

FUNDAMENTOS DE INTERNET OF THINGS (IoT)

Prof^ª. Aline Zanin

Prof^ª. Camila Andrade Santos

Prof. Cleiton Silvano Goulart

Prof. Douglas Campos de Souza

Prof^ª. Fernanda Rocha de Aguiar

Prof. Fernando Esquírio Torres

Prof. Henrique Fioravanti

Prof. Matheus da Silva Serpa

Prof. Michel Bernardo Fernandes da Silva

Prof. Miguel López

Prof^ª. Patrícia Fernanda da Silva

Prof^ª. Raiza Artemam de Oliveira

Prof. Ramiro Córdova Júnior

Prof. Ramon dos Santos Lummertz



Indaial – 2020

1ª Edição



Copyright © UNIASSELVI 2020

Elaboração:

Prof^ª. Aline Zanin

Prof.^a. Camila Andrade Santos

Prof. Cleiton Silvano Goulart

Prof. Douglas Campos de Souza

Prof.^a. Fernanda Rocha de Aguiar

Prof. Fernando Esquírio Torres

Prof. Henrique Fioravanti

Prof. Matheus da Silva Serpa

Prof. Michel Bernardo Fernandes da Silva

Prof. Miguel López

Prof.^a. Patrícia Fernanda da Silva

Prof.^a. Raiza Artemam de Oliveira

Prof. Ramiro Córdova Júnior

Prof. Ramon dos Santos Lummertz

Revisão, Diagramação e Produção:

Centro Universitário Leonardo da Vinci – UNIASSELVI

Ficha catalográfica elaborada na fonte pela Biblioteca Dante Alighieri

UNIASSELVI – Indaial.

APRESENTAÇÃO

Prezado acadêmico! Seja bem-vindo à disciplina de Fundamentos de Internet of Things, ou fundamentos da internet das coisas, ou somente fundamentos de IOT é uma disciplina de extrema importância para o nosso curso de big data e para seu desenvolvimento profissional. Ela irá apresentar como essa nova área está se desenvolvendo, sua origem e como é uma área prospera e em ampla expansão.

O futuro antes apenas imaginado, onde as casas eram automatizadas as plantações controladas por robôs, agora é uma realidade e cada vez mais frequente. Onde sensores controlam a temperatura dos ambientes e conseguem controlar a umidade da terra em uma plantação. As aplicações são infinitas, e você está preparado?

Este Caderno de Estudos foi elaborado com o intuito de contribuir e aprimorar o seu conhecimento acerca destas três unidades principais: Unidade1: Conceitos Básicos sobre a IOT, na unidade 2 veremos sobre como ocorre a conectividade das “coisas” com as redes, e quais são os protocolos utilizados. Na unidade 3 veremos algumas das diversas aplicações que já existem, usando essa tecnologia.

Esse conhecimento, sobre a área de IOT torna-se fundamental para que possamos acompanhar as constantes mudanças no mercado de trabalho, onde cada vez mais, empresas buscam através da tecnologia facilitar e deixar mais seguro nosso dia a dia.

Aproveitamos esse momento para destacar que os exercícios NÃO SÃO OPCIONAIS. O objetivo de cada exercício deste caderno é a fixação de determinado conceito, bem como o aprimoramento dos seus saberes. É aí que reside a importância de você estar realizando todas as atividades propostas. Sugerimos fortemente que, em caso de dúvida, em algum exercício você entre em contato com seu tutor externo ou com a tutoria da UNIASSELVI e que não passe para o exercício seguinte enquanto o atual não estiver completamente compreendido.

Por fim, ressalto que mesmo sendo uma área muito ampla, o Caderno de Estudos lhe oferece um início sólido e consistente sobre o tema. Desejo a você uma excelente experiência nos estudos dos conteúdos dessa disciplina!



Você já me conhece das outras disciplinas? Não? É calouro? Enfim, tanto para você que está chegando agora à UNIASSELVI quanto para você que já é veterano, há novidades em nosso material.

Na Educação a Distância, o livro impresso, entregue a todos os acadêmicos desde 2005, é o material base da disciplina. A partir de 2017, nossos livros estão de visual novo, com um formato mais prático, que cabe na bolsa e facilita a leitura.

O conteúdo continua na íntegra, mas a estrutura interna foi aperfeiçoada com nova diagramação no texto, aproveitando ao máximo o espaço da página, o que também contribui para diminuir a extração de árvores para produção de folhas de papel, por exemplo.

Assim, a UNIASSELVI, preocupando-se com o impacto de nossas ações sobre o ambiente, apresenta também este livro no formato digital. Assim, você, acadêmico, tem a possibilidade de estudá-lo com versatilidade nas telas do celular, tablet ou computador.

Eu mesmo, UNI, ganhei um novo layout, você me verá frequentemente e surgirei para apresentar dicas de vídeos e outras fontes de conhecimento que complementam o assunto em questão.

Todos esses ajustes foram pensados a partir de relatos que recebemos nas pesquisas institucionais sobre os materiais impressos, para que você, nossa maior prioridade, possa continuar seus estudos com um material de qualidade.

Aproveito o momento para convidá-lo para um bate-papo sobre o Exame Nacional de Desempenho de Estudantes – ENADE.

Bons estudos!



BATE SOBRE O PAPO ENADE!



Olá, acadêmico!

Você já ouviu falar sobre o **ENADE**?

Se ainda não ouviu falar nada sobre o ENADE, agora você receberá algumas informações sobre o tema.

Ouviu falar? Ótimo, este informativo reforçará o que você já sabe e poderá lhe trazer novidades. ✓✓



Vamos lá!

Qual é o significado da expressão ENADE?

EXAME NACIONAL DE DESEMPENHO DOS ESTUDANTES

Em algum momento de sua vida acadêmica você precisará fazer a prova ENADE. ✓✓



Que prova é essa?

É **obrigatória**, organizada pelo INEP – Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira.

Quem determina que esta prova é obrigatória... O **MEC – Ministério da Educação**.

O objetivo do MEC com esta prova é o de avaliar seu desempenho acadêmico assim como a qualidade do seu curso. ✓✓



Fique atento! Quem não participa da prova fica impedido de se formar e não pode retirar o diploma de conclusão do curso até regularizar sua situação junto ao MEC.

Não se preocupe porque a partir de hoje nós estaremos auxiliando você nesta caminhada.

Você receberá outros informativos como este, complementando as orientações e esclarecendo suas dúvidas. ✓✓



Você tem uma trilha de aprendizagem do ENADE, receberá e-mails, SMS, seu tutor e os profissionais do polo também estarão orientados.

Participará de webconferências entre outras tantas atividades para que esteja preparado para #mandar bem na prova ENADE.

Nós aqui no NEAD e também a equipe no polo estamos com você para vencermos este desafio.

Conte sempre com a gente, para juntos mandarmos bem no ENADE! ✓✓





Olá, acadêmico! Iniciamos agora mais uma disciplina e com ela um novo conhecimento.



Com o objetivo de enriquecer seu conhecimento, construímos, além do livro que está em suas mãos, uma rica trilha de aprendizagem, por meio dela você terá contato com o vídeo da disciplina, o objeto de aprendizagem, materiais complementares, entre outros, todos pensados e construídos na intenção de auxiliar seu crescimento.

Acesse o QR Code, que levará ao AVA, e veja as novidades que preparamos para seu estudo.

Conte conosco, estaremos juntos nesta caminhada!

