que uma série de informações é obtida por meio desse comando, como: endereço IP, máscara de sub-rede, endereço físico do computador (MAC Address) etc.

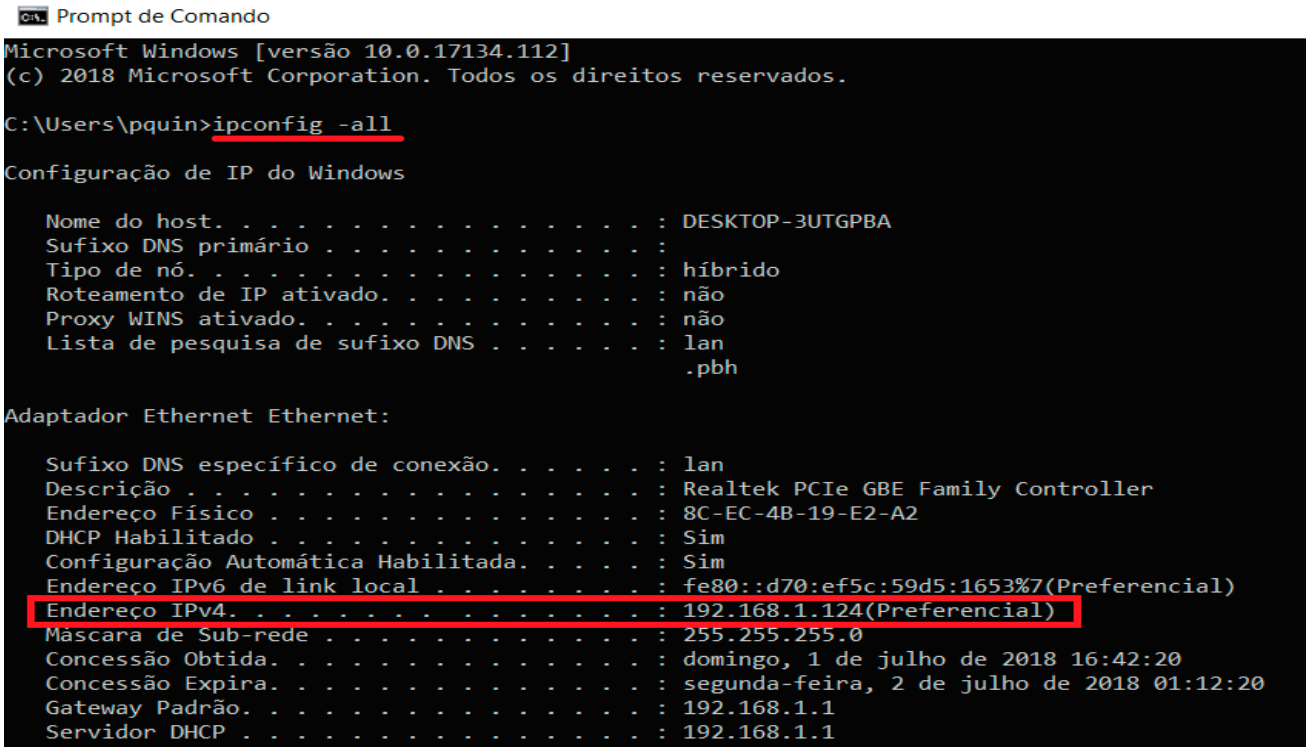


Figura. Extraída do Windows 10. Similar para Windows 8

Questão 44 (FCC/SABESP/TÉCNICO EM SISTEMAS DE SANEAMENTO 01/ELETRÔNICA/2018)

O comando do prompt do windows que exibe e modifica as tabelas de conversão de endereços IP para endereços físicos usadas pelo protocolo de resolução de endereços é:

a) Ping

b) Ipconfig

c) Route

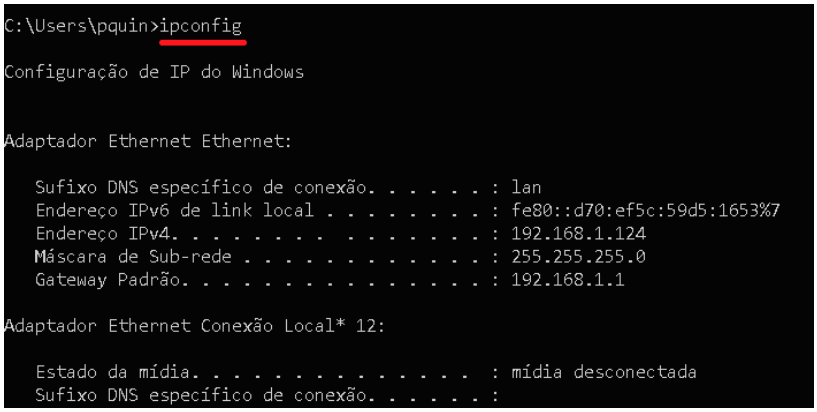
d) Arp

e) Netsh

Letra d.

