Apostila de Redes

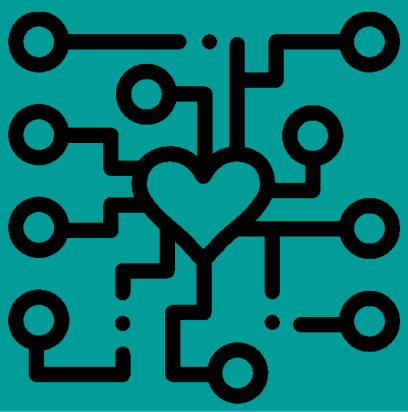
Versão 3/2021

Bruno Michel Pera

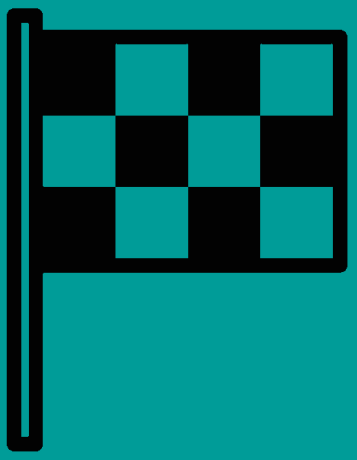
APOSTILA DE REDES, UNIVERSIDADE DO VALE DO PARAÍBA

HTTPS://WWW.UNIVAP.BR/COLEGIOS

Versão 3, Janeiro 2021



Sumário



1. Introdução

1.1 Quem está me ensinando?

Ao se iniciar um curso, seja ele remoto ou presencial é sempre importante conhecer a pessoa que irá te ensinar, para analisar a qualidade do curso que será ministrado. Mesmo se tratando de uma apostila virtual é no mínimo, interessante, conhecer a pessoa que a escreveu, por isso um breve resumo do autor deste livro virtual.

Meu nome é Bruno Michel Pera, sou formado em Engenharia da Computação pela Universidade do Vale do Paraíba e curso mestrado em Inovação Tecnológica na Universidade Federal de São Paulo. Abaixo está disposto algumas de minhas redes socias das quais vocês poderão manter contato caso seja necessário.

- https://www.univap.br/universidade.html
- http://lattes.cnpq.br/4209017189513990
- https://www.linkedin.com/in/bruno-michel-565b3a184/
- bruno.pera@univap.br

Caso haja algum problema com o conteúdo do curso ou queira deixar alguma dica ou sugestão, ficará bem mais facil entrar em contato.

Também vou deixar disponível algumas publicações já realizadas, caso tenham interesse em saber como trabalho.

- PERA, B. M.; LEMES, D. C. M. ; DOMINGOS, J. M. ; MARTINS, R. S. . VIDAINTELIGENTE: MONITORAMENTO REMOTO, PRONTUÁRIO ELETRÔNICO E E-HEALTH. 2020. (Apresentação de Trabalho/Congresso).
- João Victor Pereira Santos. Aplicativo que utiliza tecnologia híbrida para o aprendizado da língua inglesa. 2018. Iniciação Científica. (Graduando em Técnico em Informática) - Universidade do Vale do Paraíba. Orientador: Bruno Michel Pera.
- Carolina de Oliveira Rodrigues. Sitema de Automação Residencial/Empresarial Internet of Things. 2019. Iniciação Científica. (Graduando em Técnico Eletrônica) - Universidade do Vale do Paraíba. Orientador: Bruno Michel Pera.
- Gabriel Cunha Olopes. Desenvolvimento de Drones de Comunicação Híbra para Reconhe-

cimento com Visão Computacional. 2020. Iniciação Científica. (Graduando em Técnico Eletrônica) - Universidade do Vale do Paraíba. Orientador: Bruno Michel Pera.

1.2 O que estou recebendo?

Esta apostila não substitui as aulas presenciais, funciona apenas como um guia do conteúdo que irá ser visto durante o ano. Reforço que **não há necessidade de imprimir** a versão virtual ficará disposta 24h por dia, sete dias por semana durante o ano de 2021. Todo conteúdo até o final do ano está documentado aqui, lembrando que funcionará como um norte a ser seguido.

1.3 Ementa do curso de Redes

Abaixo segue a ementa do curso para o ano de 2021, será destacado todo o conteúdo que irá ser passado, todas as referências ficarão dispostas no capítulo final chamado **Referências**. Lembrando que os livros seguidos não são para livre distribuição e caso deseje utilizar algo deverá pedir permissão ao referido autor.

EMENTA

- Definições. Conceito de localidade. Componentes básicos de redes: servidor, terminais, cabos, software, placas, router, gateway, bridge, hub, switch.
- Equipamentos *smart*
- Topologias em estrela, anel, barra e híbrida.
- Modelo ISO/OSI de 7 camadas e TCP/IP de 5 camadas.
- NetBeui, IPX, TCP/IP, Aplicativos: Ping, FTP, Telnet, Tracert, DNS, DHCP e outros.
- Introdução. Benefícios. Tecnologia. Funcionamento e aplicações. Estratégias e equipamentos para conexão.
- Fundamentos da segurança da informação. Princípios da política de segurança. Classificação das informações e sua relação com as tecnologias das redes. Controles de acesso físico e de acesso lógico.
- Levantamento de requisitos. Identificação de serviços e da infra-estrutura física. Estabelecimento dos critérios de segurança. Implantação da hierarquia entre usuários. Layout e distribuição dos nós da rede. Seleção das tecnologias e dos sistemas operacionais.

Nesta ementa também está prevista laboratórios técnicos para crimpagem de cabos, teste de equipamentos que possuem Internet das Coisas e laboratórios para testes de segurança.

2. Redes de computadores

2.1 O que são redes de computadores?

O que conhecemos hoje como rede de computador surgiu primeiramente como um projeto de defesa durante o período da Segunda Guerra Mundial esse projeto recebeu o nome de ARPANet. A ideia da ARPANet era que a informação de sigilosa não ficasse concentrada em única localidade, pois, se fosse atacada os dados seriam destruídos para sempre. O princípio básico é que os pontos que recebessem essa rede funcionariam como células conectadas então se uma região fosse atacada, a região seguinte possuíria as informações;

O artigo original pode ser acessado através da url *http://docplayer.net/4288280-Multiple-computer-networks-and-intercomputer-communication-lawrence-g-roberts-advanced-research-projects-agency-washington-d-c.html?fbclid=IwAR1TsnUHJzWxBolF0NnbZlmaNnmroTRHvYFFXSZCefBvnzloXbN8RMhlEoE* em inglês. Com o final da Segunda Guerra Mundial, os EUA percebeu que tinha uma tecnologia com extremo potencial em mãos e começaram os processos de disseminação da ARPANet, a princípio para organizações militares, depois universidades e empresas e por fim a todo o público dando inicio a nossa tão amada internet.

Uma rede de computador moderna pode ser caracterizada, por haver uma máquina chamada cliente, uma máquina chamada servidor conectadas por um meio de comunicação.Porém a matéria de redes não se limita apenas os PCs (*Personal Computers*). Por mais que quando se fala em redes pensamos em conexão na via internet, outros meios também podem ser considerados redes de computadores, como por exemplo, uma conexão *bluetooth* a conexão de cabo entre o *mouse* e seu computador, uma conexão de rádio frequencia e um *drone* por exemplo. Existem diversos meios de conexão e todos eles serão vistos durante o curso.

2.1.1 Componentes básicos de Redes e Formas de Comunição

Uma rede de computador é composta pelos seguintes itens, esta rede pode sofrer alguma mudança para sua conexão, porém, a grosso modo estes são os equipamentos necessários.

- Um roteador ou um HUB ou um SWITCH
- Um equipamento com placa de rede, essa podendo ser com fio ou sem. Este equipamento é

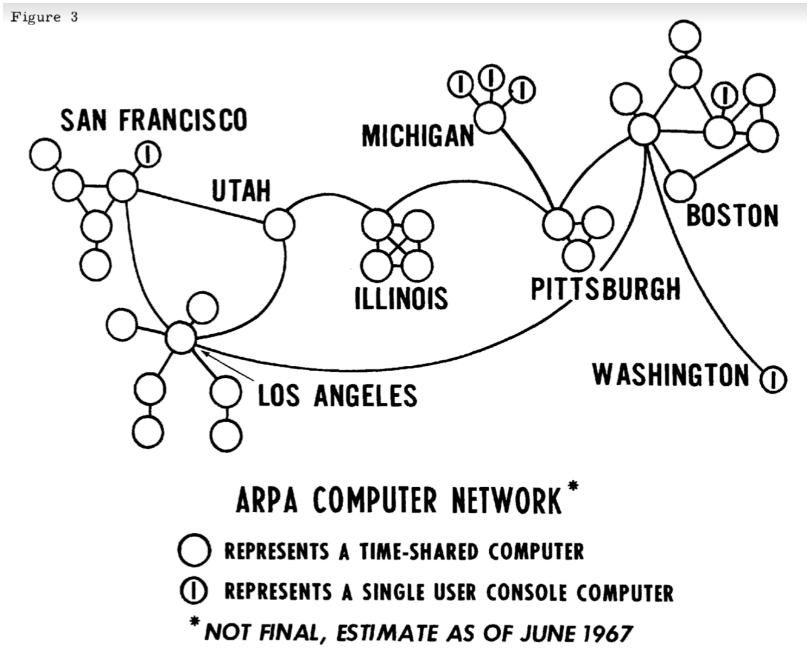


Figura 2.1: ARPANet rede inicial, https://bit.ly/3fJLY0l

chamado de cliente.
- Um banda de comunicação - Neste caso o provedor de internet.
- Uma topologia
- Um Gateway

Muitas dessas palavras podem ser novas para você, não se preocupe pois elas serão explicadas mais a frente no seu devido tempo, porém precisamos também definir alguns conceitos para que seja mais fácil o entendimento dos próximos conteúdos. Entre eles podemos destacar a palavra **protocólo** que será mencionada diversas vezes durante o texto, entenda protocólo como se fosse uma **regra** a qual o pacote de informação tem que obedecer para que seja entregue. Outra palavra que você irá ler muito nesses primeiros textos é o **IP** que vem de *Internet Protocol* este protocólo nada mais é do que o registro na internet, como se fosse seu CPF, um conjunto numérico que é capaz de te identificar. Não se preocupe quanto a essas palavras pois teremos aulas dedicadas a protocólos e IP.

Deve ter em mente é que tudo que passa na frente do seu computador nada mais é do que um conjunto de 0 e 1, esse conjunto recebe o nome de **bit** um acrônimo para *BInary DigiT*. O conjunto desses bits forma uma mensagem essa mensagem recebe o nome de **pacote** dentro do mundo de redes. O roteador que conhecemos ou HUB ou SWTICH recebem o nome genérico de **concentrador**.

2.1.2 UNICAST, MULTICAST e BROADCAST

Quando se fala de transmissão de pacotes em redes de computadores, é preciso levar em conta de qual maneira essa informação será transmitida,esses pacotes respeitam três meios de comunicação. Eles são o **UNICAST**, **MULTICAST** e o **BROADCAST**.

- UNICAST - Meio de transmissão no qual o pacote é enviado diretamente de um destino

para uma origem ignorando quaisquer outras máquinas que estejam conectadas a rede de computadores.Também conhecida como transmissão ponto a ponto.O Unicast é o sistema de roteamento mais comum usado na internet, com cada nó atribuído à um endereço IP exclusivo. Os roteadores identificam a origem e destino dos dados e determinam o caminho mais curto (ou o mais viável) para o envio dos pacotes de dados. Os dados são entregues entre roteadores até que ele chegue ao seu destino final.

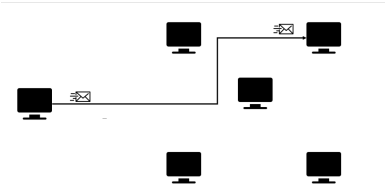


Figura 2.2: UNICAST, Fonte: O autor

- MULTICAST - Comunicação na qual um quadro é enviado para um grupo específico de dispositivos ou clientes. Os clientes da transmissão multicast devem ser membros de um grupo multicast lógico para receber as informações. Um exemplo de transmissão multicast é a transmissão de vídeo e de voz associada a uma reunião de negócios colaborativa, com base em rede. Ao invés de ser enviado para um único destino (endereço IP específico), o tráfego de multicast, permite o envio de informações para um determinado grupo de clientes, cada um com um endereço IP diferente, ao mesmo tempo. O Multicast não é normalmente usado pelos roteadores de Internet, é comum sua utilização em ambientes de redes corporativas, afim de entregar o tráfego sem o uso de uma enorme quantidade de largura de banda

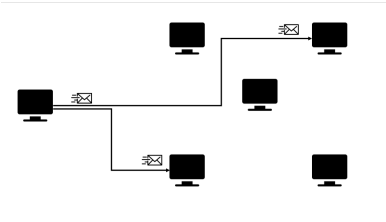


Figura 2.3: MULTICAST, Fonte: O autor

- BROADCAST - Comunicação na qual um quadro é enviado de um endereço para todos os outros endereços.Nesse caso, há apenas um remetente, mas as informações são enviadas para todos os receptores conectados. A transmissão de broadcast é essencial durante o envio da mesma mensagem para todos os dispositivos na rede local. Um exemplo de transmissão de broadcast é a consulta de resolução de endereços que o Protocolo de Resolução de Endereços (ARP, Address Resolution Protocol) envia para todos os computadores em uma rede local. Uma maneira de ser possível sempre identificar o meio de transmissão *Broadcast* é lembrar de filmes que mostram os jornais americanos neles sempre há a informação de "Broadcasting News"o que significa que a informação deve ser disseminada para o maior número possível de pessoas.

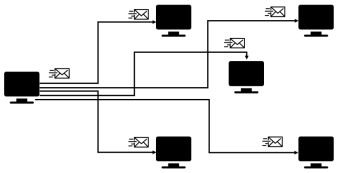


Figura 2.4: BROADCAST, Fonte: O autor

2.2 HUB, SWITCH, Roteador, BRIDGE, Repetidor e Gateway

A informática gosta de se apossar de termos que não são deles, muitos destes ao se procurar na literatura, fora do contexto de informática você irá se deparar com outro significado. Estes são equipamentos físicos que se compram em lojas e servem para que haja a distribuição do sinal de internet, nos tópicos a seguir iremos discutir um pouco sobre eles.

2.2.1 HUB - Concentrador não gerenciavel

A palavra **HUB**, se for traduzida do inglês para o português direto significa “CUBO” ou a peça em que se encaixa os raios de uma bicicleta. Na aviação a palavra HUB significa um aeroporto aonde os passageiros embarcam, desembarcam e fazem conexões, um exemplo é o hub de Guarulhos que é conhecido como GRU. Então podemos ter em mente que o HUB significa conexões ou múltiplas conexões! A área de tecnologia da informação absorveu esse significado então um HUB é uma peça física (*hardware*) que realiza conexão de computadores de uma rede e possibilita a transmissão de informações entre essas máquinas. Ele recebe o nome de concentrador "burro"ou não gerenciável justamente pela sua falta de capacidade de distrubir pacotes paralelos, ou ao menos lidar com eles.

Figura 2.5: Hub Linkbuilder Superstack, Fonte: encurtador.com.br/muIL7

Porém o HUB possui algumas desvantagens em relação aos demais componentes, o HUB não é capaz de lidar com multiplos pacotes ao mesmo tempo, o que significa que ao receber duas mensagem em um mesmo intervalo de tempo ele simplesmente irá destruir as duas mensagens e elas não serão entregues. Outra desvantagem é referente a questão da segurança, que ao enviar um pacote para um destinatário ele encaminha o pacote a todos os outros equipamentos da rede e espera que

eles neguem a informação e que somente o responsável o aceite. De forma geral é isso que acontece, entretanto ao entregar o pacote a uma máquina que não era o destino você abre uma brecha para que essa informação seja lida, existem muitas técnicas de ataque que são capazes de ler esses pacotes entre elas podemos destacar o *Man in the Middle* ou MITM, ataque este que lê os pacotes nas redes.