SUMÁRIO

UNIDADE 1 – CONCEITOS BÁSICOS. CONCEITUALIZANDO A INTERNET DAS COISAS - IoT.....	1
TÓPICO 1 – IoT.....	3
1 INTRODUÇÃO.....	3
2 A INTERNET DAS COISAS.....	3
3 CONECTIVIDADE.....	5
4 A GERAÇÃO DE NEGÓCIOS.....	7
RESUMO DO TÓPICO 1.....	12
AUTOATIVIDADE	13
TÓPICO 2 – CONCEITOS BÁSICOS SOBRE INTERNET DAS COISAS	15
1 O QUE É A INTERNET DAS COISAS?	15
2 PRÓS E CONTRAS DE COLOCAR ALGUMA “COISA” NA INTERNET	15
3 COLOCANDO O ARDUINO NA INTERNET	17
4 ARDUINOS PRONTOS PARA A IoT.....	17
5 SHIELDS DE COMUNICAÇÃO COM A INTERNET.....	18
6 OUTROS MÓDULOS DE COMUNICAÇÃO PARA IoT.....	19
7 APLICAÇÕES PRÁTICAS PARA IoT	20
7.1 MONITORAMENTO DE TEMPERATURA	20
7.2 AUTOMAÇÃO RESIDENCIAL.....	20
7.3 INDÚSTRIA 4.0.....	21
RESUMO DO TÓPICO 2.....	22
AUTOATIVIDADE	23
TÓPICO 3 – INTRODUÇÃO À INTERNET DAS COISAS NA PLATAFORMA RASPBERRY PI	25
1 INTRODUÇÃO	25
2 ELEMENTOS ARQUITETURAIS RASPBERRY PI	25
3 COMUNICAÇÃO DO RASPBERRY COM O MUNDO EXTERIOR.....	28
4 APLICAÇÕES DE IoT NO RASPBERRY PI.....	29
RESUMO DO TÓPICO 3.....	32
AUTOATIVIDADE	33
TÓPICO 4 – RASPBERRY PI E SUAS APLICAÇÕES	35
1 INTRODUÇÃO	35
2 PLACAS RASPBERRY PI.....	35
3 RASPBERRY PI: COMO USAR	38
4 PROJETOS COM RASPBERRY	41
5 ESTAÇÃO METEOROLÓGICA	44
6 FLIPERAMA	45
RESUMO DO TÓPICO 4.....	47
AUTOATIVIDADE	48

UNIDADE 2 – CONECTANDO A INTERNET DAS COISAS - IoT	49
TÓPICO 1 – TOPOLOGIAS E PROTOCOLOS DE COMUNICAÇÃO.....	51
1 INTRODUÇÃO	51
2 DEFINIÇÃO DE REDES DE COMPUTADORES	52
3 BREVE HISTÓRICO SOBRE REDES DE COMPUTADORES.....	56
4 TOPOLOGIAS DE REDES	58
5 OS MEIOS DE TRANSMISSÃO	61
6 TIPOS DE EQUIPAMENTOS DE REDES COM FIO	64
6.1 REPETIDORES E HUBS	64
6.2 PONTES (BRIDGES) E SWITCHES DE CAMADA 2.....	65
6.3 ROTEADORES	66
6.4 PATCH PANELS	67
7 EQUIPAMENTOS DE REDES WIRELESS.....	68
8 PROTOCOLOS DA CAMADA DE INTERNET.....	72
9 DATAGRAMA IP	76
10 FRAGMENTAÇÃO DE DATAGRAMAS IP	79
RESUMO DO TÓPICO 1.....	82
AUTOATIVIDADE	83
TÓPICO 2 – TECNOLOGIAS PARA IoT	
1 INTRODUÇÃO	87
2 O PADRÃO ETHERNET	87
2.1 CONTROLE DE ACESSO AO MEIO	89
3 O PADRÃO FAST ETHERNET	90
4 GIGABIT E 10 GIGABIT.....	92
5 CONCEITO E APLICAÇÃO DA IoT	94
6 DEFININDO TÉCNICAMENTE A IoT.....	95
7 O ECOSISTEMA DA INTERNET OF THINGS	
E O USO DE TECNOLOGIAS SEM FIO	98
8 ARQUITETURA PARA IoT USANDO DISPOSITIVOS MÓVEIS	99
9 TECNOLOGIAS MÓVEIS PARA SUPORTE AO ECOSISTEMA IoT	102
9.1 TECNOLOGIA CELULAR (4G/5G).....	103
9.2 LOWER-POWER WIDE AREA NETWORK (LPWAN)	104
9.3 WIRELESS PERSONAL AREA NETWORK (WPAN).....	106
9.3.1 IEEE 802.15.1: Bluetooth e Bluetooth Low Energy.....	107
9.3.2 IEEE 802.15.4: ZigBee	108
10 APLICAÇÕES DA INTERNET DAS COISAS.....	109
10.1 MONITORAMENTO E ATUAÇÃO	110
10.2 PROCESSO DE NEGÓCIOS E ANÁLISE DE DADOS	111
10.3 COLETA DE INFORMAÇÕES E CONSUMO COLABORATIVO	112
RESUMO DO TÓPICO 2.....	113
AUTOATIVIDADE	114
TÓPICO 3 – CONEXÃO DE EQUIPAMENTOS E NOÇÕES DE SEGURANÇA	117
1 INTRODUÇÃO	117
2 COMUNICAÇÃO VIA BLUETOOTH	117
3 COMPONENTES ELETRÔNICOS PARA A TROCA DE	
DADOS DO ARDUINO VIA BLUETOOTH	121
3.1 MÓDULO BLUETOOTH HC-05	121
3.2 CONEXÃO DO MÓDULO BLUETOOTH HC-05 AO ARDUINO.....	123
3.3 PROGRAMAÇÃO DO MÓDULO BLUETOOTH HC-05 LIGADO AO ARDUINO	124
3.4 CONEXÃO ENTRE O ARDUINO E O CELULAR	126
4 APLICAÇÕES DA COMUNICAÇÃO BLUETOOTH COM ARDUINO	127
4.1 AUTOMAÇÃO RESIDENCIAL (DOMÓTICA)	127

5 OS DESAFIOS DA ÁREA DE SEGURANÇA EM REDES SEM FIO PARA A IoT	128
5.2 CIBERSEGURANÇA (CYBERSECURITY).....	130
5.1 CONFIDENCIALIDADE E ACESSO	130
5.3 SEGURANÇA E PRIVACIDADE	131
5.4 IDENTIFICAÇÃO, LOCALIZAÇÃO E RASTREAMENTO	131
5.5 CRIAÇÃO DE PERFIL (PROFILING) E AUTENTICAÇÃO	132
5.6 ATAQUES A BANCOS DE DADOS E INVENTÁRIOS	132
LEITURA COMPLEMENTAR.....	133
RESUMO DO TÓPICO 3.....	141
AUTOATIVIDADE	142
 UNIDADE 3 – APLICANDO A INTERNET DAS COISAS - IoT	 151
 TÓPICO 1 – SENSORES 1.....	 149
1 INTRODUÇÃO.....	149
2 CARACTERÍSTICAS DOS SENSORES	149
3 TIPOS DE SENSORES.....	152
3.1 SENSORES DE POSIÇÃO	152
3.2 SENSORES DE VELOCIDADE.....	156
3.3 SENSORES DE ACELERAÇÃO.....	157
3.4 SENSORES DE FORÇA E PRESSÃO	158
3.5 SENSORES DE TORQUE.....	159
4 APLICAÇÕES DE CADA TIPO DE SENSOR:	160
RESUMO DO TÓPICO 1.....	161
AUTOATIVIDADE	162
 TÓPICO 2 – SISTEMAS DE RÁDIO POR FREQUÊNCIA (RFID).....	 165
1 INTRODUÇÃO	165
2 SISTEMA RFID NA GESTÃO DA ARMAZENAGEM.....	165
3 VANTAGENS DO SISTEMA RFID PARA A GESTÃO DE ARMAZENAMENTO.....	168
4 SISTEMA RFID NA AUTOMAÇÃO DE OPERAÇÕES DE ESTOCAGEM.....	169
5 ORIGEM DO RFID NO BRASIL E VANTAGENS COMPETITIVAS	170
6 VANTAGENS COMPETITIVAS DA TECNOLOGIA RFID.....	172
RESUMO DO TÓPICO 2.....	173
AUTOATIVIDADE	174
 TÓPICO 3 – BIG DATA E INTERNET DAS COISAS (IoT).....	 177
1 INTRODUÇÃO.....	177
2 CONCEITO DE BIG DATA	177
3 DADOS ESTRUTURADOS.....	178
4 DADOS NÃO ESTRUTURADOS.....	178
5 DADOS SEMIESTRUTURADOS	178
6 ANÁLISE DE DADOS	178
7 5V'S DO BIG DATA	179
8 TECNOLOGIAS PARA O BIG DATA	180
9 INTERNET DAS COISAS (IoT).....	181
10 ARQUITETURA DA IOT	181
11 ELEMENTOS DA IOT	182
12 RISCOS ASSOCIADOS À IOT.....	183
RESUMO DO TÓPICO 3.....	184
AUTOATIVIDADE	185
 REFERÊNCIAS	 187