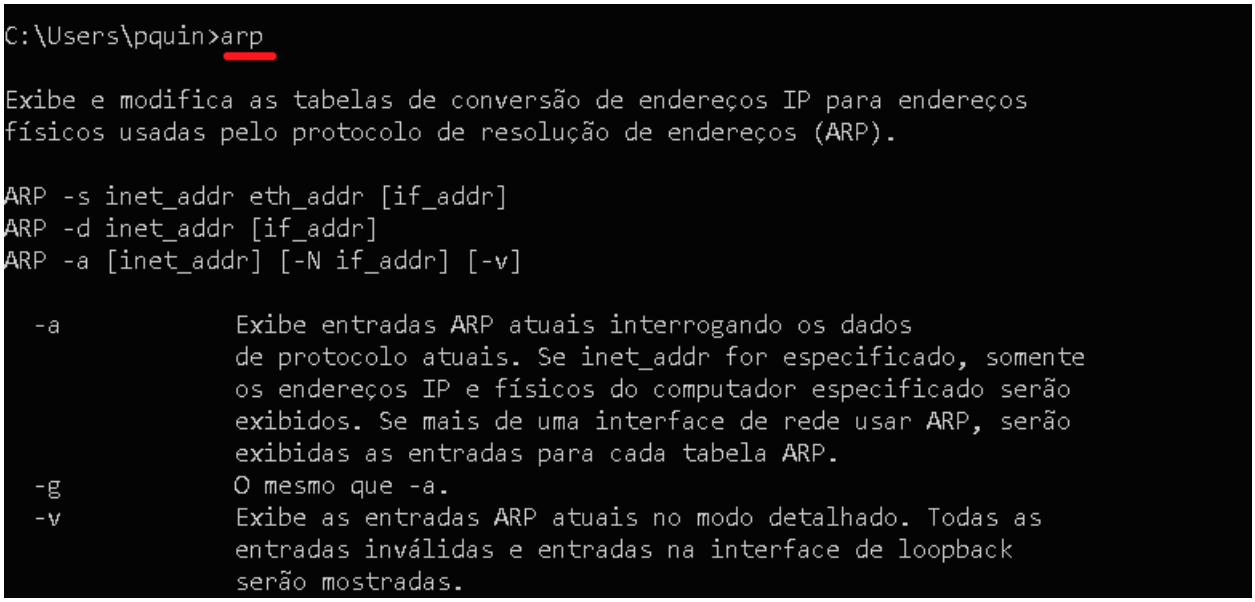
O comando **ping** verifica se há conectividade entre os dispositivos.

O comando **ipconfig** mostra os dispositivos de rede existentes no computador, bem como o respectivo endereço IP que cada dispositivo conseguiu obter, se for o caso.

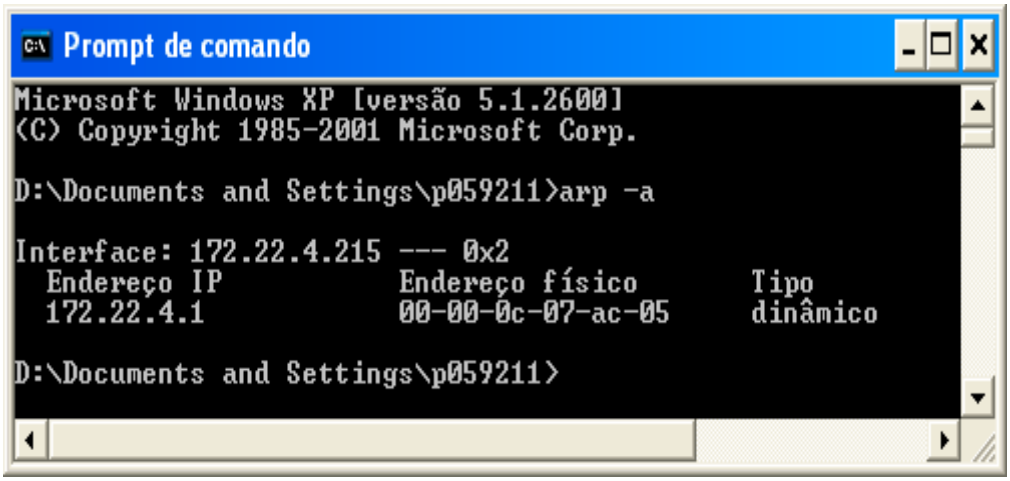


Route manipula as tabelas de roteamento (exibe e modifica a tabela do roteador). Busca traçar a rota e permite verificar qual o ponto, ao longo do caminho, que pode ter alguma retenção e interrupção da comunicação.