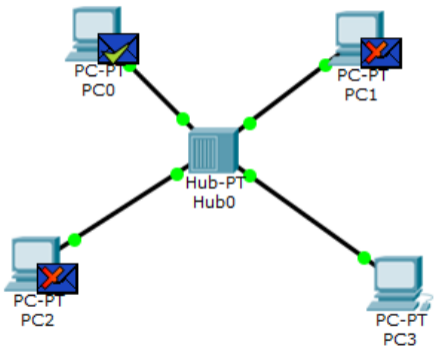


Figura 2.6: Funcionamento do HUB, Fonte: O autor

O fato de não ser um equipamento seguro o coloca como uma das opções menos viáveis para as empresas de grande porte que geralmente possuem dados sigilosos e sensíveis e que tal acesso não pode ser aberto. Mas algumas empresas quando colocam o funcionário sobre investigação costumam usar o HUB para que seja possível identificar os pacotes e ver o que está sendo enviado.

2.2.2 SWITCH - Concentrador Gerenciavel

SWITCH, são equipamentos de redes, assim como os HUBs eles são considerado concetradores e distribuem os pacotes para os computadores neles conectados, possuem normalmente de 4 a 255 portas para conexão de internet, conforme mais portas mais elevado é o valor. Ao contrário do HUB o SWITCH é capaz de lidar com multiplos pacotes paralelamente, ou seja, caso o concetrador receba mais de um pacote ele consegue manejar e distribui-lo na rede sem que haja perda de dados. Uma outra vantagem em relação ao HUB é que as informações são entregues diretamente ao destinatário o que significa que o pacote não passa por todos os equipamentos na rede antes de ser entregue, o que garante um aumento de confiabilidade na rede. Se um pacote demora a ser transmitido, não interfere tanto no desempenho da rede, viso que muitos outros pacotes estão sendo transmitidos em paralelo. Em redes empresariais onde há um grande tráfego de dados, a utilização de um switch ao invés de um hub é altamente recomendável.

Mas existem algumas desvantagens que valem a pena mencionar, tais como a rota de entrega, todo pacote tem uma rota de entrega, vamos fazer uma analogia a um carteiro, um carteiro novo que começou a pouco tempo não conhece as casas que normalmente ele entrega a informação, e normalmente ele não utiliza a rota mais otimizada partindo apenas para rota que pode ser a mais longa. No SWITCH é a mesma coisa o pacote irá passar por algumas rotas pré-definidas, aqui entende-se como rota por quais SWITCHs ou roteadores o pacote irá passar e toda troca de um roteador para o outro é chamado de *HOP* ou salto em português, e essas rotas podem levar mais tempo. Por mais que a tecnologia esteja já disseminada não podemos considerar o SWITCH como

Figura 2.7: Switch D-LINK 52 Portas, Fonte: https://bit.ly/3o1pr49

um equipamento barato, conforme maior o número de portas e opções de gerenciabilidade, maior será o valor, podendo chegar na casa dos milhares de reais. Podendo, inclusive haver equipamentos não disponíveis no Brasil depedendo de uma importação o que gera um custo ainda mais elevado.

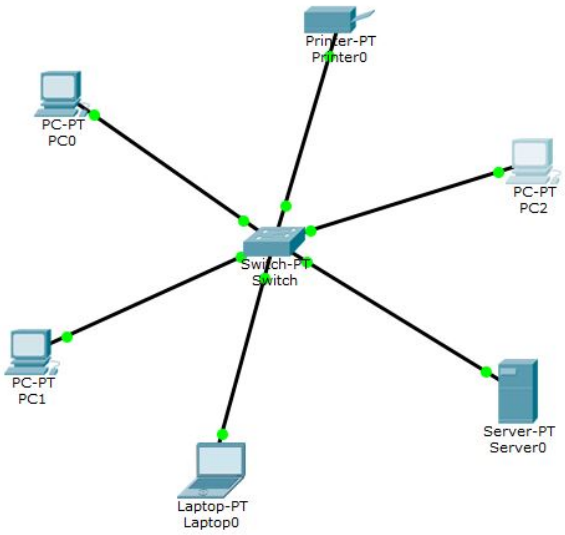


Figura 2.8: Funcionamento do Switch, Fonte: O autor

No geral os concentradores gerenciáveis são utilizados de forma conjunta com os roteadores, que iremos falar mais a frente no curso. Acabam sempre trabalhando em um sistema *master-slave*no qual o roteador fica responsável por toda a parte de rota e saltos e o Switch fica responsável apenas pela entrega dos pacotes.

2.2.3 Roteador

Roteador, pode ser considerado o equipamento mais inteligente de uma rede doméstica, após o computador, pois dentro do roteador existem algoritmos – códigos programados – que são capazes de tratar os pacotes de informações recebidos, lembrando que são vários pacotes ao mesmo tempo.

Cada pacote de informação recebido pelo roteador tem um endereço IP e uma porta destino. O roteador recebe cada pacote e encaminha para o IP de destino, de acordo com regras pré-definidas. Isto é chamado de redirecionamento de portas. Além, disso, muitos roteadores possuem firewall internos aumentando significativamente segurança da rede e também a complexidade e configuração. O Roteador de longe é o melhor equipamento para uma rede, tanto doméstica quanto empresarial obviamente um roteador dedicado a empresas será mais caro e haverá muito mais opções de configuração mas não é raro em empresas de pequeno e médio porte haver roteadores domésticos, uma vez que eles cumprem bem o papel.

Figura 2.9: Roteador Corporativo Cisco RV160W, Fonte: https://bit.ly/34WpeHW

O roteador geralmente não possui além de quatro ou cinco portas uma vez que ele trabalha nativamente com switch, podendo assim ampliar sua capacidade. É possível também ligar roteador dentro de roteador o que gera o chamado Cascateamento de Roteadores, assim como acontece quando trabalha com switch é necessário adicionar uma permissão de *master-slave* onde o roteador instrui pacotes ao outro roteador.

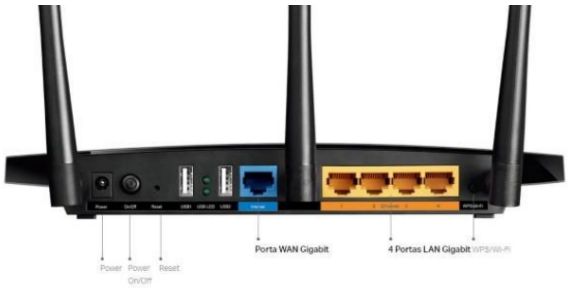


Figura 2.10: Roteador TP LINK, Fonte: O autor

Além de ser responsável por fazer a rota mais curta o roteador também faz a rota mais segura, ou seja, se durante a transmissão de algum pacote de informação algum outro roteador ficar em modo *off-line* o roteador anterior poderá remanejar a rota em sacrifício do tempo.

2.2.4 Bridge

Bridge, nada mais são do que os SWITCHS que descrevemos anteriormente, ou melhor, é um nome moderno para as Bridges. São exatamente a mesma coisa que um switch a única diferença é que a bridge possui apenas três entradas que serve para conectar duas redes, que podem estar separadas. Possuem as mesmas vantagens e desvantagens e são utilizado da mesma maneira. A partir daqui não haverá mais distinção entre brigde e swtichs.

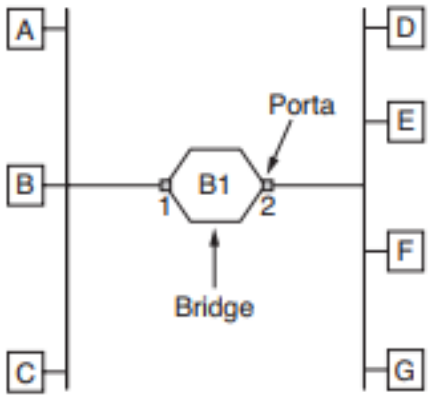


Figura 2.11: Bridge conectando duas redes, Fonte: Redes de computadores, TANENBAUM. 5ªEd. Pág. 209

Podemos concluir que bridge (ponte do inglês) como um equipamento de hardware que une duas redes com protocolos distintos , uma rede Linux com uma rede Windows, assim permitindo que elas troquem pacotes de informação e compartilhem recursos. É exatamente a mesma coisa que um switch, na realidade, definimos uma bridge como um switch com menos portas.

2.2.5 Repetidores

O sinal de internet, tanto o sem fio quando com fio devido a distância e fatores externos, como campos magnéticos ou obstrução das ondas de rádio pode e com toda certeza irá sofrer degradação, o que vai proporcionar uma baixa qualidade de sinal, um mau desempenho ou até mesmo a ausência de conexão. Para isso os repetidores permitem aumentar o sinal entre dispositivos de uma rede com o proposito de aumentar a distância entre os equipamentos, seja ela cabeada ou sem fio.

O repetidor é capaz de amplificar as ondas eletromagnéticoas oriundas de uma rede sem fio ou ligar dois segmentos de redes distintos, por exemplo, um segmento que utiliza um cabo de cobre e um segmento que utiliza um cabo de fibra óptica.

2.2.6 *Gateways*

Um *gateway* de rede é um dispositivo que permite a comunicação entre redes. De um modo genérico podemos classificar os gateways em dois tipos: os gateways conversores de meio e os tradutores de

Figura 2.12: Repetidor TP Link TIWa, Fonte: https://bit.ly/3hAFu6l

protocolos. Os gateways conversores de meio são os mais simples. Como funções básicas estão: receber um pacote do nível inferior, tratá-lo (ler cabeçalho, descobrir roteamento, construir um novo pacote inter-redes) e enviá-lo ao destino.

2.3 Meios de transimissão de dados

Os meios de transmissão de dados em uma rede de computadores são responsáveis pela troca de informação (bits) entre os dispositivos que compõe uma rede. Em outras palavras são a parte física da rede. Diversos equipamentos podem ser utilizados para fazer a comunicação de uma rede, alguns já foram citados em seções anteriores, como uma placa de rede, um roteador, entre outros. Nesse capítulo abordaremos três tipos de meios de transmissão bastante usuais no contexto das redes de computadores: as redes cabeadas (cabos de par trançado e fibra óptica) e as redes sem-fio (wireless). Cada uma delas possui suas vantagens e desvantagens (como custo, viabilidade, velocidade, preço de implantação e manutenção) que precisam ser pensadas antes de implementá-las, analisando o custo/benefício e real necessidade de cada ambiente.

2.3.1 Cabos Coaxiais

Utilizados em redes de computadores antigas e ainda hoje em cabos de antenas para redes wireless e cable modem, mas que possuíam uma série de limitações como: mal contato, conectores caros, cabos pouco maleáveis e um limite de velocidade de 10 Mbits/s.

O cabo coaxial foi por certo tempo utilizado como cabeamento responsável pela interligação de computadores em uma rede. Um cabo coaxial é basicamente composto por quatro elementos (da parte interna para a externa): um fio de cobre (responsável por transmitir sinais elétricos), um material isolante, com o intuito de minimizar interferências eletromagnéticas produzidas pelo cobre (condutor de energia), um condutor externo de malha e uma camada plástica protetora do cabo. Estes quatro elementos combinados, formam o cabo coaxial(SILVA, 2010).

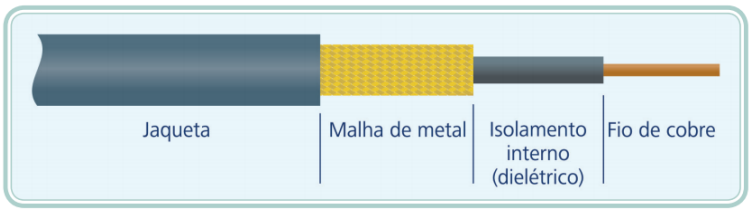


Figura 2.13: Partes do cabo coaxial, Fonte: CTISM

2.3.2 Cabos de par trançado

Os cabos de par trançado são, atualmente, os mais utilizados em uma rede local de computadores. Composto por pares de fios de cobre, trançados entre si, possuem diferentes tipos, categorias e padrões.

Existem algumas nomenclaturas que remetem ao cabo de par trançado, como por exemplo, as expressões 10Base-T ou 100Base-T, que se referem ao tipo de meio utilizado (no caso "T", como par trançado e "10" ou "100", como a taxa de transmissão em megabits). Outra expressão que nos remete a ideia de cabo de par trançado é a expressão "Ethernet" (protocolo de interconexão para redes locais), bastante usual, no funcionamento das redes de computadores. Cabos de par trançado fazem uso de material condutor (cobre) para transmitir sinais elétricos. Associado a isso temos basicamente a frequência que este sinal é transmitido e a quantidade de bits que podem ser transferidos por segundo. Por tratar-se de material condutor de sinais elétricos, os cabos de par trançado estão sujeitos a interferências eletromagnéticas externas de diferentes naturezas. e-Tec Brasil 76 Redes de Computadores.

Uma das maiores vantagens em se utilizar cabos de par trançado para implantar uma rede de computadores é o fato de possuírem baixo custo e flexibilidade em prestar manutenção, corrigir eventuais problemas ou até mesmo expandir o número de computadores ligados a esta rede.

2.3.3 Categorias de cabos de par trançado

Os cabos de par trançado são divididos em categorias como uma espécie de classificação e características do mesmo (frequência, velocidade de transmissão, etc.).

As categorias dos cabos de par trançado vão de 1 a 7. Para todas estas categorias a distância máxima permitida entre um ponto e outro onde o cabo é utilizado é de 100 metros. Fatores que influenciam no comprimento máximo do cabo já foram citados anteriormente, como frequência, taxa de transferência de dados e interferência eletromagnética.

No Quadro é possível visualizar um comparativo entre as categorias existentes, taxa de transferência possível e frequência

2.3.4 Padrões de conexão de cabo e pinagem

Um cabo de par trançado dispõe em seu interior de oito fios dispostos em pares, sendo que destes quatro pares somente dois pares são efetivamente utilizados (sendo um para transmitir e outro para receber dados). Os oito fios presentes no cabo possuem cores diferentes, como forma de simplificar a identificação dos mesmos e a crimpagem (ato de conectar o cabo ao conector RJ-45).

Para que seja mantido um padrão quanto a ordem de cores deste cabo junto ao conector, tem-se dois padrões bastante utilizados: os padrões EIA 568A e o padrão EIA 568B. O padrão EIA 568B é o mais comum e segue a ordem quanto a disposição dos fios, conforme apresentado no Quadro:

Categoria do cabo	Taxa de transferência máxima	Frequência
Cat 1	Até 01 Mbps	Até 01 MHz
Cat 2	Até 04 Mbps	Até 16 MHz
Cat 3	Até 10 Mbps	Até 16 MHz
Cat 4	Até 20 Mbps	Até 20 MHz
Cat 5	Até 100 Mbps	Até 100 MHz
Cat 5e	Até 1000 Mbps	Até 125 MHz
Cat 6	Até 1000 Mbps	Até 250 MHz
Cat 6a	Até 10 Gbps	Até 500 MHz
Cat 7	Até 10 Gbps	Até 700 MHz

Figura 2.14: Categorias de cabos de par trançado, Fonte: Morimoto, 2007

Pino do conector RJ-45	Fio
1	Branco com Laranja
2	Laranja
3	Branco com Verde
4	Azul
5	Branco com Azul
6	Verde
7	Branco com Marrom
8	Marrom

Figura 2.15: Padrão de conexão EIA 568B, Fonte: Morimoto, 2007

Já o padrão 568A, possui a seguinte ordem, representada no Quadro.