CONCEITOS BÁSICOS. CONCEITUALIZANDO A INTERNET DAS COISAS - IoT

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, você deverá ser capaz de:

- reconhecer a internet das coisas;
- descrever diferentes formas de conectividade;
- listar diferentes dispositivos para permitir a conectividade e a geração de negócios;
- definir conceitos e fundamentos da Internet das Coisas (IoT);
- reconhecer os componentes que possibilitam a comunicação do Arduino com a Internet;
- analisar as aplicações da IoT com Arduino;
- identificar os elementos arquiteturais do Raspberry Pi;
- reconhecer os componentes e os protocolos que possibilitam a comunicação com o Raspberry Pi;
- ilustrar aplicações de IoT no Raspberry Pi;
- identificar as características das placas Raspberry Pi;
- analisar a aplicabilidade e conectividades possíveis com as placas Raspberry Pi;
- exemplificar projetos com as placas Raspberry Pi.

PLANO DE ESTUDOS

Esta unidade está dividida em quatro tópicos. No decorrer da unidade você encontrará autoatividades com o objetivo de reforçar o conteúdo apresentado.

TÓPICO 1 – UTILIZAÇÃO DA IoT

TÓPICO 2 – CONCEITOS BÁSICOS SOBRE INTERNET DAS COISAS

TÓPICO 3 – INTRODUÇÃO À INTERNET DAS COISAS NA PLATAFORMA RASPBERRY PI

TÓPICO 4 – RASPBERRY PI E SUAS APLICAÇÕES



Preparado para ampliar seus conhecimentos? Respire e vamos em frente! Procure um ambiente que facilite a concentração, assim absorverá melhor as informações.

1 INTRODUÇÃO

Atualmente, é impossível não perceber o efeito e a utilização das tecnologias no dia a dia da população, bem como em empresas e indústrias, uma vez que, por meio delas, é possível que diversos processos sejam simplificados, seja em tempo ou em custo, favorecendo o funcionário, a fábrica, o fabricante, e o cliente. A internet das coisas (IoT, *internet of things*) tem se desenvolvido de forma exponencial em diversas áreas, e, para tanto, faz-se necessário conhecer e compreender a importância de diferentes dispositivos, visando a permitir a conectividade e a gerar oportunidades para negócios.

Neste tópico, você conhecerá a IoT e como ela tem afetado diferentes contextos atualmente. Além disso, perceberá, por meio dela, as diferentes formas de conectividade, bem como os seus benefícios.

2 A INTERNET DAS COISAS

A evolução tecnológica tem afetado muitas empresas, de modo que elas precisaram se adequar e evoluir rapidamente, uma situação que atinge todos os atores de uma empresa, em sua totalidade. Essa evolução e nova dinâmica obrigou as empresas a buscarem por inovações e novos processos de negócios, de modo que estes se adaptem ao uso e à incorporação de diversas tecnologias, bem como de processos e soluções corporativas.

A partir do início da internet das coisas (IoT), é importante compreender como a conectividade e a informação revolucionarão o contexto da indústria 4.0. À medida que a IoT se desenvolve no dia a dia, tecnologias relacionadas levarão a conceitos como: computação em nuvem, big data, robótica, tecnologias e serviços para um próximo nível (MAJEED; RUPASINGHE, 2017).

Ao falar de IoT, muitas definições populares são mencionadas, tais como: “[...] a IoT é resultado da convergência de três visões, designadamente orientadas para as coisas, orientadas para a Internet e visões semânticas”, “[...] a IoT é todo objeto do mundo físico ou virtual que é capaz de ser identificado e integrado redes de comunicação”, ou ainda “[...] a IoT como uma infraestrutura de rede global dinâmica que será integrada e funcionará como uma extensão da internet futura,

em que várias ‘coisas’ têm identidades únicas, atributos físicos, personalidades virtuais e interfaces inteligentes” (LU; PAPAGIANNIDIS; ALAMANOS, 2018, s.p.) a partir de um artigo de pesquisa em que uma revisão de literatura sobre IoT foi realizada.

De acordo com esses autores, a “[...] a internet das coisas é um paradigma tecnológico que visa conectar qualquer coisa e qualquer um a qualquer hora e em qualquer lugar, dando origem a novos e inovadores serviços e aplicações”. Considerada a nova revolução da internet, a IoT possibilita que objetos dispositivos sejam mais inteligentes, tornem-se reconhecíveis e adquiram inteligência, ou, ainda, façam parte de uma emaranhada rede de serviços, isso porque conseguem se comunicar entre si e tomar decisões a partir da sua configuração, podendo acessar informações adquiridas por objetos físicos, dispositivos e sensores, capacidades permitidas graças à computação em nuvem e às transições de protocolos e endereçamentos quase ilimitados da internet. Essa transformação ocorreu após o surgimento da computação em nuvem e da transição da Internet para o protocolo IPv6, com uma capacidade de endereçamento quase ilimitada.

A IoT disponibiliza soluções baseadas na integração de diversas tecnologias de informação, incluindo hardware e software, que são utilizados para armazenar, recuperar e processar informações, bem como tecnologias de comunicações, incluindo sistemas eletrônicos para a comunicação entre indivíduos ou grupos de dispositivos (Figura 1). Além disso, observa-se que a entrada de dados/ações dos usuários agrega soluções conectadas e personalizadas, base do processo remoto com a utilização de bancos de dados.

Ao implementar uma solução com IoT, três requisitos são necessários: conectividade, sensores incorporados e inteligência incorporada. Conforme Majeed e Rupasinghe (2017, s.p.), “[...] rápido desenvolvimento e convergência das tecnologias de informação e comunicação está ocorrendo em três camadas de inovação tecnológica: os canais/redes de nuvem, dados e comunicação e o dispositivo”.

FIGURA 1 – IOT E SUAS POSSIBILIDADES DE CONEXÃO



FONTE: <[www.https://bit.ly/38cXUpj](https://bit.ly/38cXUpj)>. Acesso em: 30 jun. 2020.

Nos dois últimos anos, a IoT tem recebido maior atenção, visto que possui grande potencial de aplicação, além das barreiras técnicas ligadas ao monitoramento automatizado, que vêm sendo diminuídas consideravelmente, beneficiando custos que antes eram mais elevados.