O **ARP** (**Address Resolution Protocol**) é responsável por mapear e converter os endereços IP (lógico) em endereços MAC (endereço físico), ou seja, passar do nível da camada de rede para a camada de enlace.



Veja a ilustração abaixo do uso do comando ARP. Com o comando efetuado, verifique que é mostrado o endereço IP da máquina e seu respectivo endereço físico de placa de rede (endereço MAC).



O **netsh** ou **network shell** é um utilitário que permite a configuração local ou remota dos parâmetros de rede. Permite, por exemplo, exibir configuração atual de IP, exibir estado do adaptador sem fio etc.

Veja mais: https://br.ccm.net/faq/1319-comandos-ip-de-redes-no-windows

---

Questão 45 (FCC/SABESP/TÉCNICO EM SISTEMAS DE SANEAMENTO 01/ELETRÔNICA/2018) O cabo UTP para redes 100BASE-TX e 1000BASE-T que suportam frequências de até 100 MHz é classificado como categoria

a) 3.

b) 1.

c) 2.

d) 4.

e) 5e.

Letra e.

Ao comprar um cabo de par trançado, é importante notar qual a sua CATEGORIA: **cat1, cat2, cat3, cat4, cat5, cat5e, cat6, cat7, cat7a, cat 8/8.1/8.2.** Via de regra, **QUANTO MAIOR A CATEGORIA DO CABO, MAIOR A VELOCIDADE COM QUE ELE PODE TRANSPORTAR DADOS**.

- **cat 5:** usado em redes **Fast Ethernet** em frequências de até **100 MHz** com uma taxa de **100 Mbps. (CAT5 não é mais recomendado pela TIA/EIA);**
- **Cat 5e:** é uma melhoria da categoria 5. Pode ser usado para frequências de 100 MHz em redes 1000BASE-T **gigabit ethernet**. Ela foi criada com a nova revisão da norma EIA/TIA-568-B. **(CAT5e é recomendado pela norma EIA/TIA-568-B).**

Nota: 1000BASE-T: utiliza os mesmos cabos de par trançado (categoria 5) usados nas redes Fast Ethernet. Não são necessários ajustes maiores para suportar esta tecnologia, e com a utilização de switches compatíveis a essa tecnologia, podem ser combinados nós de 10, 100 e 1000 Mbps, sem que os mais lentos atrapalhem no desempenho dos mais rápidos. As redes 1000Base-T utilizam os quatros pares disponíveis no par trançado, em vez de apenas dois pares.

Questão 46 (FCC/CÂMARA DOS DEPUTADOS/ANALISTA DE INFORMÁTICA LEGISLATIVA/2007) O padrão de velocidade e cabeamento 1000Base-T caracteriza uma tecnologia de interconexão para redes locais denominada

a) 10Mbit/s Ethernet.

b) 10-Gigabit Ethernet.

c) Gigabit Ethernet.

d) Wireless Ethernet.

e) Fast Ethernet.

Letra c.

A tecnologia **Gigabit Ethernet (802.3z)** é uma evolução das tecnologias Ethernet e Fast Ethernet, que permite a transmissão de dados à velocidade de **1Gbps**. Ela pode operar tanto usando

como no modo half-duplex como no modo full-duplex. Os padrões de meio físico mais comuns para redes Gigabit Ethernet são os seguintes:

- **1000BASE-T**: utiliza os mesmos cabos de par trançado (categoria 5) usados nas redes Fast Ethernet. Não são necessários ajustes maiores para suportar esta tecnologia, e com a utilização de switches compatíveis a essa tecnologia, podem ser combinados nós de 10, 100 e 1000 Mbps, sem que os mais lentos atrapalhem no desempenho dos mais rápidos. As redes 1000Base-T utilizam os quatros pares disponíveis no par trançado, em vez de apenas dois pares;
- 1000BASE-CX: foi o padrão inicial para Gigabit Ethernet. Nela o cabeamento é feito com cabos STP (Par Trançado Blindado), com alcance de até, no máximo, 25m;
- 1000BASE-SX: utiliza fibras ópticas e a distância máxima é de até 550 metros. Pode utilizar fibras do tipo monomodo e multimodo, sendo a mais comum a multimodo (mais barata e de menor alcance);
- 1000BASE-LX: tecnologia mais cara, pois atinge as maiores distâncias. Ela é capaz de atingir 550m, com o uso de fibras ópticas multímodo, e até 5km, com o uso de fibras ópticas monomodo.