Os dois padrões possuem grande semelhança, o que ocorre de diferente é a troca de posições entre os cabos laranja e verde. Ao fazer as conexões dos conectores RJ-45 aos cabos de rede (crimpagem) devemos seguir sempre um dos padrões citados acima (568A ou 568B) nas duas extremidades do cabo, isto serve para ligação de um computador a um switch, de um computador a um roteador, enfim, para dispositivos diferentes. Caso exista a necessidade de ligar dispositivos diretamente, como no caso um computador ligado diretamente a outro por um único cabo de rede (chamado neste caso de cabo crossover), neste caso é necessário que uma das pontas do cabo seja conectada usando o padrão 568A e a outra ponta o padrão 568B.

É importante salientar a regra a seguir: • Dispositivos diferentes (ligação de cabo par trançado entre computador/ switch ou computador/roteador, etc.) cabos com padrões iguais nas duas pontas (568A nas duas pontas ou 568B nas duas pontas). • Dispositivos iguais (cabo entre computador/computador ou switch/switch, etc.) existe a necessidade de uma ponta de conexão ser diferente da outra (uma ponta 568A e a outra ponta 568B). Com esta regra fica mais fácil a utilização de cada um levando em consideração a necessidade dos mesmos.

Pino do conector RJ-45	Fio
1	Branco com Verde
2	Verde
3	Branco com Laranja
4	Azul
5	Branco com Azul
6	Laranja
7	Branco com Marrom
8	Marrom

Figura 2.16: Padrão de conexão EIA 568A, Fonte: Morimoto, 2007

2.3.5 Fibra óptica

Os cabos de fibra óptica popularizaram-se e hoje tem um papel fundamental nas telecomunicações, principalmente em ambientes que necessitam de uma alta largura de banda como é o caso da telefonia, televisão a cabo, entre outros. A redução do preço da fibra, o alcance e quantidade de dados que é possível trafegar nela são alguns dos motivos da aceitação e utilização das fibras ópticas em longas distâncias, bem como, gradativamente nas redes locais de computadores.

Uma fibra óptica nada mais é do que uma pequena haste de vidro, revestida por materiais protetores, que utiliza-se da refração interna total, para poder transmitir feixes de luz ao longo da fibra por grandes distâncias. Junta-se a capacidade de transmissão da fibra com o fato da perda ser mínima em grande parte dos casos.

Um cabo de fibra óptica é composto por diferentes materiais, conforme pode ser descrito a seguir, da parte interna para a externa da fibra (SILVA, 2010):

- Núcleo – geralmente produzido de vidro, possui em média 125 mícrons (um décimo de um milímetro aproximadamente), por onde passa a luz emitida e refletida por toda a fibra.
- Casca – geralmente de plástico serve para revestir a fibra.
- Capa – feita de plástico tem o objetivo de proteger tanto a casca como a fibra.
- Fibras de resistência mecânica – servem para preservar o cabo evitando que o mesmo seja danificado.
- Revestimento externo – camada de plástico externa que protege os cabos de fibra óptica internos.

Os cabos de fibra óptica variam quanto a quantidade de fios existentes em seu interior, podendo ter um ou vários, dependendo do tipo e onde será utilizado. De modo geral, os cabos utilizados para interligação em uma rede de computadores local, geralmente possui um único cabo. Já, os cabos de fibra destinados a interligação de grandes distâncias e links de comunicação possuem diversos fios.

Existe uma série de vantagens em se utilizar cabos de fibra óptica no lugar dos cabos de par trançado citados anteriormente, algumas destas vantagens são:

- Como os cabos de fibra óptica são bastante finos, conforme tamanho mencionado anteriormente é possível incluir uma grande quantidade de fios em um cabo.
- A quantidade de transmissão de dados possível em uma fibra é muito maior do que a capacidade alcançada através de cabos de par trançado.

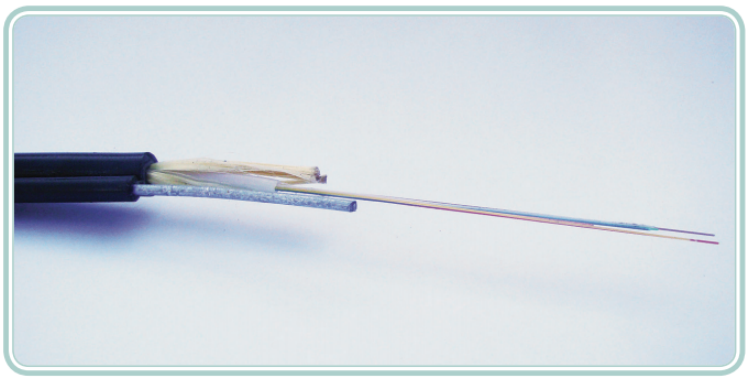


Figura 2.17: Cabo de fibra ótica, Fonte: CTISM

- Além disso, como as fibras possuem um longo alcance, necessitam de menos repetidores ou equipamentos para expansão do sinal.
- No caso de grandes distâncias a serem interligadas, acaba saindo mais barato o uso de fibras ópticas.
- Por usar refração de luz em seu núcleo a fibra é imune a interferências eletromagnéticas, podendo ser utilizada em diferentes ambientes e situações.

As fibras ópticas fazem uso de luz infravermelha para transmissão de sinais, com um comprimento de onda de 850 a 1550 nanômetros. O uso de LED's era bastante comum nos transmissores, porém, foi sendo gradativamente substituído pelos lasers devido a demanda de velocidade dos novos padrões (01 Gbps e 10 Gbps).

2.3.6 Tipos de Fibra

As fibras ópticas dividem-se em fibras de monomodo, também conhecidas como SMF (Single Mode Fibre) e as fibras de multimodo ou MMF (Multi Mode Fibre).

As fibras monomodo, têm as seguintes características:

- Possuem um núcleo de 08 à 10 mícrons de diâmetro.
- Inicialmente eram bem mais caras do que as fibras multimodo.
- A atenuação do sinal é menor do que nas fibras multimodo.
- São capazes de atingir distâncias de até 50 km sem a necessidade de retransmissores.

Já as fibras ópticas multimodo, possuem como características:

- Núcleos no tamanho de 62,5 mícrons de diâmetro.
- Inicialmente eram mais baratas que as fibras monomodo
- Possuem uma atenuação do sinal luminoso maior que as fibras monomodo.
- Podem interligar pontos até 2,5km sem necessidade de retransmissores.

A diferença entre uma fibra monomodo e uma multimodo é basicamente a forma de propagação do sinal luminoso que cada uma faz. Nas fibras monomodo, por exemplo, dado o núcleo da fibra ser menor, isso faz com que a luz trafegue na fibra mantendo uma constância do sinal, tendo desta forma um número menor de reflexões dentro da fibra, o que torna a mesma menos suscetível a perdas ou atenuação do sinal. Porém, nas fibras multimodo, acontece o inverso, ou seja, devido ao núcleo da fibra ter uma maior espessura, o sinal luminoso ricocheteia dentro da fibra em diferentes direções, fazendo com que o sinal luminoso tenha maior atenuação e maior perda durante a transmissão.

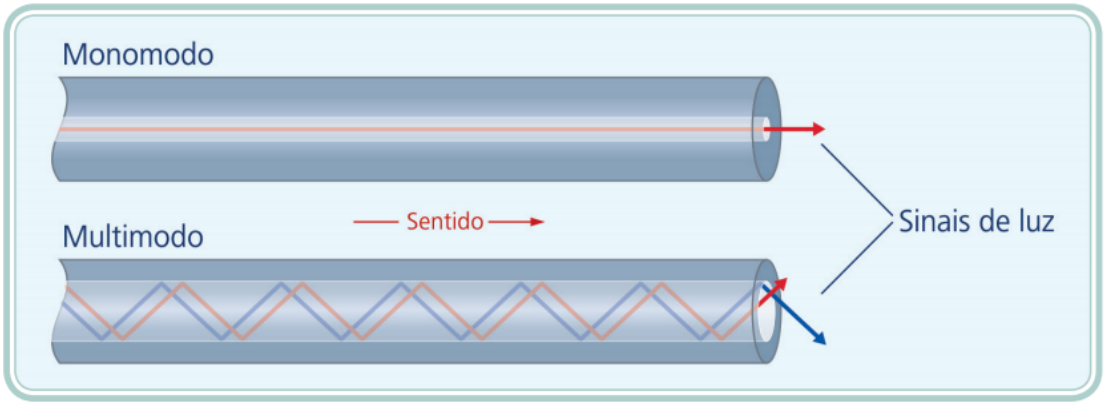


Figura 2.18: Propagação de sinal dentro da fibra óptica monomodo e multimodo, Fonte: CTISM

A figura 2.19 mostra uma tabela de trabalho das fibras ópticas monomodo e multimodo Os conectores para as fibras ópticas tem um papel importante, no que diz respeito a permitir a passagem da luz, sem que ocorra um alto nível de perda, neste processo. Existem diferentes tipos de conectores que podem ser utilizados para este fim, entre os mais usuais estão os conectores: ST, SC, LC e MT-RJ.

Tipo de Fibra	Velocidade	Distancia
Multimodo	100 Mbit/s	2 Km
Multimodo	1000 Mbit/s	200 ~ 500 m
Multimodo	10 Gbit/s	300m
Monomodo	1000 Mbit/s	2 Km
Monomodo	10 Gbit/s	10 Km

Figura 2.19: Propagação de sinal dentro da fibra óptica monomodo e multimodo, Fonte: CTISM

2.3.7 Atividade em Laboratório

Neste laboratório de redes iremos fazer a crimpagem dos cabos de cobre com o conector RJ-45 seguindo o padrão EIA 568A e EIA 568B

ATIVIDADE 1:

Utilizando o material que foi proporcionado crimpe um cabo no formato EIA 568B para conectar dos equipamentos diferentes. Faça os testes de conexão necessários. Lembrando que equipamentos diferentes devem ter o mesmo padrão de cores nas duas pontas esse tipo de cabeamento é chamdo de cabo direto ou *straigh*.

ATIVIDADE 2:

Utilizando o material que foi proporcionado crimpe um cabo no formato EIA 568B/568A para conectar dos equipamentos iguais. Faça os testes de conexão necessários. Lembrando que equipamentos iguais devem ter padrões diferentes de cores em suas pontas. Esse tipo de cabeamento

Pino do conector RJ-45	Fio
1	Branco com Laranja
2	Laranja
3	Branco com Verde
4	Azul
5	Branco com Azul
6	Verde
7	Branco com Marrom
8	Marrom

Figura 2.20: Padrão de conexão EIA 568B, Fonte: Morimoto, 2007

é chamado de *crossover*.

Pino do conector RJ-45	Fio
1	Branco com Laranja
2	Laranja
3	Branco com Verde
4	Azul
5	Branco com Azul
6	Verde
7	Branco com Marrom
8	Marrom

Figura 2.21: Padrão de conexão EIA 568B, Fonte: Morimoto, 2007

Pino do conector RJ-45	Fio
1	Branco com Verde
2	Verde
3	Branco com Laranja
4	Azul
5	Branco com Azul
6	Laranja
7	Branco com Marrom
8	Marrom

Figura 2.22: Padrão de conexão EIA 568A, Fonte: Morimoto, 2007

2.3.8 Conexão sem fio ou *wireless*

As redes de transmissão e comunicação sem-fio, também conhecidas como wireless, são, sem dúvida, uma grande alternativa aos meios de transmissão cabeados (par trançado e fibra óptica), pois se utilizam do ar para enviar e receber sinais de comunicação.

Este tipo de comunicação é útil em situações onde a utilização por meio de cabos se torna inviável, porém, como qualquer outra tecnologia, apresenta suas vantagens e desvantagens. Na sequência desse capítulo, abordaremos algumas tecnologias de transmissão sem-fio, como: rádio, Bluetooth, Wi-Fi, infravermelho, laser, entre outros.

2.3.9 Rádio

As tecnologias de transmissão via rádio utilizam-se de ondas de rádio para realizar a comunicação. Entre as vantagens deste tipo de tecnologia estão a facilidade na geração das ondas, a possibilidade de comunicação de grandes distâncias, além da flexibilidade em realizar mudanças (inserção de novos pontos de comunicação, entre outros).

Para efeitos de classificação, a transmissão via ondas de rádio pode ser feita de forma direcional ou não direcional. Na transmissão direcional a ideia é ter uma antena (geralmente uma parabólica pequena) apontando diretamente para a outra antena (na mesma direção, de forma a ficarem alinhadas, sem obstáculos), para fazer a comunicação entre duas redes distintas, por exemplo. Como vantagem da transmissão direcional está o fato da segurança, uma vez que somente as duas redes se comunicarão, mas como está exposta ao ar livre não está livre dos problemas relacionados ao ambiente externo, como um tempo nublado, chuva, raios, etc.

Com relação a transmissão não direcional, a ideia é que seja colocada uma antena transmissora em um local alto (antena do tipo omnidirecional, que propaga o sinal em diferentes direções a partir da fonte), que propicie aos clientes (antenas que irão se comunicar com a antena servidora) captar o sinal emitido. Este tipo de transmissão por estar exposto (qualquer pessoa com um dispositivo específico poderia captar o sinal) necessita de uma criptografia na transmissão dos dados (SILVA, 2010).

Este tipo de comunicação tem como vantagens o fato de ser viável economicamente e eficiente no que se propõe. Fatores como alcance da rede e taxa de transferência estão diretamente relacionados a qualidade e especificações dos equipamentos utilizados na rede.

2.3.10 Bluetooth

O Bluetooth é uma tecnologia de transmissão de dados sem-fio, que permite a comunicação entre computadores, notebooks, smartphones, mouse, teclado,impressoras, entre outros dispositivos de forma simples e com um baixo custo, bastando que estes dispositivos estejam em uma mesma área de cobertura.

A tecnologia Bluetooth (padronizada pela IEEE 802.15) possui características como: baixo consumo de energia para seu funcionamento e um padrão de comunicação sem-fio para dispositivos que façam uso desta tecnologia. Dessa forma, a comunicação entre estes dispositivos ocorre através de radiofrequência, independente da posição deste dispositivo, desde que o mesmo se encontre dentro de uma mesma área de abrangência dos demais dispositivos que queiram comunicar-se.

A área de cobertura do Bluetooth abrange três tipos de classes diferentes, conforme Quadro 2.23.

Classe	Potência (máxima)	Alcance (máximo)
1	100 mW	100 metros
2	2,5 mW	10 metros
3	1 mW	1 metro

Figura 2.23: Classes da Tecnologia Bluetooth, Fonte: Alecrim 2008b

A velocidade de transmissão em uma rede Bluetooth varia conforme a versão da tecnologia, neste caso temos:

- Versão 1.2, com taxa de transmissão de 1 Mbps (taxa máxima).
- Versão 2.0, com taxa de transmissão de 3 Mbps (taxa máxima)
- Versão 3.0, com taxa de transmissão de 24 Mbps (taxa máxima).

Quanto a frequência e operação do Bluetooth, o mesmo opera na frequência de 2,45 GHz, padrão de rádio aberta utilizável em qualquer lugar do mundo. A faixa de operação chamada ISM (Industrial Scientific Medical), possui variações de 2,4 à 2,5 GHz.

2.3.11 Wi-Fi

O termo Wi-Fi (*Wireless Fidelity*), refere-se a um padrão (IEEE 802.11) para redes sem-fio. Através da tecnologia Wi-Fi é possível realizar a interligação de dispositivos compatíveis como notebooks, impressoras, tablets, smartphones, entre outros. Assim como outras tecnologias sem-fio, o Wi-Fi utiliza-se da radiofrequência para transmissão de dados. Esta flexibilidade e facilidade de construir redes utilizando este padrão fez com que o Wi-Fi se tornasse popular, sendo hoje utilizado em diferentes locais como hotéis, bares, restaurantes, hospitais, aeroportos, etc. A tecnologia Wi-Fi é baseada no padrão 802.11, conforme citado anteriormente, que estabelece regras (normas) para criação e uso das redes sem-fio

O alcance das redes Wi-Fi variam conforme os equipamentos utilizados, mas em geral cobrem áreas de centenas de metros. As redes Wi-Fi, são subdivididas em categorias ou padrões, como forma de organização e normatização da tecnologia, conforme descrito a seguir.