Saarikko, Westergren e Blomquist (2017) salientam que os equipamentos técnicos utilizados, como computadores e sensores, estão cada vez menores e mais eficientes em relação ao consumo de energia. Já as taxas de tráfego de dados diminuíram desde que surgiu uma infraestrutura de redes de alta capacidade, permitindo fornecer aos usuários conectividade contínua.



link/tQaEX

Para mais informações acerca da IoT, acesse o link a seguir: <https://qrqo.page.link/tQaEX>.

3 CONECTIVIDADE

Seguidamente, pode-se encontrar em reportagens que “tudo parece estar ligado a um futuro próximo”, no entanto, a partir do uso da IoT, parece ser mais coerente dizer que “tudo pode ser conectado”. A IoT está se tornando cada vez mais desenvolvida e criativa, permitindo diferentes tipos de conexão, que ocorrem das mais variadas formas.

Smartphones e tablets também serviram para impulsionar a IoT, oportunizando que componentes fossem diminuídos e, conseqüentemente, mais capacidade coubesse em dispositivos cada vez menores. Diversos dispositivos na IoT estão tendo a conectividade suprida por meio de tecnologias de curto alcance por redes *meshcom*, algoritmos de roteamento com múltiplos saltos e redes de longo alcance (GMS, de *Global System for Mobile Communications* [Sistema Global para Comunicações Móveis]). Entretanto, essa abordagem, em geral, tem impactado na eficiência do uso de energia, aumentando o consumo e, assim, aumentando o preço de dispositivos de gerenciamento de rede e de dados trafegados, o que eleva o custo da solução (GARCIA; KLEINSCHMIDT, 2017).

Garcia e Kleinschmidt (2017) afirmam, ainda, que, a partir do aumento de aplicações na IoT, diferentes projetos necessitam de tecnologias para poder habilitar redes de longo alcance, baixo consumo de energia e que sejam menos onerosas, tais como as redes LPWAN (do inglês *low-power wide-area network*), que surgem como uma nova opção para a conectividade em redes M2M (do inglês *machine-to-machine*) na IoT, o que deverá possibilitar um grande número de dispositivos (bilhões de unidades).

Desse modo, as redes LPWAN possivelmente cumprirão requisitos e poderão ter longo alcance, baixo consumo de energia e capacidade de sinal. A Figura 2, a seguir, mostra uma representação da IoT e da conectividade.

FIGURA 2 – IOT E CONECTIVIDADE



FONTE: <<https://bit.ly/38chr9c>>. Acesso em: 30 jun. 2020.

Ao estudar as redes LPWAN, Garcia e Kleinschmidt (2017) destacam que esse tipo de rede de baixa potência consegue fornecer energia e permite a construção de sensores baratos e móveis, que apresentam material com duração de, no mínimo, 10 anos.

A tecnologia utilizada é específica para aplicações IoT, assim, os sensores são adaptados, visando a facilitar a transferência de dados extensos em longas distâncias (exceto para imagens e outras formas de multimídia). A tecnologia LPWAN possibilita dar cobertura para uma cidade pequena com centenas de sensores, fornecendo cobertura de rede com apenas 5 ou 6 estações-base (GARCIA; KLEINSCHMIDT, 2017). Desse modo, cidades inteiras podem ser conectadas, bem como fornecer dados em tempo real, de modo que as autoridades possam monitorar questões de segurança pública, para que o comércio possa ver a preferência dos seus compradores.

Outra utilização da IoT é em plataformas para serviços, pois um produto conectado fornece possibilidades de combinações (produtos e serviços) com soluções personalizadas, tanto para o mercado como para os clientes. Os produtos, no entanto, são associados à natureza digital, pois são conectados.

A IoT apresenta uma estrutura de serviços de informação global que permite levar a Internet para o mundo físico, rompendo limites físicos e componentes virtuais. A IoT e a realização da rede digital demandam o uso e a integração de diversas tecnologias de informação para implementar o processo de aquisição, transmissão e aplicação de informações. Para tanto, objetos do contexto social e do ambiente do usuário poderão comunicar-se e cooperar com

os seus ambientes físico e virtual para que tarefas sejam realizadas e atendam às necessidades das pessoas sem causar limitações.

A IoT, por meio da sua inteligência e arquitetura global, permite que bens e serviços sejam trocados, assim como a interação entre objetos inteligentes possibilita criar serviços. A partir do surgimento do conceito da IoT, oportunidades de inovação em serviço também passaram a surgir constantemente.

Segundo Lu, Papagiannidis e Alamanos (2018, s.p.), “[...] os sistemas sociais estão a caminho da conectividade total, criando uma sociedade em que cada dispositivo está conectado, e é por isso que a IoT tem sido considerada uma revolução tecnológica e um processo de mudança social”. Além disso, a IoT possibilita conectividade nas mais variadas formas e intensifica diariamente suas aplicações, cabendo ao ser humano simplesmente ter imaginação para a criação de novas oportunidades e negócios que façam uso dessas tecnologias.

Todavia, ao verificar tudo o que a IoT pode proporcionar, também existem desafios e ressalvas, uma vez que a sua disseminação e a enorme quantidade de dados gerados produzem preocupações em relação à invasão de privacidade, visto que o mundo está totalmente conectado.



Acesse o *link* a seguir e assista ao vídeo de Renata Rampim no TEDx Petrópolis, em que o tema IoT é abordado de forma rápida e contextualizada.

<https://qrqo.page.link/kzExH>

4 A GERAÇÃO DE NEGÓCIOS

A IoT tem grande potencial para oportunizar diversas vantagens, sejam elas tangíveis ou intangíveis, para as mais variadas partes. Por exemplo, comunicação, automação, robótica e simulação virtual poderão modificar drasticamente os setores que conhecemos hoje a partir do planejamento, da inovação de soluções de IoT, do aumento de vendas e de marketing, visando a dimensionar serviços, dar suporte e buscar co inovação, expandindo cada vez mais suas atividades.

Os dispositivos móveis e a conexão possibilitam que as pessoas estejam conectadas a todo tempo e em todo lugar. Os produtos são oferecidos diretamente ao cliente, e este tem a sua escolha uma série de serviços. Ao mesmo tempo, a empresa consegue estabelecer com o seu cliente uma relação mais estreita, o que diminui a possibilidade de concorrência.

De acordo com Majeed e Rupasinghe (2017), o conceito de fábrica futura será orientado de forma que possa garantir e possibilitar que informações relevantes possam ser processadas em tempo real, isso graças à conectividade.

É possível também que a cadeia de valor possa evoluir, passando a ser em tempo real, tendo em vista a interação entre seres humanos, objetos e demais dinâmicas do sistema, o que pode auxiliar no ajuste de diversos objetivos de negócios, reduzir custos, criar condições favoráveis de recursos, bem como proporcionar alta disponibilidade.

Para as empresas, é importante que possam, diante desse contexto, primeiramente atribuir uma identidade visual para objetos físicos, e, a partir daí, questões de logística, tempo e custo poderão ser diminuídas. Questões como conectividade e acesso remoto passaram a receber maior atenção, desafiando até mesmo as empresas mais tradicionais e consolidadas no mercado, as quais sofrem ameaças constantes de novos investidores e produtos.