O padrão **Gigabit Ethernet** utiliza a interligação por meio de hubs ou switches, formando uma topologia física em estrela.

Questão 47 (FCC/TRT-9ª REGIÃO/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2010) O cabo par trançado tradicional de categoria 5 é composto de

a) um par de fios.
b) dois pares de fios.
c) três pares de fios.
d) quatro pares de fios.
e) cinco pares de fios.

Letra d.

O par trançado tradicional (categoria 5) possui quatro (4) pares de fios de cobre, os quais são trançados entre si para criar uma blindagem eletromagnética, de modo a proteger as trans-

missões de interferências externas e minimizar a necessidade de usar blindagem física. No entanto, opera apenas com 4 fios (dois conjuntos de par trançado).

Questão 48 (FCC/TRT-9ª REGIÃO/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2010) Quanto ao tipo de rede, considere:

I – Ethernet Padrão (10 Mbps).

II – Gigabit Ethernet (1 Gbps).

III – Fast Ethernet (100 Mbps).

IV – 10G Ethernet (10 Gbps).

Com referência ao cabo par trançado, considere:

1) um par de fios.
2) dois pares de fios.
3) três pares de fios.
4) quatro pares de fios.
5) cinco pares de fios.

Quanto ao uso da quantidade de par de fios do cabo na rede, é correta a associação

a) I-1, II-2, III-3 e IV-4.

b) I-2, II-3, III-4 e IV-5.

c) I-2, II-4, III-2 e IV-4.

d) I-3, II-3, III-4 e IV-4.

e) I-3, II-4, III-4 e IV-5.

Letra c.

I – Ethernet Padrão (10 Mbps) = 2 pares de fios.

II – Gigabit Ethernet (1 Gbps) = 4 pares de fios.

III – Fast Ethernet (100 Mbps) = 2 pares de fios.

IV – 10G Ethernet (10 Gbps) = 4 pares de fios.

Questão 49 (FCC/TRT-MG/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2005)

Em relação ao padrão ETHERNET, considere os Itens abaixo:

I – Cabo Coaxial Fino

II – Fast Ethernet

III – Gigabit Ethernet

IV – 10 Gigabit Ethernet

I, II, III e IV referem-se, respectivamente:

a) 10Base5, 100BaseT, IEEE802.3g, IEEE702.3ae

b) 10Base5, 100BaseX, IEEE802.3g, IEEE802.3gg

c) 10Base5, 10BaseX, IEEE802.3ae, IEEE802.3z

d) 10Base2, 100BaseT, IEEE802.3z, IEEE802.3ae

e) 10Base2, 100BaseG, IEEE802.3ae, IEEE802.3z

Letra d.

Cabo Coaxial Fino está relacionado a 10 Base 2. Portanto, já podemos eliminar as assertivas "a", "b" e "c". Não existe a tecnologia 100BaseG, o que já elimina a letra "e". Nesse caso, a resposta é a letra "d". Aqui temos:

10 Base 2 – utiliza cabo coaxial fino;

100 Base T – suporta o padrão Fast Ethernet;

IEEE802.3z – 1000BASE-X Gbit/s Ethernet usando fibra ótica a 1 Gbit/s (125 MB/s);

IEEE802.3ae – 10 Gbit/s (1,250 MB/s) Ethernet usando fibra ótica.

Questão 50 (FCC/DETRAN-MA/ASSISTENTE DE TRÂNSITO/2018) Atualmente, o acesso à internet é realizado por meio de uma estrutura composta tipicamente por um provedor de acesso à internet, um Modem/roteador de acesso ao provedor, um Access Point/roteador sem fio Wi-Fi (802.11g) e um computador portátil. Com relação à comunicação Wi-Fi, é correto afirmar que

a) utilizar o WEP é mais seguro que a comunicação por cabo de par trançado.

b) permite o acesso à internet, mas não à intranet.

c) possui velocidade de transmissão maior que um cabo de par trançado Categoria 5.

d) opera na frequência de 2,4 GHz, ou seja, micro-ondas.

e) opera na mesma frequência dos telefones sem fio, ou seja, 900 MHz.