Padrão 802.11 Criada originalmente em 1997, opera com frequências definidas pelo IEEE (*Institute of Electrical and Electronic Engineers*) de 2,4 GHz à 2,48 GHz, possuindo uma taxa de transmissão de dados de 1 Mbps à 2 Mbps. Quanto às formas que o padrão 802.11 utiliza para transmissão do sinal de radiofrequência, tem-se: o DSSS (*Direct Sequence Spread Spectrum*) e o FHSS (*Frequency Hopping Spread Spectrum*). O DSSS faz o uso de vários canais de envio simultâneo, enquanto o FHSS transmite a informação utilizando diferentes frequências.

Padrão 802.11b Este padrão (802.11b) é uma atualização do padrão 802.11 original. Como característica principal apresenta diferentes velocidades de transmissão, que são: 01 Mbps, 02 Mbps, 5,5 Mbps e 10 Mbps. A taxa de frequência é igual ao padrão anterior (2,4 GHz à 2,48 GHz) sendo que a distância máxima de comunicação neste padrão pode chegar a 400 metros, para ambientes abertos e 50 metros para ambientes fechados (salas, escritórios, etc.).

Padrão 802.11a Disponível em 1999, esta tecnologia possui as seguintes características:

- Taxa de transmissão de dados: 06, 09, 12, 18, 24, 36, 48 e 54 Mbps
- Alcance máximo de 50 metros
- Frequência de operação de 05 GHz
- Utiliza a técnica de transmissão denominada OFDM (*Orthogonal Frequency Division Multiplexing*), que permite a informação ser trafegada e dividida em pequenos segmentos transmitidos simultaneamente em diferentes frequências

Padrão 802.11g Disponível desde 2002, este padrão veio a substituir o padrão 802.11b. Como características este padrão possui:

- Taxas de transmissão de até 54 Mbps
- Frequências na faixa de 2,4 GHz.
- Técnica de transmissão OFDM

Padrão 802.11n Sucessor do padrão 802.11g, o padrão 802.11n teve seu início a partir de 2007. Sua principal característica está no fato de conseguir transmitir utilizando várias vias de transmissão (antenas) em um padrão chamado MIMO (*Multiple-Input Multiple-Output*), propiciando com isso taxas de transmissões na faixa de 300 Mbps

Com relação a frequência de operação, o padrão 802.11n pode operar tanto na faixa de 2,4 GHz como na faixa de 5 GHz, tornando-se compatível com padrões anteriores. Quanto a abrangência é

possível chegar a 400 metros.

Padrão 802.11ac O padrão 802.11ac, sucessor do padrão 802.11g, faz parte de uma nova geraçãode padrões de alta velocidade das redes sem-fio. Sua principal vantagem está na velocidade da transmissão de dados entre dispositivos do mesmo padrão: de 450 Mbps à 1 Gbps. Preparada para trabalhar na frequência de 5 GHz, contará com um sistema avançado de modulação chamado MU-MIMO (*Multi User – Multiple Input Multiple Output*) (ALECRIM, 2008a).

Figura 2.24: Mapa mental padrão 802.11, Fonte: O autor

2.3.12 Placa de rede

As placas de rede ou interfaces de rede, também denominadas de NIC (*Network Interface Card*) são a comunicação inicial entre um computador ou notebook, por exemplo, e os demais dispositivos da rede (switch, hub, ponto de acesso, etc.), permitindo que este dispositivo conecte-se a outro na rede.

As placas de rede podem ser on-board, neste caso já vem integradas ao computador em questão, ou off-board, neste caso são placas vendidas separadamente que são encaixadas na placa mãe do computador (slots).

Basicamente o que uma placa de rede faz é transmitir e receber dados através da rede. Entre suas principais funções estão: gerar sinais que são captados na rede e controlar o fluxo de dados.

2.4 Servidores

A palavra servidor remete aquele que serve ou servente, e é exatamente isso que ele faz, nos oferece serviços, ou de uma melhor maneira, é uma rede que disponibiliza ou armazena recursos para os seus elementos – neste caso os clientes. Existem vários tipos de serviços que nos são oferecidos pelos servidores tais como:

- Servidor de impressão.
- Servidor Web.
- Servidor DNS.
- Servidor em Nuvem.
- Servidor de E-mail.
- Servidor de Arquivos.
- Servidor DHCP.

Isso quer dizer que um servidor não é físico? Bem, a resposta é depende! Ele pode ser físico ou virtual. Empresas gigantes como o Google, Microsoft e Facebook possuem salas e mais salas extremamente refrigeradas para manter seus serviços rodando em seus equipamentos físicos. Um servidor também fornecer processamento, já que estas, são peças altamente poderosas e superam os convencionais computadores de mesa ou laptops, isso quer dizer, que se você necessita de um processamento mais forte, não precisa investir 10 mil reais em um servidor, apenas "alugue" o processamento dele pelo tempo necessário.

2.4.1 Servidor de Impressão

Recomendado para redes com pelo menos dez computadores, este servidor faz o controle das tarefas enviadas para as impressoras tanto locais como as de rede, como por exemplo, empresas em que o uso desse equipamento é compartilhado. Esse servidor proporciona controle do que vai ser impresso, do quanto vai ser impresso e por quem vai ser impresso. Através da criação de usuários de rede, os administradores podem fazer o acompanhamento de qual impressora o usuário irá usar e do que ele irá imprimir.

2.4.2 Servidor Web

É o servidor que é responsável pela internet como a conhecemos, esses servidores armazenam os sites dos quais acessamos, claro que não simplesmente adicionar os arquivos lá, eles possuem parâmetros, dados que são esperados para que o arquivo enviado seja tratado como um site, por exemplo ter a extensão ".html", ".php",".css" e por assim em diante.

2.4.3 Servidor DNS

DNS(*Domain Name System* ou Sistema de Nomes de Domínios) é usado diariamente por todos os computadores, mas muitos usuários mal sabem de sua existência. Trata-se um sistema de direção de nomes distribuídos para computadores, são essenciais para tudo que envolve pesquisa, localização e acesso dos sites. Em outras palavras, é aquele servidor encarregado pela localização, tradução e então conversão para IP dos sites que digitamos nos navegadores. Toda informação referente aos nomes dos domínios é associadas pelo Servidor DNS. Por exemplo: eu digito www.bugbusters.com.br, o servidor DNS vai traduzir esse endereço para um endereço IP, que é o real endereço do site. Isso influencia na velocidade da sua navegação.

2.4.4 Servidor em Nuvem

A maioria das pessoas já sabem o que é servidor em nuvem. Mas já parou para pensar que horrível seria se seus dados fossem corrompidos e você os perdesse? Até dá para tentar recuperá-los, mas há um custo considerável para que isso seja feito. Para evitar esse tipo de problema, a Nuvem pode ser uma solução. Mas não podemos confundir os serviços de sincronismo(os chamados Cloud Sync) com os serviços de armazenamento online(*Cloud Storage*).

Cloud Backup: Trata-se de uma cópia do dado. Com ele, você pode recuperar o backup do arquivo que foi feito em determinada data em específico e terá acesso a exatamente o arquivo que existia naquele momento do backup.

Cloud Storage: São espaços virtuais na internet onde você pode gravar seus arquivos, sem necessariamente utilizar um aplicativo de sincronismo. É mais como um pendrive ou um HD externo, porém, em nuvem.

2.4.5 Servidor de E-mail

Para enviarmos e recebermos mensagens de e-mail, precisamos de todo um sistema de correio eletrônico por trás. Precisamos de programas que suportem clientes de e-mail e seus servidores, pois é através de um endereço de correio eletrônico que é possível transferir as mensagens de um usuário para outro.

2.4.6 Servidor de Arquivos

O servidor de arquivos é projetado para permitir o armazenamento e recuperação rápida dos dados onde a computação é fornecida pelas estações de trabalho. Você encontra esses servidores em escolas e escritórios, por exemplo. Esse servidor se trata de um computador conectado a uma determinada rede com a finalidade de possibilitar um ambiente para armazenar compartilhamento de arquivos(documentos, imagens, músicas, dentre outros) para que sejam acessados por todos ligados à determinada rede de computadores. Nesse caso: Servidor – máquina principal Cliente – máquinas conectadas ao servidor Em outras palavras, quando uma equipe desejar usar um arquivo, eles poderão acessá-lo diretamente pelo servidor de arquivos ao invés de repassar o arquivo entre cada máquina. Detalhe: os arquivos sempre são atualizados em tempo real.

2.4.7 Servidor DHCP

Quando falamos em redes, existem alguns recursos que são utilizados e facilitam muito a nossa vida, mas nem os percebemos. Um deles é o protocolo DHCP. Do inglês Dynamic Host Configuration Protocol (que ficaria, em português, algo como Protocolo de Configuração Dinâmica de Endereços de Rede), é um protocolo utilizado em redes de computadores que permite às máquinas obterem um endereço IP automaticamente.

2.4.8 Atividade em Laboratório

Neste laboratório iremos simular uma rede com servidores utilizando o *software* Cisco Packet Tracer.

O Packet Tracer é um programa educacional gratuito que permite simular uma rede de computadores, através de equipamentos e configurações presente em situações reais. O programa apresenta uma interface gráfica simples, com suportes multimídia (gráfica e sonora).

Para simulação será necessário fazer o *download* do arquivo, para isso acesse o site Computer Networking e escolham a versão mais atual.

Uma vez instalado o programa você pode fazer o cadastro no site da Cisco Neste Link. Apoós criado a conta clique Neste Link e se inscreva no curso que é gratuito.

Com o cadastro feito inicie o programa e faça a seguinte atividade:

Crie os servidores abaixo dentro da mesma máquina.

- Servidor de impressão.
- Servidor Web.
- Servidor DNS.
- Servidor de Arquivos.

2.5 Lista de Exercícios

1- Ao se falar de meios transmissão, lembramos de internet cabeada e sem fio, mas quais são os sentidos que esses meios de transmissão podem ter?

A) Unicast, Broadcast, Multicast, de Retorno e Reservado.
B) Broadcast, Multicast, de Retorno, não Especificados e Reservado.
C) Broadcast, Multicast, Simucast, Especificado e Reservado.
D) Unicast, Broadcast, Multicast.
E) Broadcast, Unicast, Multicast, Especificado e de Retorno

2- Qual meio transmissão que envia pacotes de informação a todos sem distinção de grupos?
A) Multicast
B) Anycast
C) Unicast
D) Podcast
E) Broadcast

3- Ao se falar em concentradores, um se destaca por sua falta de confiabilidade a falta de capacidade de gerenciar mais de um pacote ao mesmo tempo. Este seria?
A) Roteador
B) Hub
C) Switch
D) Bridge
E) Repetidor

4- Qual equipamento utiliza uma programação chamada Distância de Hamming para poder recuperar o sinal de internet?
A) Roteador
B) Hub
C) Switch
D) Bridge
E) Repetidor

5- Quais equipamentos são considerados Concentradores Gerenciáveis?
A) Roteador, HUB e Placa de rede
B) Hub, Switch e Roteador
C) Gateway, Placa de Rede e Repetidor

D) Gateway, Placa de Rede e Roteador
E) Roteador, Switch e Bridge

6- Quais dos tipos de conexão abaixo são consideradas conexões sem fio
A) Wi-Fi, Bluetooth, Infra-Vermelho e Rádio
B) Wi-Fi, Bluetooth, IFRD, Fibra óptica
C) RJ-45, RJ-11 e 802.11
D) Gateway, Placa de Rede e Roteador
E) Roteador, Switch e Bridge

7- Qual concentrador é capaz de fazer a melhor rota para entrega dos pacotes?
A) Repetidor
B) *Hotspot*
C) HUB
D) Bridge
E) Roteador

8- Qual o esquema de cores do padrão EIA 568A?
A) Verde, Branco com Verde, Laranja, Azul, Branco com Azul, Branco com Laranja, Branco com Marrom, Marrom
B) Branco com Verde, Verde, Branco com Laranja, Azul, Branco com Azul, Laranja, Branco com Marrom, Marrom
C) Branco com Verde, Verde, Branco com Laranja, Azul, Branco com Azul, Laranja, Branco com Marrom, Marrom
D) Azul, Verde, Branco com Laranja, Azul Claro, Branco com Azul, Laranja, Branco com Marrom, Marrom
E) Branco com Verde, Vermelho com Laranja, Branco com Laranja, Azul, Branco com Azul, Laranja, Branco com Marrom, Marrom

9- Qual o esquema de cores do padrão EIA 568B?
A) Verde, Branco com Verde, Laranja, Azul, Branco com Azul, Branco com Laranja, Branco com Marrom, Marrom
B) Branco com Verde, Verde, Branco com Laranja, Azul, Branco com Azul, Laranja, Branco com Marrom, Marrom
C) Branco com Verde, Verde, Branco com Laranja, Azul, Branco com Azul, Laranja, Branco com Marrom, Marrom
D) Branco com Laranja, Laranja, Branco com Verde, Azul, Branco com Azul, Verde, Branco com Marrom, Marrom
E) Branco com Verde, Vermelho com Laranja, Branco com Laranja, Azul, Branco com Azul, Laranja, Branco com Marrom, Marrom

10- Ao se crimpar um cabo de cobre é necessário utilizar um conector padrão, qual é o conector?
A) RJ-11
B) P2
C) RJ-45
D) RJ-12

E) HDMI

11- Dados os cabos CAT 1, 4 e 7 assinale a taxa de transferência máxima respectiva.
A) Até 1 Mbps. Até 20 Mbps. Até 10 Gbps
B) Até 10 Mbps. Até 30 Mbps. Até 100 Gbps
C) Até 1 Mbps. Até 150 Mbps. Até 100 Gbps
D) Até 5 Mbps. Até 50 Mbps. Até 1 Gbps
E) Até 1 Mbps. Até 200 Mbps. Até 1000 Gbps

12- Qual dessas tecnologias utiliza luz para a transmissão de bits:
A) Cabo de Cobre
B) Cabo Coaxial
C) Cabo de Aço
D) Fibra óptica
E) Cabo Direto

13- Qual tipo de cabeamento utiliza sinais luminosos contendo um número maior de reflexões para a transmissão dos bits.
A) Fibra óptica Monomodo
B) Fibra óptico Multimodo
C) Cabo de Cobre Monomodo
D) Cabo de Cobre Multimodo
E) Wi-Fi

14- Para que serve um servidor DNS?
A) Converter o nome do site no endereço IP e Vice Versa.
B) Gerenciar a fila de impressão assim como seus arquivos.
C) Fazer becape.
D) Enviar arquivos a outro computador.
E) Gerenciar e-mails.

15- Para que serve um servidor WEB?
A) Controlar e-mails.
B) Priorizar acesso a sites importantes à empresa.
C) Armazenar os arquivos de um site para que possam ser acessados.
D) Enviar arquivos a outro computador.
E) Gerenciar redes sociais.

16- Para que serve um servidor de impressão?
A) Converter o nome do site no endereço IP e Vice Versa.
B) Gerenciar a fila de impressão assim como seus arquivos.
C) Fazer becape.
D) Enviar arquivos a outro computador.
E) Gerenciar e-mails.

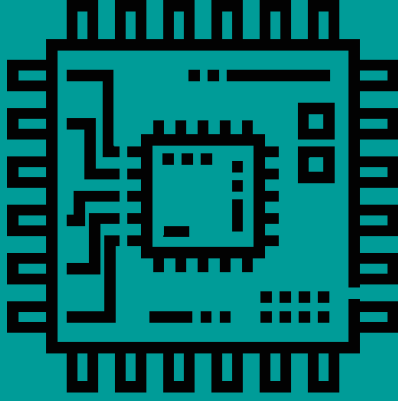
17- Para que serve um servidor de Arquivos?