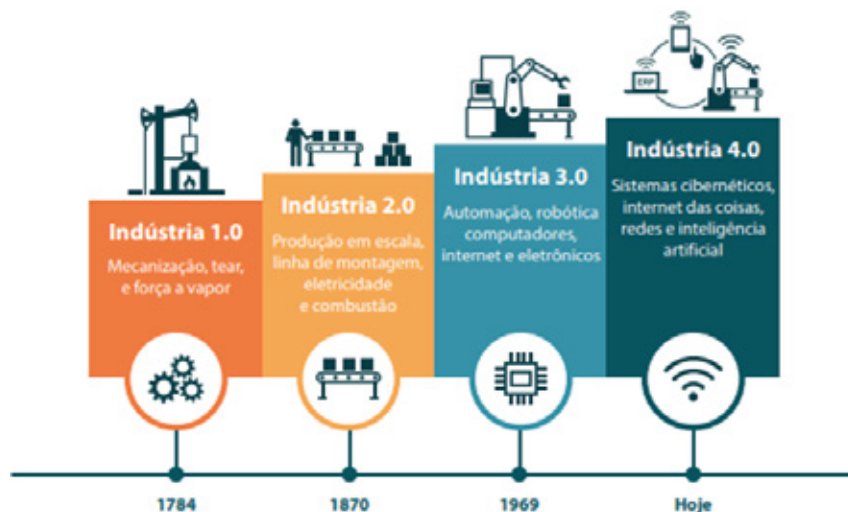
A IoT tem estado frente a mudanças sociais e de produtos com as mais variadas funções para diferentes áreas, impactando na interação de compra do consumidor, bem como no design de produtos. Segundo Chang *et al.* (2014 *apud* LU *et al.*, 2014, s.p.) as intenções de compra são delimitadas por seis características principais, assim como pelas experiências do cliente. De acordo com os autores, as características são:

- a) IoT Connectivity: “o grau em que as coisas estão interconectadas”.
- b) Interatividade IoT: sentimento dos clientes que ocorre quando a comunicação da informação é bidirecional e a resposta é oportuna.
- c) Telepresença da IoT: os sentimentos subjetivos dos clientes sobre “a medida em que a mídia representa o ambiente físico e social”.
- d) IoT Intelligence: funções de reconhecimento intrincadas e precisas, capacidade de raciocínio e julgamento corretos.
- e) Conveniência da IoT: “o grau em que os consumidores economizam tempo e esforço no processo de planejamento, compra e uso de um produto”.
- f) Segurança da IoT: evitar danos quando se trata de ativos vulneráveis e valiosos.

Atualmente, o grande desafio da geração de negócios, em meio a um contexto alicerçado por dispositivos e conectividade, é o desenvolvimento de produtos e a diversidade de oferta, que as empresas buscam por diferentes maneiras de competir, tanto na experiência e expertise como nos preços.

Com o desenvolvimento tecnológico e a Revolução Industrial, que ocorre de forma exponencial, a produção deverá seguir por novos percursos, fazendo o homem e as máquinas ficarem cada vez mais ligados e conectados entre si (Figura 3) (MAJEED; RUPASINGHE, 2017).

FIGURA 3 – REVOLUÇÃO INDUSTRIAL



FONTE: Adaptado de: <<https://bit.ly/2ZorVOJ>>. Acesso em: 30 jun. 2020.

Diante do uso de diferentes tecnologias nas indústrias, as pessoas terão de trabalhar com muitos processos, redes de processos, máquinas, sensores, robótica e dispositivos, em meio também a um sistema que exigirá variados conhecimentos para que uma melhor operação e relação homem-máquina possa ocorrer.

Em um futuro não muito distante, processos rápidos e inteligentes de fabricação serão um diferencial e uma vantagem competitiva para a empresa, pois, hoje, grande parte das instalações de manufatura e produção desenham um sistema que faz dos dispositivos e máquinas adaptáveis, integrados, analíticos e ainda mais eficientes, o que permite que desenvolvam suas atividades de modo muito semelhante a pessoas.

Para Majeed e Rupasinghe (2017), uma nova Revolução Industrial está por vir, a qual será denominada fábrica do futuro. Esse modelo possibilitará uma era de fabricação inteligente, com base em total automação, e envolverá um aumento no processo de fabricação, em que equipamentos e sistemas mecânicos irão ao encontro da era digital (Figura 4). Os dados serão mais rápidos e terão maior acúmulo, necessitando de um sistema configurado e adequado para o processamento de dados.

Este novo conceito de “fábrica do futuro” será organizado para que todas as informações relevantes sejam disponibilizadas em tempo real, o que só é possível graças à conectividade disponível em todos os lugares e espaços possíveis. Além disso, acredita-se que, pela interação entre homem e máquina, objetos e diferentes dinâmicas do sistema, muitas informações e valores possam ser oferecidos em tempo real, ajudando diferentes formas de negócios, tais como redução de custos, otimização de recursos etc.

FIGURA 4 – AUTOMAÇÃO DE PROCESSOS



FONTE: Adaptado de: <<https://bit.ly/3dPf11s>>. Acesso em: 30 jun. 2020.

Os trabalhadores, os fabricantes, as fábricas e os clientes deverão perceber que a cadeia de suprimentos futuros será cada vez mais complexa, incluindo numerosos processos, operação de máquinas e componentes de forma integrada, o que, por sua vez, exigirá vários conceitos operacionais entre homem e máquina, visando à eficiência e à redução de tempo para a colocação de produtos no mercado, garantindo que os fabricantes possam reduzir custos operacionais, bem como maximizar a utilização de recursos.



Acesse o link a seguir e leia o artigo *Aplicação das tecnologias IoT no desenvolvimento de novos produtos e serviços*, apresentado no 11º Congresso de Inovação e Gestão de Inovação do Produto, em 2017.

<https://qrgo.page.link/YdyQL>



Majeed e Rupasinghe (2017, s.p.) exemplificam sobre o mercado global das fábricas inteligentes, conectividade e IoT no artigo *Internet of things (IoT) embedded future supply chains for industry 4.0: an assessment from an ERP-based fashion apparel and footwear industry*:

Espera-se que o mercado global de fábricas inteligentes totalize cerca de 67 mil milhões de dólares até 2020, aumentando a uma taxa de crescimento anual composta de 6% entre 2014 e 2020. Comunicação, automação, robótica e simulação virtual vão mudar o setor de produtos como o conhecemos hoje. Fornecedores como a SAP planeja acelerar a inovação em seu portfólio de soluções de IoT, aumentar vendas e *marketing*, dimensionar serviços, suporte e co-inovação e expandir seu ecossistema de parceiros e *startups* no mercado de IoT, que deve chegar a € 250 mil milhões em 2020.



RESUMO DO TÓPICO 1

Neste tópico, você aprendeu que:

- Cada vez mais, as pessoas usam no seu dia a dia objetos que estão em constante comunicação entre si e também com a internet. O que, por sinal, tem facilitado muito o desenvolvimento de diversas atividades cotidianas tanto no trabalho como no lazer.
- Parar e refletir sobre o início e o desenvolvimento dessas ferramentas parece ser algo distante, pois elas passaram a ser usadas não faz muito tempo, porém já parece impossível viver sem fazer uso de todos os benefícios e da praticidade apresentada pela internet of things.



- 1 A IoT tem possibilitado diferentes experiências no dia a dia, principalmente no que diz respeito à conexão. Assinale a assertiva com o conceito que melhor define internet of things (IoT).
 - a) () Através de dispositivos, tenta fazer conexões em tempo real a longas distâncias, possibilitando abundância de rede e conexão.
 - b) () Por meio da tecnologia, conecta qualquer coisa, independentemente de tempo e espaço, originando serviços e aplicações inovadores.
 - c) () Busca conectar qualquer coisa por meio de redes, independentemente de tempo e espaço, e origina diferentes formas de negócios e inovação.
 - d) () Através de redes de grande extensão, conecta tecnologias em tempo real e possibilita que as pessoas possam interagir com máquinas.
 - e) () Por meio da tecnologia, conecta outras tecnologias, possibilitando diferentes formas de interagir e se comunicar.