Letra d.

A transmissão em uma rede sem fio é feita através de ondas eletromagnéticas, que se propagam pelo ar e podem cobrir áreas na casa das centenas de metros.

a) Errado. WEP (Wired Equivalency Privacy - sigla de "Privacidade Equivalente à de Redes com Fios") foi a primeira tentativa de se criar um protocolo eficiente de proteção de redes WI-FI em 1997. Hoje é um protocolo obsoleto no quesito segurança. WPA (Wi-Fi Protected Access - sigla de "Acesso Protegido a Wi-Fi") é um subconjunto dos padrões 802.11i, e serviu como um padrão de "transição" entre o WEP e o WPA2. O WPA2 segue o **padrão 802.11i** e **substitui formalmente o WEP**. Assim, é mais seguro do que o WEP!

b) Errado. Wi-Fi permite o acesso a qualquer rede, incluindo a Internet, intranet etc.

c) Errado. O cabo de par trançado categoria 5 pode suportar até 100Mbps, enquanto o padrão 802.11g alcança até 54Mbps.

d) Certo. O padrão 802.11g opera na frequência de 2,4 GHz, exatamente a mesma frequência das ondas de rádio liberadas no uso de micro-ondas. Tecnologias mais novas, como o 802.11 a, 802.11n utilizam 5GHz.

e) Errado. Opera na frequência de 2,4 GHz.

REFERÊNCIAS

ALBUQUERQUE, F. **TCP/IP – Internet: Protocolos & Tecnologias**. 3 ed. Rio de Janeiro: Axcel Books do Brasil Editora Ltda. 2001.

AZURE. **LAN, WLAN, MAN, WAN, PAN: conheça os principais tipos de redes.** Disponível em: <https://azure.microsoft.com/pt-br/overview/what-is-cloud-computing/>. Acesso em: 21 jul. 2019.

BARRÉRE, E. **Fundamentos de Redes de Computadores**. Apostila Licenciatura em Computação. 2011.

Cisco, **CCNA Exploration** v. 4.0, 2010.

INFOTECNEWS. **Modelo TCP/IP – Definição, camadas e funcionamento**. Disponível em: <http://infotecnews.com.br/modelo-tcpip/>. Acesso em: 09 jun. 2019.

KUROSE, James F. **Redes de Computadores e a Internet**: uma abordagem top-down. 5a ed. São Paulo: Addison Wesley, 2010.

MAIA, L. P. **Arquitetura de Redes de Computadores**, LTC, 2009.

QUINTÃO, P. L. Informática-**FCC-Questões Comentadas e Organizadas por Assunto**, 2014. 3ª. Edição. Ed. Gen/Método.

QUINTÃO, P. L. **Informática-1001 Questões Comentadas – Cespe/UnB**, 2017. 2ª. Edição. Ed. Gen/Método.

QUINTÃO, P. L. **Informática para Concursos.** 2020**.**

QUINTÃO, P. L. **Tecnologia da Informação para Concursos.** 2020**.**

TANENBAUM, A. S. **Redes de Computadores,** *4ª. edição, 2003.*

COMER, D. E. **Interligação de Redes com TCP/IP**. Campus, 2006.

STEVENS, W. R. **TCP/IP Illustrated** – Vol. 1. Addison-Wesley Professional. 1994.

PROJETOS DE REDES. Disponível em: <http://www.projetoderedes.com.br/>. Acesso em: 20 jun. 2018.

TELECO. Disponível em: <http://www.teleco.com.br/>. Acesso em: 20 jun. 2018.