A) Controlar e-mails.
B) Priorizar acesso a sites importantes à empresa.
C) Armazenar os arquivos de um site para que possam ser acessados.
D) Enviar arquivos a outro computador.
E) Gerenciar redes sociais.

18- São exemplos de servidores em nuvem:
A) Google, Facebook e LinkedIn
B) GMail, Outlook e YMail
C) Outlook, Google Drive e DropBox
D) Hulu, Netflix, Amazon Prime video
E) Twitter, Instagram e Whatsapp.

19- Para que serve um servidor DHCP?
A) Controlar e-mails.
B) Priorizar acesso a sites importantes à empresa.
C) Armazenar os arquivos de um site para que possam ser acessados.
D) Enviar arquivos a outro computador.
E) Distribuir IPs na rede.

20- Se o servidor é tão eficiente porque algumas empresas preferem alugar espaços do ter um próprio?
A) Servidores são peças caras e sua compra pode afetar o recurso de uma pequena e média empresa.
B) Todas as empresas possuem servidores devido ao baixo custo.
C) Todas as empresas possuem servidores devido a não necessidade de mão de obra especializada.
D) O custo e a mão de obra não influenciam na compra de um servidor.
E) Os servidores ainda não são tão conhecidos e por isso muitas empresas não possuem.



3. Internet das Coisas

Agora que você já possui experiência com servidores e com o programa Packet Tracer, vamos começar o novo assunto de Internet das Coisas ou *Internet of Things* (IoT). Com o avanço da tecnologia e também de sua popularização, a internet tem estado cada vez mais lugares e com isso um novo ramo de redes de computadores surgiu que é a Internet das Coisas, o que consiste em pegar algum objeto e colocar sensores e conexão com internet para que se possa haver comunicação.

Muitas aplicações começaram a ser desenvolvidas, grande parte voltada para área de vendas de comércio uma outra parte para aplicações na saúde. Neste capítulo 3 vamos aprender sobre essa nova área de estudo e realizar algumas simulações de *Smart House* utilizando o Packet Tracer.

3.1 O que é Internet das Coisas?

A tecnologia tem evoluído a passos largos, coisas que antes eram impensáveis hoje se tornam triviais, como por exemplo seu *smartphone*, é uma ferramenta poderosa, com alta capacidade de processamento e tudo isso dentro do seu bolso!

Ao se falar de IoT precisamos ter em mente qu estamos falando de sensores e conexão, aqui eu faço uma pausa para explicar sobre conexão. No geral quando pensamos em Wi-Fi pensamos em internet, nossos sites favoritos, nossas músícas favoritas e assim por diante mas o Wi-Fi, é uma conexão entre dois objetos que trocam informação e recursos sem fio, pense no Wi-Fi como um cabo gigante que você conecta os dispositivos o que eu quero dizer é que o Wi-Fi não serve só para acessar a internet e sim como um cabo de conexão.

3.1.1 Cidades Inteligentes

IoT flerta com Cidades Inteligentes, pois como dito anteriormente, o IoT é a capacidade de se pegar um objeto, colocar sensores nele captar dados e enviar esses dados, geralmente a um servidor na nuvem, este servidor na nuvem pode tirar conclusões em cima desses dados, veja o exemplo da figura abaixo.

Nesta figura temos uma lâmpada simples aonde se adicionaram dois sensores, um de movimento e outro de presença e um microprocessador com Wi-Fi que irá enviar as informações na nuvem.

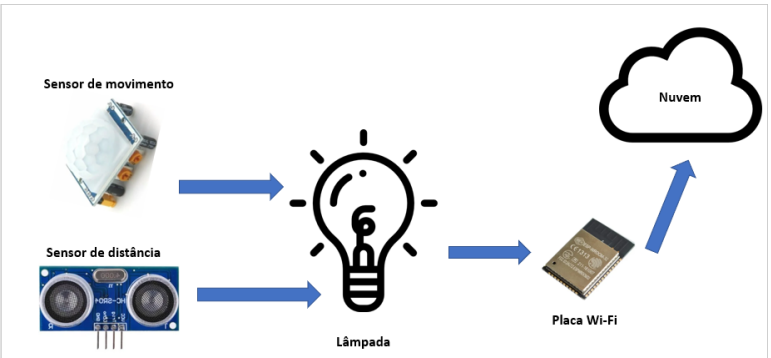


Figura 3.1: Sensores em uma lâmpada, Fonte: O autor

Podemos então com esses sensores enviar para nuvem, por exemplo, a quantidade de vezes que a lampâda foi acesa, podemos definir por quanto tempo ela ficou acesa e calcular um consumo de energia em cima daquele objeto. Pode-se também acender a lâmpada quando houver movimento, mas se houver alguém presente na sala, de acordo com o sensor de distância, o objeto ficará aceso.

Em cima dessa figura consegue-se ter o que pode ser aplicado por exemplo nas ruas, imagina postes de luzes que acendem de acordo com a presença? Isso irá gerar mais segurança para a pessoa e a prefeitura responsável conseguirá visualizar em quais regiões há menos tráfego de pessoas a noite e assim incluir medidas de mais segurança.

São José dos Campos é um epicentro de inovação não apenas para as pequenas empresas mas também para gigantes como Google e Facebook, um exemplo bem legal que temos são os *Smart Lights* próximo ao INPE que de acordo com a quantidade de pessoas o semáforo controla sua velocidade de abrir ou fechar.

Figura 3.2: Semaforo inteligente em parceria com o Google, Fonte: PMSJC

3.1.2 Economia Inteligente

Mede a capacidade econômica da cidade e as empresas instaladas na cidade

- Qualidade das empresas instaladas
- Ambiente para o empreendedorismo
- Incentivos a empresas para o desenvolvimento de soluções tecnológicas
- Investimentos em infraestrutura
- Melhoria do ambiente de negócios com legislação adequada
- Incentivo ao empreendedorismo e startups

3.1.3 População Inteligente

Mede o desenvolvimento econômico e social da população da cidade

- Educação
- Emprego
- Renda
- Projetos de inclusão digital
- Programas de educação científica e tecnológica

3.1.4 Governança Inteligente

Mede a qualidade e transparência dos serviços públicos

- Facilidade no uso dos serviços públicos
- Investimento em tecnologia
- Transparência dos dados
- Portais de transparência e de dados abertos
- Portais de participação popular
- Integração de serviços públicos

3.1.5 Mobilidade Inteligente

Mede a facilidade da mobilidade na cidade

- Ônibus, bicicleta, carro, metrô, trem, barcos
- Quilômetros de congestionamento
- Tamanho da malha metroviária
- Uso do transporte público
- Número de usuários por carro, ônibus, trem
- Monitoramento em tempo real do tráfego
- Monitoramento de vagas livres de estacionamento
- Incentivo no uso de transporte com energia limpa, barata ou renovável

3.1.6 Meio Ambiente Inteligente

Mede a sustentabilidade da cidade e seu relacionamento com o meio ambiente

- Poluição ambiental
- Eficiência no uso de recursos como água e energia elétrica
- Reciclagem de resíduos
- Monitoramento da qualidade do ar e água
- Número de usuários por carro, ônibus, trem
- Uso de fontes renováveis de energia

- Medição em tempo real dos recursos utilizados em residências

3.1.7 Vida Inteligente

Mede a qualidade de vida da população

- Entretenimento
- Segurança
- Cultura
- Quantidade de áreas verdes
- Número de bibliotecas e centros culturais
- Aplicações para o acompanhamento da saúde
- Processamento automático de imagens de câmeras de segurança
- Aplicativos sobre eventos culturais e esportivos programados na cidade

3.1.8 Casa Inteligente

Mede a capacidade de controle da sua casa por um dispositivo.

- Luzes
- Ventiladores
- Termostatos
- Ralos
- Câmeras
- Portões

3.2 Atividade em Laboratório

Utilizando o programa Packet Tracer crie uma casa automatizada e controlada por um telefone celular.

Existem algumas condições que precisam ser obedecidas:

- A casa deve ter pelo menos 7 cômodos.
- A câmera de segurança deverá ser acionada quando detectar uma presença
- Sensores de Presença
- Detector de CO2
- Controle de ralos
- O Jardim deve ser regado sempre que a umidade chegar a menos de 3%
- Todos os dispositivos precisam ser controlado por um telefone celular
- Descreve qual deles são atuadores - sensores - passivos e ativos.

Considerações Finais

Todos os itens devem ser feito utilizando o simulador packet tracer na sua opção de IoT para casas inteligentes. Tomar cuidado pois pode haver algumas dessas opções dentro do ícone de fábrica do programa.

A atividade pode ser desenvolvida em duplas mas o ideal é que se faça individualmente. Ao finalizar exercício um arquivo no formato PKT será gerado, apenas basta envia-lo não há necessidade de enviar login ou senha ou o e-mail.

Caso esteja utilizando alguma versão que não tenha dispositivos IoT, favor acessar o site no capítulo 2 baixar a versão mais atual.

3.3 Lista de Exercícios

1- Quais são os componentes básicos de IoT?

A) Um objeto, sensores e um meio de comunicação

B) Apenas sensores

C) Apenas objetos

D) Sensores e Objetos, sem a necessidade de um meio de comunicação

E) Sensores e lâmpadas, pois atualmente é o único objeto em que se pode aplicar IoT

2- "Mede o Desenvolvimento econômico e social da população da cidade". A afirmação refere-se a:

A) Economia Inteligente

B) População Inteligente

C) Governança Inteligente

D) Mobilidade Inteligente

E) Meio Ambiente Inteligente

3- Entretenimento, segurança e cultura estão relacionados a qual subtópico de cidades inteligentes?

A) Casa Inteligente

B) Mobilidade Inteligente

C) Vida Inteligente

D) Sensores

E) Econômia Inteligente

4- Uma cidade que possui um portal da transparência, claro, efetivo e intuitivo pode ser considerado como parte de Cidades Inteligentes?

A) Não pode, pois um portal das transparência não serve para averiguar gastos.

B) Pode, se encaixa perfeitamente no conceito de Econômia Inteligente.

C) Não pode, apesar de flertar com Governança Inteligente.

D) Não pode, afinal o portal da transparência só pode ser considerado efetivo se houver opção de download das informações em PDF.

E) Pode, se encaixa perfeitamente em Governança Inteligente

5- Quais dos itens abaixo se encaixa em "Meio Ambiente Inteligente".

A) Um sistema de luzes inteligentes.

B) Um sistema de casa inteligente.

C) Um sistema de tráfego inteligente.

D) Um sistema que monitora o barulho da cidade.

E) Um sistema que garante Wi-Fi por toda cidade.

6- Ao se falar de casa inteligente podemos definir que:

A) Atuadores e controle via bluetooth somente

B) Um sistema interconectado por fibra óptica.

C) Um sistema conectado por Rádio.

D) Atuadores passivos somente

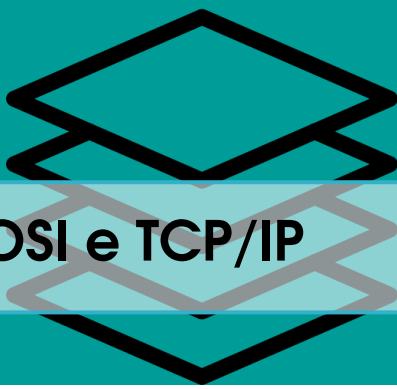
E) Sensores nesta casa e um controle via Smartphone

7- Eficiência elétrica é considerado qual subtópico de cidades inteligentes
A) Vida Inteligente
B) Casa Inteligente
C) População Inteligente
D) Econômia Inteligente
E) Meio Ambiente Inteligente

8- Número de usuários por carro, ônibus e trem. São considerados qual subtópico de cidades inteligentes?
A) Casa Inteligente
B) Mobilidade Inteligente
C) Vida Inteligente
D) Sensores
E) Econômia Inteligente

9- Ao se enviar dados na nuvem, podemos inferir que:
A) Os dados serão armazenados e nunca usados.
B) Serão armazenados e poderão gerar informações e análises estátisticas.
C) Não se envia mais dados para nuvem devido a falta de autorização de cada usuário.
D) Não há interesse em enviar os dados.
E) Devido a limitação tecnológica os dados não são enviados.

10- Assinale o termo que não compete a cidades inteligentes.
A) Gestão Inteligente
B) Economia Inteligente
C) Carro Inteligente
D) Smartphones
E) Roteadores



4. Modelos de referência ISO/OSI e TCP/IP

O modelo de referência ISO/OSI não determina uma arquitetura de rede específica, apenas define um modelo ou padrão que pode ser seguido para a construção de uma arquitetura de rede. A importância da discussão do modelo de referência OSI está, principalmente, na forma como os conceitos estão organizados em camadas com funções bem definidas. Entender o modelo OSI significa compreender o desafio envolvido na comunicação entre computadores com visão de diferentes níveis ou camadas de abstrações envolvidas. O modelo OSI está organizado em sete camadas bem definidas: física, enlace, rede, transporte, sessão, apresentação e aplicação. Cada camada tem como objetivo abstrair a complexidade das camadas inferiores, com funções definidas e formas de usar os recursos da camada imediatamente inferior. Uma camada fornece à camada superior um serviço através de uma interface simplificada.

4.1 Descrevendo as 7 camadas

Nas seções abaixo será descrito sobre cada camada do modelo ISO/OSI.

4.1.1 Camada Física

A camada física fornece as características mecânicas, elétricas, funcionais e de procedimentos para manter conexões físicas para a transmissão de bits entre os sistemas ou equipamentos (SOARES, et al., 1995).

A camada física trata apenas de permitir transmissão de bits de dados, na forma de sinais elétricos, ópticos ou outra forma de onda eletromagnética. Na camada física não há qualquer controle de erros de transmissão. Estão incluídos na camada física os meios de transmissão: cabos metálicos (transmissão de sinais elétricos), cabos ópticos (transmissão de ondas luminosas), entre outros e os componentes de hardware envolvidos na transmissão: interfaces, hub, hardware para transmissão de ondas no espectro eletromagnético (rede sem-fio), etc. Na camada física são tratadas questões como taxa de transferência de bits, modo de conexão (simplex, half-duplex, full-duplex), topologia de rede, etc.

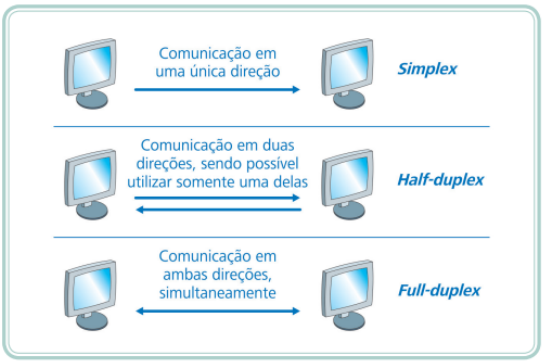


Figura 4.1: Diferenças entre modo de comunicação: simplex, half-duplex e full-duplex, Fonte: CTISM

4.1.2 Camada de enlace

O objetivo da camada de enlace é detectar e opcionalmente corrigir erros de transmissão da camada física, assim convertendo um canal de transmissão não confiável em um canal confiável, para uso pela camada de rede, logo acima.

Para se conseguir um canal de transmissão confiável na camada de enlace, geralmente são usadas algumas técnicas de identificação ou correção nos quadros de bits transmitidos, por meio de inclusão de bits redundantes. A correção ou retransmissão de um quadro, quando detectado um erro, é opcional e geralmente é deixada para as camadas superiores do modelo.

A camada de enlace também tem a função de prover um mecanismo de controle de fluxo. Essa função controla o envio de dados pelo transmissor de modo que o receptor não seja inundado com uma quantidade de dados que não consiga processar (SOARES, et al., 1995).