- 2 A IoT tem apresentado diversos benefícios em sua utilização, principalmente no que tange à agilidade e à comunicação. No entanto, todos esses recursos disponíveis também trouxeram algumas dificuldades e preocupações, à medida que sua utilização tem aumentado exponencialmente. Assinale a alternativa que apresenta as supostas dificuldades que surgiram após aumentar o uso da IoT.
 - a) () Aumento do consumo de energia, capacidade de sinal insuficiente e custo elevado.
 - b) () Diminuição no consumo de energia, melhora na qualidade do sinal e baixo custo.
 - c) () Aumento do consumo de energia, melhora na capacidade do sinal e custo elevado.
 - d) () Diminuição no consumo de energia, capacidade de sinal insuficiente e baixo custo.
 - e) () Aumento do consumo de energia, melhora na capacidade do sinal e baixo custo.

- 3 Para proporcionar o uso da IoT de forma satisfatória e com o uso de todo o seu potencial, é necessário obedecer e seguir alguns requisitos. Tendo em vista as aplicações de uso de rede na IoT, quais os requisitos para que uma rede possa atendê-la de forma ideal?
 - a) () Oferecer alcance, ter consumo de energia e capacidade de sinal.
 - b) () Ter alcance, baixo consumo de energia e bom sinal.
 - c) () Atender longo alcance, ter baixo consumo de energia e capacidade de sinal.
 - d) () Ter alcance, consumo de energia e capacidade de sinal.
 - e) () Atender longo alcance, ter consumo de energia e bom sinal.

4 O uso da IoT, além de facilidades, trouxe preocupações e desafios para o mundo dos negócios. Assinale a alternativa que apresenta os dois maiores desafios da geração de negócios mediante o contexto atual, que é alicerçado por dispositivos e conectividade.

- a) () Venda de produtos e controle de materiais.
- b) () Adequação de produtos e marketing.
- c) () Busca por produtos e diferencial na oferta.
- d) () Criação de produtos e adequação de oferta.
- e) () Desenvolvimento de produtos e diversidade de oferta.

5 Novos processos de manufatura deram origem à Revolução Industrial. Atualmente, acredita-se que uma nova Revolução Industrial esteja por vir, originando a fábrica do futuro. Diante dessas mudanças, o que é esperado para a fábrica do futuro?

- a) () Trabalhos manuais serão substituídos por máquinas automatizadas.
- b) () A interação homem-máquina será substituída por automação.
- c) () Equipamentos e sistemas serão comandados pelo homem.
- d) () Equipamentos e sistemas mecânicos irão ao encontro da era digital.
- e) () A automação passará a contar com o auxílio da programação do homem.

CONCEITOS BÁSICOS SOBRE INTERNET DAS COISAS

1 O QUE É A INTERNET DAS COISAS?

Antes de falarmos da Internet das Coisas, vamos entender o que é a internet. A **internet** começou como um projeto de pesquisa da interligação de alguns computadores universitários nas décadas de 1970 e 1980. Naquele momento, o conteúdo disponível era muito pequeno e tinha um foco bem restrito ao ambiente acadêmico e militar. Com o passar do tempo, cada vez mais computadores foram sendo inseridos nessa rede, de forma que hoje chega a ser impraticável contar quantos computadores estão conectados a essa rede. Atualmente, a internet é um meio de comunicação extremamente versátil, rápido e poderoso (COMER, 2016).

A **Internet das Coisas**, ou simplesmente **IoT** (*Internet of Things*), é um conceito que foi idealizado na década de 1990. Historicamente, a primeira “coisa” que foi conectada à internet, dentro desse conceito, foi uma torradeira elétrica na feira INTEROP, em 1990. A ideia da torradeira era simples: basicamente, ela estava ligada a um computador equipado com rede e, por meio de comandos enviados através da internet, era possível ligar ou desligar a torradeira. Na edição seguinte dessa mesma feira, o projeto foi melhorado com o acréscimo de um braço robótico que pegava o pão e o colocava na torradeira - com todos os comandos recebidos via internet (ROMKEY, 2017).

O conceito de IoT ainda carece de alguma padronização para que seja bem entendido. Apesar das divergências existentes, a ideia central por trás da definição de IoT é a de que objetos comuns do nosso dia a dia passem a ser conectados à internet. Vários podem ser os objetivos dessa conexão - por exemplo, podemos ter os objetos que monitoram alguma condição, digamos a temperatura de uma sala de computadores; através da internet, esses objetos/ sensores disponibilizam a temperatura em tempo real a quem tenha o acesso a eles. A grande vantagem é que uma pessoa pode monitorar a temperatura dessa sala mesmo estando em outro país, pois hoje a internet permite conexão em qualquer lugar do planeta.

2 PRÓS E CONTRAS DE COLOCAR ALGUMA “COISA” NA INTERNET

Assim como a internet permite uma comunicação mais rápida, fazendo a informação circular em uma velocidade extraordinária, a IoT permite disseminar

muitas informações na internet. As oportunidades que são abertas com a possibilidade de os objetos utilizarem esse recurso talvez sejam o maior trunfo da IoT.

A comodidade é uma grande oportunidade que a IoT permite - por exemplo, nos sistemas de automação residencial, nos quais você pode controlar as lâmpadas da sua casa pela internet, não importa onde esteja. Assim que estiver retornando a sua casa, você pode enviar um comando para ligar o aparelho de ar-condicionado, para que quando, você chegar, o ambiente já esteja climatizado (COMER, 2016).

Com os dispositivos de uma casa conectados à internet, eles podem ainda ajustar o seu ciclo de funcionamento conforme o horário de pico, em que a energia elétrica é mais cara, permitindo, assim, uma otimização do consumo energético.

Nas indústrias, a IoT também tem muito a contribuir. A IoT é um dos pilares da Indústria 4.0, em que podemos, por exemplo, instalar sensores e atuadores da planta industrial conectados à internet. Desse modo, a unidade de controle da fábrica pode ficar instalada de forma remota, trazendo certo nível de segurança para os operadores e facilitando a gestão de várias plantas similares, ao permitir a instalação de uma única central de controle, por exemplo. Até os custos com a implantação de cabos de comunicação podem ser reduzidos, porque, se todos os dispositivos forem conectados a uma única rede, toda a camada física de controle fica mais simples.



Você sabe o que é a **Indústria 4.0**? Este é um termo que designa um conjunto de práticas que vêm sendo aplicado nas indústrias para melhorar sua gestão interna. No conceito de Indústria 4.0 podemos encontrar várias tecnologias inovadoras, sendo que um de seus pilares fundamentais é a IoT (SANTOS; MANHÃES; LIMA, 2018).

As indústrias estão incorporando cada vez mais dispositivos conectados, a fim de deixar os processos mais rápidos e mais automatizados. Lembre-se de que a Indústria 4.0 incorpora outras tecnologias além da IoT.

Apesar dessas vantagens, devemos reconhecer que a IoT ainda tem alguns desafios a vencer. Por exemplo, o aspecto da segurança e da privacidade ainda são fatores em que a IoT não possui um padrão bem estabelecido que garanta a inviolabilidade do controle de um dispositivo na rede. Muitas indústrias ainda resistem à implantação da IoT em suas plantas industriais devido a esse aspecto. Se existem hackers que conseguem “invadir” até os computadores mais seguros, será que eles não irão conseguir invadir o sistema de controle de uma planta industrial, por exemplo.

3 COLOCANDO O ARDUINO NA INTERNET

Várias são as opções para se colocar um dispositivo qualquer na internet. Vamos agora conhecer os principais dispositivos que, associados ao Arduino, permitem a comunicação com a internet. Veremos alguns dos principais Arduinos que já têm suporte nativo para comunicação na internet e alguns acessórios que permitem a conexão com a internet e podem ser adaptados em placas sem conectividade nativa.