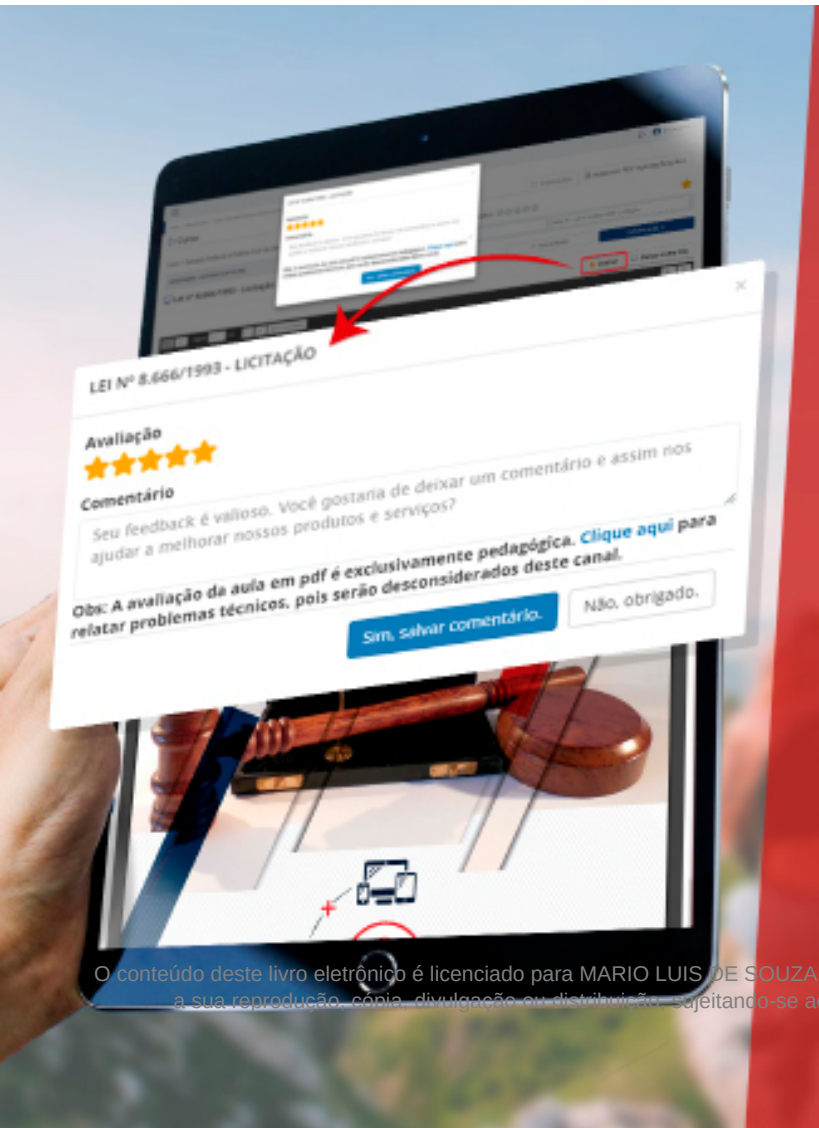
Patrícia Quintão

Mestre em Engenharia de Sistemas e computação pela COPPE/UFRJ, Especialista em Gerência de Informática e Bacharel em Informática pela UFV. Atualmente é professora no Gran Cursos Online; Analista Legislativo (Área de Governança de TI), na Assembleia Legislativa de MG; Escritora e Personal & Professional Coach.
Atua como professora de Cursinhos e Faculdades, na área de Tecnologia da Informação, desde 2008. É membro: da Sociedade Brasileira de Coaching, do PMI, da ISACA, da Comissão de Estudo de Técnicas de Segurança (CE-21:027.00) da ABNT, responsável pela elaboração das normas brasileiras sobre gestão da Segurança da Informação.
Autora dos livros: Informática FCC - Questões comentadas e organizadas por assunto, 3ª. edição e 1001 questões comentadas de informática (Cespe/UnB), 2ª. edição, pela Editora Gen/Método.
Foi aprovada nos seguintes concursos: Analista Legislativo, na especialidade de Administração de Rede, na Assembleia Legislativa do Estado de MG; Professora titular do Departamento de Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia; Professora substituta do DCC da UFJF; Analista de TI/Suporte, PRODABEL; Analista do Ministério Público MG; Analista de Sistemas, DATAPREV, Segurança da Informação; Analista de Sistemas, INFRAERO; Analista - TIC, PRODEMGE; Analista de Sistemas, Prefeitura de Juiz de Fora; Analista de Sistemas, SERPRO; Analista Judiciário (Informática), TRF 2ª Região RJ/ES, etc.

@coachpatriciaquintao
/profapatriciaquintao
@plquintao
t.me/coachpatriciaquintao

ANOTAÇÕES

ANOTAÇÕES



NÃO SE ESQUEÇA DE AVALIAR ESTA AULA!

SUA OPINIÃO É MUITO IMPORTANTE PARA MELHORARMOS AINDA MAIS NOSSOS MATERIAIS.

ESPERAMOS QUE TENHA GOSTADO DESTA AULA!

PARA AVALIAR, BASTA CLICAR EM LER A AULA E, DEPOIS, EM AVALIAR AULA.

AVALIAR