4.1.3 Camada de rede

A camada de rede deve fornecer à camada de transporte um meio para transferir datagramas (também chamados de pacotes dependendo do contexto) pelos pontos da rede até o seu destino. Os datagramas (ou pacotes) são unidades básicas de dados, fragmentos de dados das camadas superiores ou aplicações, com os cabeçalhos necessários para a transmissão. Nessa camada temos o conceito de encaminhamento (ou roteamento) de datagramas, que trata da forma como os datagramas devem ser encaminhados (roteados) pelos nós (roteadores) da rede, de um computador de origem a um computador de destino.

A camada de rede oferece duas classes de serviços: orientados à conexão e não orientados à conexão. No serviço orientado à conexão primeiramente, um transmissor e um receptor estabelecem uma conexão. Todos os pacotes transmitidos posteriormente entre eles são pertencentes àquela conexão (circuito) e normalmente, seguem o mesmo caminho.

No serviço de datagrama não orientado à conexão, cada datagrama enviado é independente dos enviados anteriormente, sem estabelecimento de conexão. Cada datagrama contém em seu cabeçalho a informação do endereço do transmissor (origem, remetente do pacote) e do receptor (destinatário). Os nós intermediários (roteadores) se encarregam de selecionar o melhor caminho e encaminhar (rotear) os datagramas (pacotes) do transmissor (remetente) até o receptor (destinatário) (SOARES, et al., 1995).

4.1.4 Camada de transporte

Até agora, na camada de rede e inferiores, a transferência ocorre, de fato, apenas entre os nós (máquinas) próximos na rede. A camada de transporte, por outro lado, permite que os dados trafeguem em um circuito virtual direto da origem ao destino, sem preocupar-se com a forma que os pacotes de dados viajam na camada de rede e inferiores. A camada de transporte, dessa forma, é responsável pela transferência fim a fim de dados entre processos de uma máquina de origem e processos de uma máquina de destino.

A transferência de dados, na camada de transporte, ocorre de modo transparente, independente da tecnologia, topologia ou configuração das redes nas camadas inferiores. É tarefa da camada de transporte cuidar para que os dados sigam ao seu destino sem erros e na sequência correta, condições para que se crie a ideia de um caminho fim a fim.

Além da detecção e recuperação de erros e controle da sequência dos dados, outras funções desta camada são: multiplexação de conexões e controle de fluxo. A multiplexação permite que vários processos diferentes nas máquinas de origem e destino troquem dados ao mesmo tempo. Os pacotes de dados de vários processos de uma máquina de origem são enviados para vários processos em uma máquina de destino.

Como o meio, usado nas camadas inferiores é compartilhado, os pacotes de dados precisam ser multiplexados (escalonados, embaralhados, misturados), de modo que se tem a impressão de que as transferências ocorrem simultaneamente, em paralelo. O aluno, neste ponto, pode estar se perguntandocomo os pacotes multiplexados dos vários processos encontram os processos de destino corretos? Para que isso ocorra, a camada de transporte possui mecanismos para identificar cada pacote ao seu devido fluxo de dados entre os processos. Uma forma de identificação ou endereçamento de pacotes, com relação ao processo de origem e destino, será vista quando tratarmos dos protocolos de transporte da internet.

O controle de erros possui mecanismo para identificar erros de transmissão (pacotes com dados corrompidos, por exemplo) e prover a recuperação desse erro, seja por meio da retransmissão do pacote ou outra forma de reconstrução da informação do pacote. O controle de sequência visa garantir a ordem correta da informação, independentemente da ordem em que os pacotes de dados chegaram ao destino.

Outra função importante da camada de transporte é o controle de fluxo. O destinatário e o emissor dos pacotes podem ter limites diferentes quanto a quantidade de dados que podem receber ou enviar. Um mecanismo de controle de fluxo evita que o destino receba mais dados do que tem condi- ções de receber e processar. Basicamente, o controle de fluxo permite que a máquina de origem ajuste o seu volume de pacotes enviados de acordo com a capacidade do destino em receber pacotes naquele momento, seja aumentando ou diminuindo a vazão do fluxo de pacotes, conforme a reação observada do destino.

4.1.5 Camada de sessão

A camada de sessão possui mecanismos que permitem estruturar os circuitos oferecidos pela camada de transporte. As principais funções da camada de sessão são: gerenciamento de token, controle de diálogo e gerenciamento de atividades.

O gerenciamento de token é necessário em algumas aplicações, quando a troca de informações é half-duplex, ao invés de full-duplex. O gerenciamento de token permite que apenas o proprietário do token possa transmitir dados naquele momento.

O controle de diálogo usa o conceito de ponto de sincronização. Quando a conexão para a trans-

ferência de dados de uma aplicação é interrompida, por erro, a transferência pode ser reestabelecida do ponto onde havia parado.

O conceito de atividade permite que as aplicações ou serviços oferecidos aos usuários coordenem as partes constituintes da transferência de dados. Cada atividade possui um conjunto de dados que devem ser trocados entre o serviço na origem e na aplicação de destino. Apenas uma atividade é executada (dados transmitidos) por vez, porém, uma atividade por ser suspensa, é reordenada e retomada

4.1.6 Camada de apresentação

A camada de apresentação cuida da formatação dos dados, transformação, compressão e criptografia. Não há multiplexação de dados na camada de apresentação. O propósito desta camada é converter as informações que são recebidas da camada de aplicação para um formato "entendível" na transmissão desses dados.

Como exemplo de conversão, estão os caracteres diferentes do padrão usual ASCII que precisam ser "tratados" ou quando os dados recebidos são criptografados sobre diferentes formas de criptografia, desta forma também sendo necessário uma conversão destes dados (SILVA, 2010).

4.1.7 Camada de aplicação

Na camada de aplicação estão os aplicativos, propriamente ditos, dos usuá- rios ou os serviços dos sistemas. Esta camada cuida da comunicação entre as aplicações, sendo que cada aplicação possui protocolos específicos de comunicação.

As aplicações que oferecem recursos aos usuários ou aos sistemas mais conhecidos atualmente são aquelas que oferecem serviços no padrão da internet: aplicação para navegação; transferência de arquivos; transferência de e-mail, terminal remoto e outros. A camada de aplicação diz respeito, também, aos protocolos usados na comunicação de dados entre essas aplicações.

4.2 A arquitetura TCP/IP

O modelo de referência TCP/IP é mais simplificado que o modelo de referência OSI, possuindo quatro camadas principais: aplicação, transporte, internet e interface de rede.

A semelhança entre o modelo de referência OSI e o modelo TCP/IP está no fato dos dois estarem baseados no conceito de pilha (contendo protocolos independentes). Como características o modelo TCP/IP possui:

- Quatro camadas – sendo as camadas de rede, transporte e aplicação, comum tanto ao modelo de referência OSI, como ao modelo TCP/IP.
- Adaptativo – sua criação baseou-se na adaptação para protocolos existentes, enquanto que o modelo de referência OSI (criado antes dos protocolos) apresenta-se como mais genérico e flexível.

4.2.1 Camada de Interface de Rede

Esta camada tem como objetivo principal conectar um dispositivo de rede (computador, notebook, etc.) a uma rede, utilizando para isso um protocolo. Nesta camada, a exemplo de como ocorre na camada física do modelo OSI, é tratada a informação em mais baixo nível (bits que trafegam pela rede) entre as diferentes tecnologias para este fim: cabo de par trançado, fibra óptica, etc. (SCRIMGER, 2001).

4.2.2 Camada de Internet

Esta camada tem o objetivo de permitir aos dispositivos de rede enviar pacotes e garantir que estes pacotes cheguem até seu destino. Cabe a camada de internet especificar o formato do pacote, bem como, o protocolo utilizado, neste caso o protocolo IP (Internet Protocol).

Semelhante a camada de rede do modelo de referência OSI, cabe a camada de internet realizar a entrega dos pacotes IP no destino e realizar o roteamento dos pacotes.

4.2.3 Camada de Transporte

A camada de transporte do modelo TCP/IP possui a mesma função da camada de transporte do modelo de referência OSI, ou seja, garantir a comunicação entre os dispositivos de origem e destino do pacote. Fazem parte desta camada dois protocolos bastante populares nas redes de computadores: o protocolo TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol).

- Protocolo TCP – considerado um protocolo confiável (devido a quantidade de verificações, confirmações e demais procedimentos realizados), o protocolo TCP garante a entrega dos pacotes aos computadores presentes na rede. O fluxo dos pacotes de rede passa desta camada (depois de fragmentados) para a camada de internet (para onde são encaminhados). No computador destino é feita a verificação e montagem de cada um dos pacotes, para então ser efetivado o recebimento dos mesmos.
- Protocolo UDP – protocolo sem confirmação (UDP) é comumente utilizado na transferência de dados, porém, não realiza nenhuma operação de confirmação e verificação de pacotes na estação destino (procedimento realizado pela própria aplicação). Apesar de ser classificado como um protocolo não-confiável, o UDP é mais rápido que o TCP (justamente por ter um mecanismo de funcionamento mais simplificado), sendo utilizado em requisições que não necessitam de confirmação, como é o caso de consultas DNS.

4.2.4 Camada de Aplicação

sta camada tem por objetivo realizar a comunicação entre os aplicativos e os protocolos de transporte, responsáveis por dar encaminhamento a estes pacotes.

Os protocolos da camada de transporte são usualmente conhecidos e desempenham diferentes funções, conforme exemplos a seguir:

- Protocolo SMTP – responsável pela comunicação junto ao servidor de e-mails, para entrega destes, ao programa cliente que recebe as mensagens.
- Protocolo HTTP – acionado cada vez que um usuário abre um browser (navegador) e digita um endereço de um site da internet.
- Protocolo FTP – utilizado cada vez que um usuário acessa um endereço de FTP, para fazer download ou upload de arquivos (KUROSE, 2010).

4.3 Lista de Exercícios

1- Quais são as sete camadas do modelo OSI?

2- Das camadas citadas na resposta da questão 1, qual a principal função de cada uma?

3- Quais as diferenças entre os modos de comunicação: simplex, half-duplex e full-duplex?

4- Quais são as camadas do modelo TCP/IP?

5- Qual camada você achou mais importante no modelo OSI e no modelo TCP/IP? Por quê?

6- Com base no Modelo de Camadas OSI (Open System Interconnection), assinale a alternativa que contempla a camada relacionada à sintaxe e à semântica das informações transmitidas.

A) Camada de Sessão.

B) Camada de Aplicação.

C) Camada de Apresentação.

D) Camada de Enlace de Dados.

E) Camada Física.

7- O modelo de referência OSI (*Open System Interconnection* – interconexão de sistemas abertos) foi uma proposta desenvolvida pela ISO (International Standards Organization) para padronização internacional dos protocolos utilizados nas várias camadas. Revisado em 1995, ele trata da interconexão dos sistemas abertos à comunicação com outros sistemas, sendo composta por sete camadas. De acordo com o exposto, analise a seguinte afirmativa: "[...] é uma verdadeira camada de ponta a ponta, que liga a origem ao destino. Em outras palavras, um programa na máquina de origem mantém uma conversação com um programa semelhante instalado na máquina de destino". (TANENBAUM, 2011). Assinale a alternativa correta referente a essa camada.

A) Rede.

B) Sessão.

C) Transporte.

D) Enlace de Dados.

E) Física.

8- De acordo com Tanenbaum, a camada que tem como principal serviço transferir dados da camada de rede da máquina de origem para a camada de rede da máquina de destino, é a camada de:

A) Rede.

B) Sessão.

C) Transporte.

D) Aplicação.

E) Física.

9- Enumere as colunas de acordo com as funcionalidades das camadas do modelo OSI, e marque a opção com a sequência correta.

(1) Física ( ) Representação de dados

(2) Rede ( ) Processos de rede para aplicativos

(3) Sessão ( ) Conexões fim a fim

(4) Transporte ( ) Transmissão binária

(5) Aplicação ( ) Endereço e melhor caminho

(6) Apresentação ( ) Comunicação entre hosts

(7) Enlace de Dados ( ) Acesso ao meio

A) 1-3-2-4-5-7-6

B) 7-6-1-4-3-2-5

C) 6-7-4-1-3-5-2

D) 3-7-4-1-6-2-5

E) 4-3-5-7-6-2-1

10- Sobre os tipos de transmissão de dados, correlacione as colunas abaixo e, em seguida, assinale a alternativa que contém a sequência correta.

( ) É o tipo de transmissão que é unidirecional, ou seja, em um único sentido. Não existe retorno do receptor.

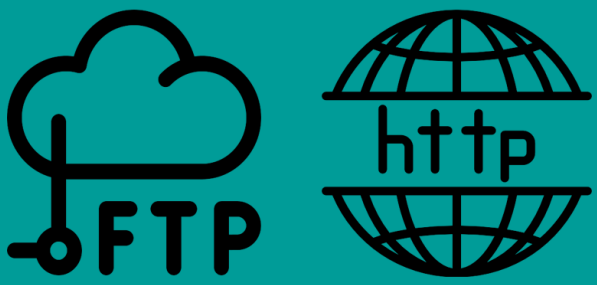
( ) É o tupo de transmissão como aquela em que um bit de cada vez, em sequência, é transmitido por uma única vi física de transmissão.

( ) É o tupo de transmissão em que os dados podem ser transmitidos e recebidos ao mesmo tempo, em ambos os sentidos, por meio de dois canais simultâneos.

( ) É o tipo de transmissão que ocorre nos dois sentidos (biderecional), porém, não simultaneamente, transmitindo em um sentido de cada vez.

1. Full-duplex.
2. Serial.
3. Simplex.
4. Duplex.

A) 2-1-3-4
B) 1-3-2-4
C) 3-1-4-2
D) 3-2-1-4
E) 4-3-2-1



5. Protocolos de redes de computadores

Protocolos em sua essência são regras e procedimentos de comunicação. Na comunicação em redes de computadores os protocolos definem as regras que os sistemas precisam seguir para comunicar-se entre si. Já, os pacotes são conjuntos de bits ou sinais que são agrupados de forma que possam trafegar pelo meio de transmissão (MORAES, et al., 2003). Os protocolos não dependem da implementação, o que significa que sistemas e equipamentos de fabricantes diferentes podem comunicar-se, desde que sigam as regras do protocolo. Dessa forma, os protocolos da arquitetura TCP/IP estão organizados em uma pilha de protocolos, a exemplo da organização em camadas da arquitetura.

5.1 Protocolos da camada de aplicação

Nessa seção serão abordados os principais protocolos da camada de aplicação, bem como, suas características e aplicabilidade. Os protocolos pertencentes a esta camada são responsáveis pela funcionalidade das aplicações utilizadas pelo usuário.

5.1.1 HTTP

O protocolo de transferência de hipertexto (HTTP – HiperText Transfer Protocol) é o principal protocolo da World Wide Web (WWW) ou simplesmente web. O HTTP é usado na web para a comunicação e transferência de documentos HTML (HiperText Markup Language) entre um servidor web e um cliente. O HTTP é um protocolo da camada de aplicação e usa o protocolo TCP para o transporte dos documentos e das mensagens (pedidos e respostas).

Baseado no modelo de arquitetura cliente/servidor e no paradigma de requisi- ção e resposta, o HTTP é responsável pelo tratamento de pedidos e respostas entre um cliente e um servidor. Além disso, utiliza como padrão a porta 80. O protocolo HTTP é a base da funcionalidade da internet. Construído sob o modelo de referência TCP/IP é caracterizado como um protocolo veloz, leve e orientado à conexão.

5.1.2 SMTP

Protocolo responsável pelo envio de e-mails, o SMTP (Simple Mail Transfer Protocol) realiza a comunicação entre o servidor de e-mails e o computador requisitante. Este protocolo utiliza por padrão a porta 25.