4 ARDUINOS PRONTOS PARA A IoT

Alguns modelos de Arduino, como o Arduino Uno Wi-Fi, a linha Arduino MKR Wi-Fi e ainda o Arduino Yun, já contam com módulos de comunicação wireless soldados na mesma placa, o que facilita o processo de comunicação com a internet. Eles geralmente são equipados com processadores dotados de mais memória e maior poder de processamento, o que é necessário para uma comunicação com a internet (ARDUINO, 2019b).

O Arduino Uno Wi-Fi, que você pode ver na Figura 5, é um modelo de baixo custo que vem equipado com um microcontrolador com mais memória e com mais capacidade de processamento, além dos circuitos necessários para a comunicação sem fios. A programação dele é realizada na mesma interface, como um Arduino qualquer, só que, para utilizar a conectividade Wi-Fi, é necessário utilizar algumas bibliotecas específicas.

FIGURA 5 – ARDUINO UNO Wi-Fi REV.2. ESTE ARDUINO JÁ VEM EQUIPADO COM OS CIRCUITOS NECESSÁRIOS PARA A COMUNIDADE Wi-Fi



FONTE: Adaptado de Arduino (2019a)

A linha Arduino MKR é uma linha nova de Arduinos, que é marcada pela presença de processadores mais potentes e mais robustos, porém compatíveis com os demais circuitos e programas do Arduino. Dentro dessa linha, temos o Arduino MKR Wi-Fi 1010, mostrado na Figura 2, que além do processador do Arduino conta ainda com um módulo ESP32 para fazer a comunicação Wi-Fi. O módulo ESP32 é bastante popular e é considerado por muitos como um dos

melhores módulos para IoT de baixo custo disponíveis no mercado (ARDUINO, 2019d).

FIGURA 6 – ARDUINO MKR Wi-Fi 1010, NOVA LINHA DE ARDUINOS QUE CONTA COM UM MÓDULO ESP32 PARA COMUNICAÇÃO VIA Wi-Fi



FONTE: Adaptado de Arduino (2019b)

O Arduino Yun, mostrado na Figura 7, é um exemplo de Arduino que já vem pronto para projetos de IoT. Ele conta com um microprocessador Atheros AR9331 além do microcontrolador do Arduino, para cuidar de todos os protocolos de rede e da comunicação física, por Wi-Fi ou por cabo RJ45. Dessa forma, você pode programar o Arduino normalmente e ainda conta com o microprocessador adicional para cuidar de toda a comunicação de rede.

FIGURA 7 – ARDUINO YUN, PLACA QUE JÁ VEM COM SUPORTE NATIVO PARA REDE CABEADA (RJ45) E REDE WIRELESS



FONTE: Adaptado de Arduino (2019c)

5 SHIELDS DE COMUNICAÇÃO COM A INTERNET

Mesmo um Arduino que não possua um módulo Wi-Fi embutido pode se conectar à internet com o uso de *shields*, isto é, placas de expansão específicas para IoT. Por exemplo, a Ethernet Shield 2 traz todo o hardware necessário para que o

Arduino possa se comunicar com uma rede cabeada no padrão RJ45 (ARDUINO, 2019d). Existe ainda a Shield XBee, a qual utiliza um modem *Wi-Fi* que emprega o protocolo Zigbee.



A Zigbee Alliance é uma associação de várias empresas cujo objetivo é estabelecer um padrão para IoT com a premissa de otimizar o consumo energético do dispositivo. A Zigbee está consolidada desde 2002, e já existem vários projetos e produtos no mercado que utilizam o protocolo e os padrões estabelecidos por ela. Para conhecer mais sobre essa aliança consulte, acesse o link a seguir.

<https://www.zigbee.org>

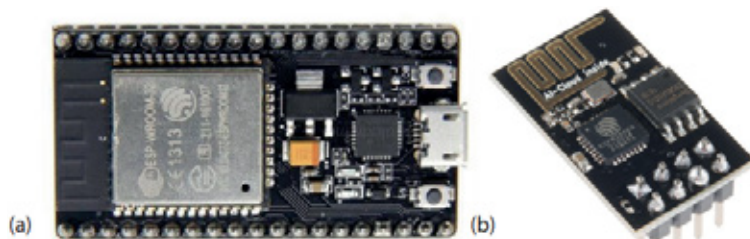
6 OUTROS MÓDULOS DE COMUNICAÇÃO PARA IoT

Além dos *shields* oficiais e os modelos de Arduino que já vêm embarcados com alguma solução para conectividade com a rede, existem ainda outros módulos que podem ser facilmente conectados ao Arduino para permitir a comunicação com a internet. Um exemplo muito interessante e de baixíssimo custo são as plataformas ESP8266 e ESP32, da Expressif, que você pode ver na Figura 8.

A diferença básica entre essas plataformas está na sua capacidade de processamento: o ESP8266 é um processador mais simples com uma capacidade menor do que o ESP32, o qual já vem equipado com processador de dois núcleos com arquitetura 32 bits. Ambas as plataformas são, essencialmente, um circuito com todo o hardware necessário para comunicação via Wi-Fi, sendo que alguns submodelos suportam ainda o protocolo Bluetooth (ESPRESSIF SYSTEMS, 2019).

O microprocessador desses módulos pode ser reprogramado para cuidar de toda a comunicação com a internet, enquanto que o Arduino fica responsável por controlar o dispositivo propriamente dito. Apesar de serem módulos muito versáteis, eles ainda carecem de certificações e testes para que sejam amplamente aceitos pelo meio industrial. Em aplicações que não necessitam do rigor exigido pelas indústrias, esses módulos são uma excelente opção.

FIGURA 8 – MÓDULOS DE COMUNICAÇÃO Wi-Fi(a) E (b) ESP8266, QUE PODEM SER CONECTADOS AO ARDUINO



FONTE: (a) ESP 32 (2018); (b) ESP8266 (2019).

Por se tratar de uma tecnologia muito nova e muito promissora, a cada dia surgem novos módulos, cada um com mais recursos e mais possibilidades. Sendo assim, recomendamos que você continue a pesquisar e estudar sobre os novos módulos e as novas tecnologias que estão disponíveis ao iniciar um projeto de IoT.

7 APLICAÇÕES PRÁTICAS PARA IoT

Vejamos agora algumas das principais aplicações que podem ser concretizadas com a IoT, utilizando o Arduino. Lembre-se: o limite para a criação de dispositivos associados à IoT está na sua imaginação.

7.1 MONITORAMENTO DE TEMPERATURA

O monitoramento remoto da temperatura de uma sala ou de um ambiente uma das aplicações mais simples para a IoT. Imagine, por exemplo, um data center com vários computadores ligados ao mesmo tempo. O técnico responsável pela manutenção desse ambiente deve saber a cada instante como está a temperatura, porque, se a temperatura se eleva muito, ela pode causar danos nos computadores. Uma solução simples é equipar um sensor de temperatura com uma placa de conexão Wi-Fi, por exemplo, para que ele envie a temperatura periodicamente para o técnico, ou ainda envie um e-mail diário com o histórico de temperaturas ao longo do dia.

Já existem dispositivos comerciais que realizam essa aplicação, inclusive alguns com a capacidade de controlar o sistema de refrigeração do ambiente caso seja detectado alguma anomalia.

7.2 AUTOMAÇÃO RESIDENCIAL

Uma aplicação muito interessante da IoT é a automação residencial, que consiste em equipar uma casa com vários dispositivos para o controle e

monitoramento remoto. Na automação residencial, é possível, por exemplo, controlar todo o sistema de iluminação por meio de um smartphone, com a IoT.

Sistemas mais complexos incluem ainda o monitoramento da presença em cada cômodo da casa, controle de acesso para as portas e para o portão da garagem e até mesmo controle de climatização. Já existem casas equipadas em que você programa o sistema para que ele saiba a hora que você sai do trabalho, de forma que, assim que você chega em casa, o aparelho de ar condicionado já está ligado e a casa já está climatizada. Com os recursos da IoT, caso você saia mais cedo do trabalho, pode enviar um comando para a casa, via internet, e todos os dispositivos se ajustam, por exemplo, o sistema de climatização.