O protocolo SMTP tem a função de somente enviar e-mails (a um destinatário ou mais) fazendo a transmissão do mesmo. Para recebimento das mensagens de um servidor utiliza-se outro protocolo, o POP3 que tem a função de receber mensagens do servidor para o programa cliente de e-mail do usuário (Outlook, entre outros).

Para que seja efetivado o envio de e-mails através deste protocolo, uma conexão é estabelecida entre o computador cliente e o servidor responsável pelo envio de e-mails (servidor SMTP, devidamente configurado).

5.1.3 POP3

Responsável pelo recebimento de e-mails, o protocolo POP3 (Post Office Protocol) controla a conexão entre um servidor de e-mail e o cliente de e-mail. De modo geral, sua função é permitir "baixar" todos os e-mails que se encontram no servidor para sua caixa de entrada.

O protocolo POP3 realiza três procedimentos básicos durante sua operação de recebimento de e-mails que são: autenticação (realizada geralmente pelo nome de usuário e uma senha), transação (estabelecimento de conexão cliente/servidor) e atualização (finalização da conexão cliente/servidor).

5.1.4 FTP

O protocolo FTP (File Transfer Protocol) é utilizado na transferência de arquivos cliente/servidor, tanto para download quanto upload de arquivos. Para tal procedimento este protocolo utiliza as portas 20 e 21. A porta 20 é utilizada para transmissão de dados, enquanto que a porta 21 é utilizada para controle das informações.

Os serviços de FTP subdividem-se em: servidores e clientes de FTP. Os servidores de FTP permitem criar uma estrutura (serviço) onde é possível acessar via navegador, por exemplo, um endereço específico ao serviço (Ex.: ftp.exemplo.com.br) e fazer upload e/ou download de arquivos de forma on-line. Este tipo de servidor de FTP pode ser privado (na qual exige uma autenticação do usuário, mediante nome de usuário e senha) ou público, onde o acesso não necessita autenticação para acesso aos serviços.

Já os clientes de FTP, são programas instalados no computador do usuário, utilizados para acessar os servidores de FTP de forma personalizada. São exemplos destes programas aplicativos: Filezilla, Cute FTP, WS FTP, entre outros.

5.1.5 DNS

O Sistema de Nomes de Domínio (DNS – Domain Name System) é um esquema hierárquico e distribuído de gerenciamento de nomes. O DNS é usado na internet para manter, organizar e traduzir nomes e endereços de computadores. Na internet toda a comunicação entre dois computadores de usuários ou servidores é feita conhecendo-se o endereço IP da máquina de origem e o endereço IP da máquina de destino. Porém, os usuários preferem usar nomes ao se referir a máquinas e recursos.

Os computadores dispostos em uma rede de computadores são identificados por seu número IP (endereço lógico) e seu endereço MAC (identificação física, designada na fabricação do dispositivo de rede). Os endereços IP na versão 4 (IPv4), compostos de 32 bits, geralmente são difíceis de serem memorizados, conforme aumenta a quantidade de computadores na rede, servidores, entre outros.

Como forma de facilitar a memorização de computadores, sites, servidores e demais dispositivos que trabalham com a numeração IP, foi criado o sistema DNS, que torna possível relacionar nomes aos endereços IP, realizando a troca (endereço por nome). Dessa forma, torna-se mais simples lembrar um determinado endereço (www.exemplo.com.br) do que um número IP relacionado ao domínio (como por exemplo: 200.143.56.76)

O funcionamento do DNS baseia-se em um mapeamento de IPs em nomes. Estes ficam armazenados em tabelas dispostas em banco de dados nos servidores DNS. Nestes servidores são realizadas as trocas de endereços IP em nomes e vice-versa.

A estrutura de nomes na internet tem o formato de uma árvore invertida onde a raiz não possui nome. Os ramos imediatamente inferiores à raiz são chamados de TLDs (Top-Level Domain Names) e são por exemplo “.com”, “.edu”, “.org”, “.gov”, “.net”, “.mil”, “.br”, “.fr”, “.us”, “.uk”, etc. Os TLDs que não designam países são utilizados nos EUA. Os diversos países utilizam a sua própria designação para as classificações internas. No Brasil, por exemplo, temos os nomes “.com.br”, “.gov.br”, “.net.br”, “.org.br” entre outros.

Cada ramo completo até a raiz como, por exemplo, “puc-rio.br”, “acme. com.br”, “nasa.gov”, e outros, são chamados de domínios. Um domínio é uma área administrativa englobando ele próprio e os subdomínios abaixo dele. Por exemplo, o domínio “.br” engloba todos os subdomínios do Brasil.

Uma hierarquia de nomes é utilizada para caracterizar o uso de cada extensão do domínio. Na figura 5.1, são caracterizados alguns dos principais domínios utilizados e seu respectivo significado.

Nome do domínio	Significado
com	Organizações comerciais
edu	Instituições educacionais
gov	Instituições governamentais
mil	Agências militares
net	Organizações da rede
org	Organizações não comerciais
int	Organizações internacionais
Código de países	Identificador de 2 letras para domínios de países específicos

Figura 5.1: Tipos de domínios, Fonte: Tanenbaum

5.1.6 DHCP

O protocolo DHCP (Dynamic Host Configuration Protocol), possui a função de distribuir a gerenciar endereços IP em uma rede de computadores. Mais do que isso, este protocolo em conjunto com um servidor DHCP é capaz de distribuir endereços, gateway, máscaras, entre outros recursos necessários a operação e configuração de uma rede de computadores.

5.1.7 SNMP

O protocolo SNMP (Simple Network Management Protocol), ou Protocolo Simples de Gerência de Rede tem a função de monitorar as informações relativas a um determinado dispositivo que compõe uma rede de computadores.

É através do protocolo SNMP que podemos obter informações gerais sobre a rede como: placas, comutadores, status do equipamento, desempenho da rede, entre outros. A obtenção destas informações é possível graças a um software denominado agente SNMP presente nos dispositivos de rede, que extrai as informações do próprio equipamento, enviando os mesmos para o servidor de gerenciamento. Este por sua vez recebe as informações, armazena e analisa.

5.1.8 SSH

O protocolo SSH (Secure Shell), tem uma função importante na pilha de protocolos da camada de aplicação que é permitir a conexão segura (criptografada) a outro computador (da mesma rede ou de outra rede distinta) e poder controlá-lo (dependendo do nível de acesso e privilégios) remotamente. Esta função de acessar um computador distante geograficamente e poder utilizá-lo/ manipulá-lo como se o usuário estivesse presente fisicamente em frente do computador e ainda de forma criptografada, faz com que o protocolo SSH seja utilizado amplamente nas redes de computadores.

Existem diversos programas aplicativos que permitem gerenciar computadores desktop e servidores a distância e através de um outro computador ou a partir de seu próprio smartphone. A seguir, alguns exemplos destes programas aplicativos de administração remota de computadores.

5.2 Protocolos da camada de transporte

Na arquitetura TCP/IP, a camada de transporte encontra-se logo abaixo da camada de aplicação e diretamente provê um serviço para esta camada. A camada de Transporte oferece um serviço de circuito virtual fim-a-fim entre uma entidade (processo ou aplicação) na máquina de origem e outra entidade na máquina de destino.

Um conceito importante introduzido na camada de transporte da arquitetura TCP/IP é o de portas. As portas provêm um mecanismo interessante para identificação e endereçamento correto dos pacotes aos processos correspondentes nas máquinas de origem e de destino.

Cada aplicação, normalmente, está associada a uma porta conhecida pelas máquinas de origem e destino. Os dois principais protocolos da camada de transporte, o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol) oferecem as aplicações em diferentes níveis de serviço e confiabilidade.

Normalmente cada aplicação usa um dos dois protocolos, conforme a necessidade de confiabilidade e desempenho, para transporte das mensagens geradas na aplicação do cliente e do servidor. Nessa seção analisaremos mais detalhadamente esses dois principais protocolos.

5.2.1 O TCP (Transmission Control Protocol)

O TCP (Transmission Control Protocol – Protocolo de Controle de Transmissão) é o protocolo mais importante da camada de transporte e juntamente com o IP (Internet Protocol), da camada de rede, forma a dupla de protocolos mais mportantes na arquitetura do TCP/IP. O TCP permite a criação de um canal virtual confiável, livre de erros, fim-a-fim, entre uma aplicação ou serviço na máquina origem e uma aplicação na máquina de destino. O TCP é um protocolo robusto e confiável, por isso um grande número de aplicações dos usuários faz uso deste para transferência de dados. Algumas características importantes do TCP são:

Orientado a conexão – significa que antes que qualquer transmissão de mensagens ou dados da aplicação seja feita, a camada de transporte, por meio do TCP, deve estabelecer uma conexão. Basicamente, uma conexão é estabelecida após o envio de um pedido de conexão de uma das

máquinas envolvidas e a confirmação de ambas. Somente após o estabelecimento da conexão é que as mensagens da aplicação começam a ser enviadas. Todos os pacotes de dados trafegados após o estabelecimento da conexão são associados com uma conexão específica.

Ponto-a-ponto – uma conexão é estabelecida entre duas entidades, mais especificamente, ligando um processo na máquina de origem e um processo na máquina de destino.

Confiabilidade – o TCP usa um mecanismo para tratar erros durante a transmissão, como pacotes perdidos ou pacotes com dados corrompidos. Todos os pacotes transmitidos devem ser confirmados pelo receptor. Simplificadamente, a falta de uma confirmação do receptor, significa que o pacote foi perdido no caminho e deve ser automaticamente retransmitido. O TCP usa uma soma de verificação (checksum) em campo de cabeçalho (Figura 4.1), que é verificado pelo receptor. Se a soma de verificação não estiver correta, significa que os dados foram corrompidos no caminho, o pacote é descartado e a origem deve retransmitir o pacote.

Full-duplex - transferência simultânea em ambas as direções, envio e recebimento ao mesmo tempo.

Entrega ordenada – o TCP possui um campo de cabeçalho para identificação da sequência (Figura 4.1) do pacote dentro da conexão. Mesmo que os pacotes cheguem fora de ordem no destino, a mensagem da aplicação é reconstruída na ordem correta.

5.2.2 O protocolo UDP

O protocolo UDP (User Datagram Protocol) é um protocolo simples da camada de transporte. Diferentemente do TCP, o UDP é um protocolo não confiável, sem controle de sequência em que não há garantia de entrega dos pacotes.

Apesar da falta de confiabilidade do UDP, ele possui um desempenho melhor que o TCP, pois não há gasto extra (overhead) de processamento e de bits extras trafegados na rede. Por sua simplicidade o UDP é mais eficiente e rápido. Aplicações em que a confiabilidade na entrega não é tão importante, porém o desempenho é essencial, geralmente, fazem uso do UDP.

Exemplos de aplicação que usa o UDP como protocolo de transporte é o streaming de áudio e de vídeo. Nessas aplicações a falta de alguns dados durante a transmissão prejudica apenas a qualidade da imagem ou do áudio quando recebido, sem afetar completamente a transmissão. Na transmissão de áudio ou vídeo em tempo real, a agilidade na entrega dos dados é geralmente o fator mais importante.

5.3 Protocolos da camada internet da arquitetura TCP/IP

Estudaremos nesta seção os principais protocolos da camada internet (camada de rede no modelo de referência OSI), os protocolos relacionados ou auxiliares e os mecanismos de roteamento.

5.3.1 O Protocolo da Internet – IP

O IP (Internet Protocol – Protocolo da Internet) é o protocolo essencial da arquitetura TCP/IP e o principal protocolo da camada de rede. A função principal do IP é a transferência de dados, na forma de datagramas, entre os nós (computador, roteador) da rede.

O serviço oferecido pelo IP não é confiável, também chamado de “melhor esforço”. O protocolo tentará entregar o datagrama no destino, mas não há garantia de que os datagramas cheguem ordenados (pois podem seguir caminhos diferentes na rede e ter a ordem de entrega alterada), duplicados, não há garantia nem mesmo que o datagrama chegue ao destino. Embora o IP ofereça

um serviço de datagrama não confiável, a confiabilidade na transferência dos dados é uma função que pode ser adicionada nas outras camadas da arquitetura, como é estudado nas demais seções. Os roteadores, nesta camada de rede são responsáveis pela escolha do caminho que os datagramas utilizam até chegarem ao seu destino (inter-redes ou internet).

A Figura abaixo, representa os campos do cabeçalho de um datagrama IP, na sua versão 4, a versão mais usada na atualidade. Cada campo do cabeçalho está ligado a uma função dentro do protocolo:

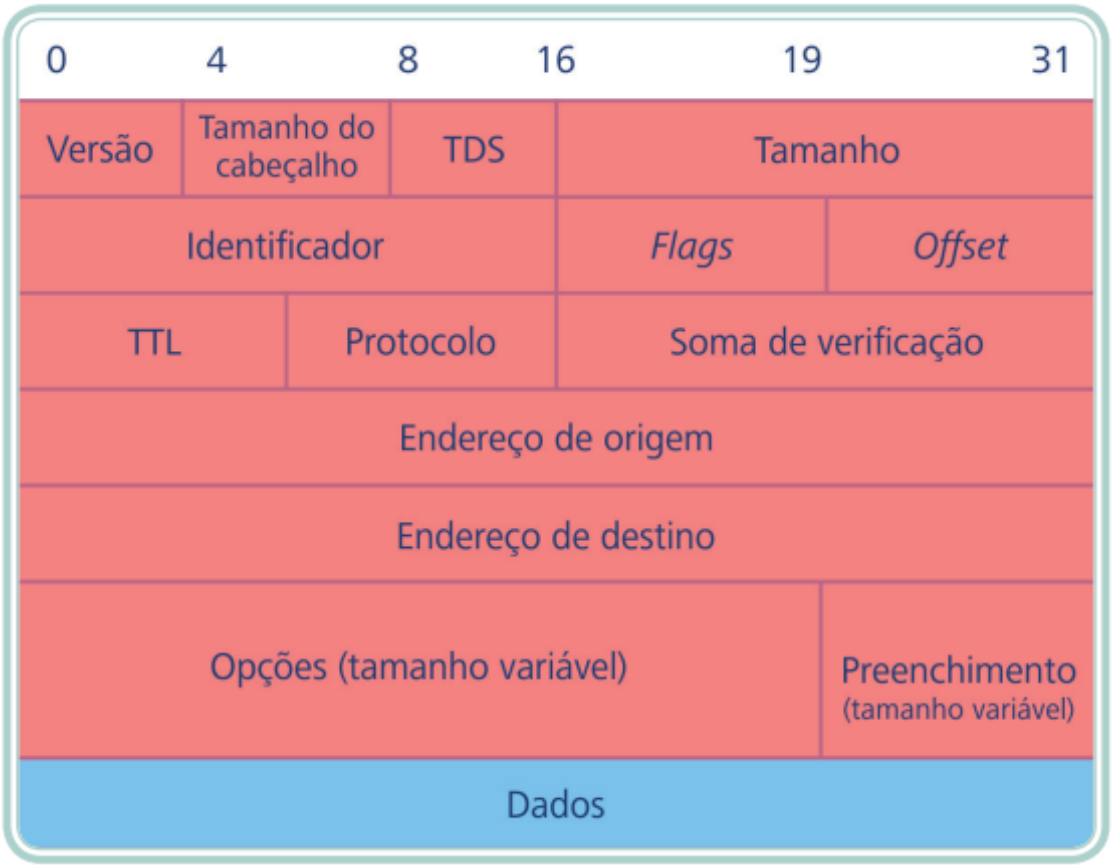


Figura 5.2: Formato de um pacote IPv4, Fonte: Fonte: CTISM, adaptado de Davie e Bruce, 2004, p. 173

- Versão – com quatro bits identifica a versão do protocolo. Atualmente a versão 4 (IPv4) é a mais usada, mas a implantação da versão 6 (IPv6) está crescendo rapidamente.
- Tamanho do cabeçalho – essencialmente serve para especificar onde começa a porção de dados do datagrama.
- TDS, tipo de serviço – basicamente serve para definir diferentes tipos de prioridades aos datagramas de diferentes serviços da internet.
- Tamanho – comprimento total do datagrama, incluindo cabeçalho e dados. Quando o tamanho do datagrama é maior que o tamanho máximo de datagrama que a rede suporta, o datagrama é quebrado em fragmentos menores
- Identificador – usado para identificar fragmentos de um mesmo datagrama original.

- Flags – usado para controlar e identificar fragmentos.
- Offset – permite ao receptor identificar o local de um fragmento no datagrama original.
- TTL (Time To Live – tempo de vida) – determina o número máximo de nós que um datagrama pode passar antes de ser descartado. O objetivo desse campo é evitar que um datagrama fique circulando pelas redes (internet) infinitamente. Cada vez que o datagrama passa (roteado) por um nó da rede, o valor do campo TTL é diminuído em uma unidade (decrementado). Quando o valor do TTL chega a zero o datagrama é descartado. Essa situação pode acontecer, por exemplo, quando há algum erro de roteamento e os datagramas são encaminhados indefinidamente (loop). Dessa forma o campo TTL evita problemas maiores nas redes.
- Protocolo – campo usado para identificar o protocolo usado junto com o IP, por exemplo, TCP (6) ou o ICMP (1).
- Soma de verificação (checksum) – usado para a verificação da integridade do cabeçalho IP. Esse valor é recalculado em cada nó (roteador).
- Endereço IP de origem – endereço IP de destino – usados para identificar as máquinas de origem e destino respectivamente.
- Opções – Campos de cabeçalhos adicionais, normalmente não são usados (DAVIE; BRUCE, 2004)

5.3.2 Endereçamento IP

O endereçamento IP permite identificar um dispositivo pertencente a uma rede de computadores. Para que isso seja possível cada um destes equipamentos conectados a uma rede (computadores, servidores, notebooks, smartphones, entre outros) deve possuir um número de identificação único (endereço IP) para que os roteadores possam fazer a entrega de pacotes de forma correta.

Atualmente o endereçamento IPv4 ainda é o mais utilizado, sendo gradativamente substituído pelo endereçamento IPv6 (que será abordado na sequência).

Os endereços IPv4 são constituídos por 32 bits, divididos em quatro octetos, em outras palavras, quatro seções de 08 bits, separados por ponto que formam o endereço IP na versão 4 (IPv4). Destes quatro octetos uma parte representa a rede enquanto outra representa a quantidade de computadores que podem estar presentes em cada rede.

Um número IP pode variar do endereço 0.0.0.0 ao endereço 255.255.255.255, embora vejamos que existem algumas particularidades tanto na utilização, quando distribuição dos números IPs nas redes de computadores.

Como forma de organização e funcionamento inicial das redes de computadores, os endereços IPs foram divididos em classes (A, B, C, D e E), conforme a representação.

Classe	Faixa	N° endereços
A	1.0.0.0 – 126.255.255.255	16.777.216
B	128.0.0.0 – 191.255.0.0	65.536
C	192.0.0.0 – 223.255.255.0	256
D	224.0.0.0 – 239.255.255.255	*Multicast*
E	240.0.0.0 – 255.255.255.254	Testes (IETF) e uso futuro

Figura 5.3: Classes de endereços IPv4, Fonte: SILVA, 2010

5.3.3 IPv6

O IPv6, também conhecido como IP versão 6, é uma espécie de atualização do IPv4, oferecendo inúmeras vantagens para seus utilizadores, como por exemplo, um maior número de endereços IPs disponíveis. A ideia do IPv6 surgiu basicamente por dois motivos principais: a escassez dos endereços IPv4 e pelo fato de empresas deterem faixas de endereços IPv4 classe A, inteiras.

Em um endereço IPv6 são utilizados 128 bits, o que permite um total de 340.282.366.920, endereços disponíveis seguidos de mais 27 casas decimais (diferentemente do IPv4, onde são utilizados 32 bits, para formar o endereço IP). Os endereços IPv6 são formados por oito quartetos de caracteres hexadecimais, separados pelo caractere ":" (dois pontos)

Exemplo: **2800 : 03f0 : 4001 : 0804 : 0000 : 0000 : 0000 : 101f**

Considerando o sistema hexadecimal, cada caractere representa 04 bits, ou 16 combinações. Ainda, considerando uma base hexadecimal temos a representação de 0 a 9 e a utilização das letras A, B, C, D, E e F, que são as representações das 16 combinações possíveis.

No IPv6 os endereços são divididos (assim como no IPv4) em dois blocos: os primeiros 64 bits identificando a rede (os primeiros 04 octetos) e os últimos 64 bits identificando os hosts. Vale lembrar aqui, que diferentemente do IPv4, no IPv6 não existem mais as máscaras de tamanho variável (CIDR) visto anteriormente.

5.3.4 Máscara de Rede

No IPv6 os endereços são divididos (assim como no IPv4) em dois blocos: os primeiros 64 bits identificando a rede (os primeiros 04 octetos) e os últimos 64 bits identificando os hosts. Vale lembrar aqui, que diferentemente do IPv4, no IPv6 não existem mais as máscaras de tamanho variável (CIDR) visto anteriormente.

5.3.5 O protocolo de controle de erros – ICMP

O protocolo ICMP (Internet Control Message Protocol) tem a função de identificar erros em uma rede de computadores. Computadores, servidores, gateways, entre outros dispositivos da rede utilizam-se do protocolo ICMP para enviar mensagens e comunicar-se entre si.

5.3.6 Tradução de endereços – ARP

Agora que compreendemos como funciona o endereçamento IP, percebemos que teremos duas formas distintas de endereçamento para os computadores da rede local: o endereço da camada de enlace, também conhecido como endereço MAC (corresponde ao endereço físico do computador) e o endereço da camada internet, também conhecido como endereço lógico ou endereço IP.

Você pode estar se perguntando agora: "As duas formas de endereçamento são usadas na mesma rede?". A resposta à pergunta é "Sim!". Nas redes locais TCP/IP, usamos ambas as formas de endereçamento, em camadas diferentes

5.4 Protocolos na Camada física

Nesta quarta e última parte estudaremos os principais protocolos da camada de interface de rede do modelo TCP/IP, também conhecida como camada física. Esta camada aborda protocolos que trabalham no nível mais próximo ao hardware (interfaces, periféricos, entre outros).

5.4.1 Ethernet

Padronizada pelo padrão IEEE 802.3, o protocolo Ethernet é amplamente utilizado nas redes locais (LAN). Este protocolo, baseado no envio de pacotes é utilizado na interconexão destas redes. Dentre as características deste protocolo estão:

- Definição de cabeamento e sinais elétricos (camada física).
- Protocolos e formato de pacotes.

O padrão Ethernet baseia-se na ideia de dispositivos de rede enviando mensagens entre si. Cada um destes pontos de rede (nós da rede) possui um endereço de 48 bits, gravado de fábrica (endereço único mundialmente), também conhecido como endereço MAC, que permite identificar uma máquina na rede e ao mesmo tempo manter os computadores com endereços distintos entre si.

5.5 Lista de Exercícios

1- Dada as camadas do modelo TCP/IP, liste os principais protocolos que operam em cada uma destas camadas.

2- Diferencie o protocolo TCP do protocolo UDP, citando três diferenças entre eles

3- Com relação ao IPv4 e ao IPv6, qual a diferença entre estes protocolos? O que muda de um para o outro e como são formados?

4- Qual a função do protocolo ICMP?

5- Cite três protocolos da camada de aplicação, o que fazem e para que servem.

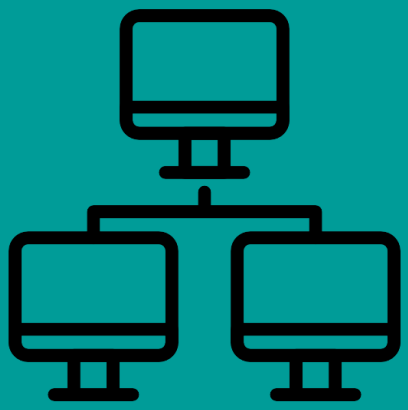
6- Por que o TCP é orientado a conexão?

7- O que é IP?

8- Cite exemplo de redes/tecnologias orientandas a conexão.

9- Cite exemplo de redes/tecnologias não orientandas a conexão.

10- Explique o que é DHCP.



6. Classificação das redes e suas topologias

As redes podem ser classificadas pelo seu tamanho geográfico, temos as seguintes classificações:

- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

6.1 Redes Pessoais (PAN)

As redes pessoais, ou PANs (Personal Area Networks), permitem que dispositivos se comuniquem pelo alcance de uma pessoa. Um exemplo comum é uma rede sem fio que conecta um computador com seus periféricos. Quase todo computador tem monitor, teclado, mouse e impressora conectados. Sem usar tecnologia sem fio, essa conexão deve ser feita com cabos.

6.2 Redes locais(LAN)

A próxima etapa é a rede local, ou LAN (Local Area Network). Uma LAN é uma rede particular que opera dentro e próximo de um único prédio, como uma residência, um escritório ou uma fábrica. As LANs são muito usadas para conectar computadores pessoais e aparelhos eletrônicos, para permitir que compartilhem recursos (como impressoras) e troquem informações. Quando as LANs são usadas pelas empresas, elas são chamadas redes empresariais. As LANs sem fo são muito populares atualmente, especialmente nas residências, prédios de escritórios mais antigos e outros lugares onde a instalação de cabos é muito trabalhosa.

6.3 Redes metropolitanas (MAN)

Uma rede metropolitana, ou MAN (Metropolitan Area Network), abrange uma cidade. O exemplo mais conhecido de MANs é a rede de televisão a cabo disponível em muitas cidades. Esses sistemas cresceram a partir de antigos sistemas de antenas comunitárias usadas em áreas com fraca recepção

do sinal de televisão pelo ar. Nesses primeiros sistemas, uma grande antena era colocada no alto de colina próxima e o sinal era, então, conduzido até as casas dos assinantes.

6.4 Redes longas distâncias (WAN)

Uma rede a longa distância, ou WAN (Wide Area Network), abrange uma grande área geográfica, com frequência um país ou continente. Vamos começar nossa discussão com as WANs conectadas por fios, usando o exemplo de uma empresa com filiais em diferentes cidades.

6.5 Topologia de rede

Uma topologia de rede tem o objetivo de descrever como é estruturada uma rede de computadores, tanto fisicamente como logicamente. A topologia física demonstra como os computadores estão dispersos na rede (aparência física da rede). Já a topologia lógica demonstra como os dados trafegam na rede (fluxo de dados entre os computadores que compõe a rede). A topologia de uma rede pode ter diferentes classificações. As principais são:

- Barramento
- Anel
- Estrela
- Malha
- Árvore
- Híbrida

6.5.1 Barramento

Na topologia em barramento todos os computadores trocam informações entre si através do mesmo cabo, sendo este utilizado para a transmissão de dados entre os computadores. Este tipo de topologia é utilizado na comunicação ponto-a-ponto. De acordo com Silva (2010), as vantagens da topologia em barramento são:

- Estações de trabalho compartilham do mesmo cabo.
- São de fácil instalação.
- Utilizam pouca quantidade de cabo.
- Possui baixo custo e grande facilidade de ser implementada em lugares pequenos.

Como desvantagens deste tipo de topologia, está o fato de que somente um computador pode transmitir informações por vez. Caso mais de uma estação tente transmitir informações ao mesmo tempo, temos uma colisão de pacotes. Cada vez que uma colisão acontece na rede é necessário que o computador reenvie o pacote. Esta tentativa de reenvio do pacote acontece várias vezes, até que o barramento esteja disponível para a transmissão e os dados cheguem até o computador receptor.

- Problemas no cabo afetam diretamente todos os computadores desta rede.
- Velocidade da rede variável, conforme a quantidade de computadores ligados ao barramento.
- Gerenciamento complexo (erros e manutenção da rede).

6.5.2 Anel

Uma rede em anel corresponde ao formato que a rede possui. Neste caso, recebem esta denominação pois os dispositivos conectados na rede formam um circuito fechado, no formato de um anel (ou círculo). Neste tipo de topologia os dados são transmitidos unidirecional mente, ou seja, em uma única direção, até chegar ao computador destino. Desta forma, o sinal emitido pelo computador

origem passa por diversos outros computadores, que retransmitem este sinal até que o mesmo chegue ao computador destino. Vale lembrar aqui que cada computador possui seu endereço que é identificado por cada estação que compõe a rede em anel.

Como vantagens esta topologia estão:

- Inexistência de perda do sinal, uma vez que ele é retransmitido ao passar por um computador da rede.
- Identificação de falhas no cabo é realizada de forma mais rápida que na topologia em barramento.

Como desvantagens desta topologia estão:

- Atraso no processamento de dados, conforme estes dados passam por estações diferentes do computador destino.
- Confiabilidade diminui conforme aumenta o numero de computadores na rede.

6.5.3 Estrela

Uma rede em estrela possui esta denominação, pois faz uso de um concentrador na rede. Um concentrador nada mais é do que um dispositivo (hub, switch ou roteador) que faz a comunicação entre os computadores que fazem parte desta rede. Dessa forma, qualquer computador que queira trocar dados com outro computador da mesma rede, deve enviar esta informação ao concentrador para que o mesmo faça a entrega dos dados.

A topologia em estrela apresenta algumas vantagens, as quais são:

- Fácil identificação de falhas em cabos.
- Instalação de novos computadores ligados a rede, ocorre de forma mais simples que em outras topologias.
- Origem de uma falha (cabo, porta do concentrador ou cabo) é mais simples de ser identificada e corrigida.
- Ocorrência de falhas de um computador da rede não afeta as demais estações ligadas ao concentrador.

Como desvantagens ligadas a esta topologia, estão:

- Custo de instalação aumenta proporcionalmente a distância do computador ao concentrador da rede.
- Caso de falha no concentrador afeta toda a rede conectada a ele.

6.5.4 Malha

A topologia em malha refere-se a uma rede de computadores onde cada estação de trabalho está ligada a todas as demais diretamente. Dessa forma, é possível que todos os computadores da rede, possam trocar informações diretamente com todos os demais, sendo que a informação pode ser transmitida da origem ao destino por diversos caminhos.

Como vantagens deste tipo de rede, podemos citar:

- Tempo de espera reduzido (devido a quantidade de canais de comunicação).
- Problemas na rede não interferem no funcionamento dos demais computadores

Desvantagem

- Alto custo financeiro.

6.5.5 Arvore

Neste tipo de topologia um concentrador interliga todos os computadores de uma rede local, enquanto outro concentrador interliga as demais redes, fazendo com que um conjunto de redes locais (LAN) sejam interligadas e dispostas no formato de árvore.

6.5.6 Híbrida

Este tipo de topologia é aplicada em redes maiores que uma LAN. É chamada de topologia híbrida pois pode ser formada por diferentes tipos de topologia, ou seja, é formada pela união, por exemplo de uma rede em barramento e uma rede em estrela, entre outras.

6.6 Lista de Exercícios

1- O que é uma rede do tipo malha?

2- O que é topologia Híbrida? Como funciona?

3- Cite um ponto positivo e um ponto negativo, quanto as topologias: Estrela, Anel e Barramento.

4- Uma empresa multinacional o contratou para montar a rede de uma das filiais, explique qual topologia escolheria.

5- Qual topologia tem como desvantagem o custo de instalação?

6- Por que a barramento não é indicada para empresas?

7- Qual das topologias é capaz de lidar com o maior número de pacotes de informação rapidamente?

8- Além das vantagens citadas na apostila, tente por você, enxergar outra vantagem da topologia estrela e o porquê.

9- É possível montar uma rede com mais de uma topologia? Justifique.

10- É vantajoso ou desvantajoso?