A IoT tem um papel essencial nesse processo de automatização de uma residência. Uma forma muito interessante de se fazer toda essa automação funcionar é equipando todos os dispositivos com a conectividade com a internet, de forma que seja bastante cômodo a configuração de todos os parâmetros, além de permitir o controle deles, mesmo que você esteja fora da sua casa.

7.3 INDÚSTRIA 4.0

A Indústria 4.0 consiste em uma série de práticas que visa, acima de tudo, a permitir um maior fluxo da informação dentro do meio industrial. Os pilares fundamentais da Indústria 4.0 são o conceito de Big data, a IoT, e o processamento da nuvem (*cloud*). O conceito de Big data se relaciona ao alto volume de informações. Algumas máquinas de processo produtivo têm a capacidade de produzir esse alto volume de informações, as quais demandam processos e técnicas específicas para serem processadas a fim de produzir algum conteúdo que agregue valor ao produto (SANTOS; MANHÃES; LIMA, 2018).

Uma abordagem que permite o tratamento dessa Big data é o processamento na nuvem, isto é, por meio dos data centers (centros de processamento de dados), na qual encontramos vários computadores de grande porte conectados à internet para fazer o processamento das mais variadas informações, conforme a demanda. Essas instalações são caras e possuem um alto custo operacional, o que inviabiliza a instalação de um data center em cada indústria, daí surge o processamento na nuvem, o qual é outro pilar fundamental da Indústria 4.0.

A IoT é um dos pilares fundamentais dessa filosofia porque, por meio dela, as máquinas são capazes de enviar as informações produzidas pelo processo diretamente para a nuvem, onde esse alto volume de dados será processado por meio de data centers. Estratégias de manutenção, de produção e até mesmo de tendências de mercado podem ser obtidas pelo processamento desses dados. Com isso, as indústrias passam a ter uma base mais sólida para a tomada de decisões, o que reduz custos, acelera processos e permite fazer o produto final ter mais valor agregado.



RESUMO DO TÓPICO 2

Neste tópico, você aprendeu que:

- A Indústria 4.0 é uma filosofia em que as indústrias passam a lançar mão de novas tecnologias para que possam agregar valor ao produto e tornar o seu processo cada vez mais competitivo. E, com referência à Internet das Coisas (IoT), ela contribui sendo um dos pilares fundamentais dessa nova filosofia emergente.



- 1 A ideia central da Internet das Coisas (IoT) gira em torno de os equipamentos e os objetos terem a capacidade de se conectar na Internet. Essa conectividade traz muitos benefícios e alguns aspectos negativos. Dentre eles, o aspecto mais crítico é:
 - a) () Falta necessidade de aplicações, o que limita o processo criativo.
 - b) () Falta de módulos preparados para dar a conectividade aos dispositivos.
 - c) () Falta de aceitação do meio industrial, o que atrasa o desenvolvimento da IoT.
 - d) () Falta de padronização, o que pode acarretar falhas de segurança.
 - e) () Falta de informação técnica, o que gera muitos problemas.

- 2 A Indústria 4.0 é a nova revolução pela qual as indústrias estão passando, em busca de melhorias no processo produtivo e otimização dos custos de produção. A Internet das Coisas (IoT) é um dos pilares fundamentais dessa filosofia, pois contribui:
 - a) () Coletando e organizando informações produzidas pelas máquinas.
 - b) () Processando as informações produzidas pelas máquinas.
 - c) () Agregando valor às máquinas do processo produtivo das indústrias.
 - d) () Sendo uma ponte entre as máquinas e a equipe de manutenção.
 - e) () Acelerando o fluxo de informação produzido pelas máquinas para a nuvem.

- 3 O Arduino é uma plataforma de hardware livre, que permite o desenvolvimento de dispositivos para as mais variadas atividades. Por meio do uso de *shields* e/ou módulos específicos, ele consegue se conectar na Internet. Um módulo que vem sendo muito empregado nessa prática é o ESP32, o qual se torna bastante útil por:
 - a) () Ser um shield do Arduino responsável por conexão cabeada – RJ-45.
 - b) () Ser um shield do Arduino capaz de fazer comunicação exclusivamente por bluetooth.
 - c) () Ser um módulo de baixo custo com propriedades bem equilibradas para a demanda da IoT.
 - d) () Ser um módulo que pode ser usado no Arduino para comunicação RFID.
 - e) () Ser um módulo de alto custo com propriedades bem equilibradas para aplicações industriais.

- 4 A Internet das Coisas (IoT) se caracteriza, essencialmente, por permitir que qualquer objeto do uso diário possa, de alguma forma, conectar-se à internet. Isso implica que:

- a) () Os objetos possam estar continuamente carregados com suas baterias.
- b) () Os objetos possam enviar e receber informações e comandos conforme a necessidade.
- c) () Os objetos possam manter suas redes sociais sempre atualizadas.
- d) () A Internet vai deixar de existir para os seres humanos e somente os objetos vão usá-la.
- e) () A Internet vai ficar cada vez mais lenta com tantos objetos conectados nela.

5 A automação das residências, de forma que o proprietário possa ter controle remoto sobre os mais variados aspectos da casa, é possível graças à tecnologia da Internet das Coisas (IoT). Com esses avanços será possível, por exemplo, que uma pessoa possa programar o funcionamento da climatização da casa. Qual é o ganho direto que será obtido ao se realizar esse tipo de programação?

- a) () Menor segurança ao entrar em casa e maior economia de energia.
- b) () Maior segurança ao entrar e sair de casa.
- c) () Economia de energia elétrica e consumo de água.
- d) () Economia de energia elétrica e maior comodidade.
- e) () Maior comodidade ao preço de maior consumo elétrico.

INTRODUÇÃO À INTERNET DAS COISAS NA PLATAFORMA RASPBERRY PI

1 INTRODUÇÃO

Raspberry Pi é uma placa que pode ser utilizada como um computador de baixo custo. Com ela é possível inicializar um sistema operacional completo (geralmente os baseados em Linux) e instalar o ambiente de desenvolvimento necessário para criação de software (mais indicado, nesse caso, para Python e JavaScript). Utilizando Raspberry Pi, é possível conectar periféricos de saída, como mouse, teclado e fone de ouvido. Muitas são as utilizações dessa placa que surgiu para ser utilizada apenas para fins educacionais, proporcionando ensino de programação com computador de baixo custo, mas que evoluiu e se popularizou com uma gama enorme de utilizações e vantagens.

Neste tópico, você estudará sobre a arquitetura dessa placa explorando seus componentes básicos, bem como a forma de comunicação do Raspberry Pi com o mundo e do mundo com o Raspberry Pi, através da análise de seus protocolos de comunicação e dos componentes utilizados para ele. Ao final, vamos conferir como se desenvolve um software para IoT utilizando Raspberry Pi.

2 ELEMENTOS ARQUITETURAIS RASPBERRY PI

Nesta seção, exploraremos os componentes que fazem parte de uma placa Raspberry, buscando entender a importância de cada um deles. Estes componentes estão disponíveis na maioria das versões de Raspberry Pi, sendo que cada versão agrega, remove ou reduz recursos para se adaptar ao propósito para o qual foi desenvolvida (UPTON; HALFACREE, 2017).

System-on-chip (SoC): mais conhecido por Circuito Integrado ou Chip, é localizado próximo do centro da placa, em formato quadrado, e é o que fornece ao Raspberry as funções de processamento de propósito geral, renderização gráfica e gerenciamento de recursos de entrada e saída.

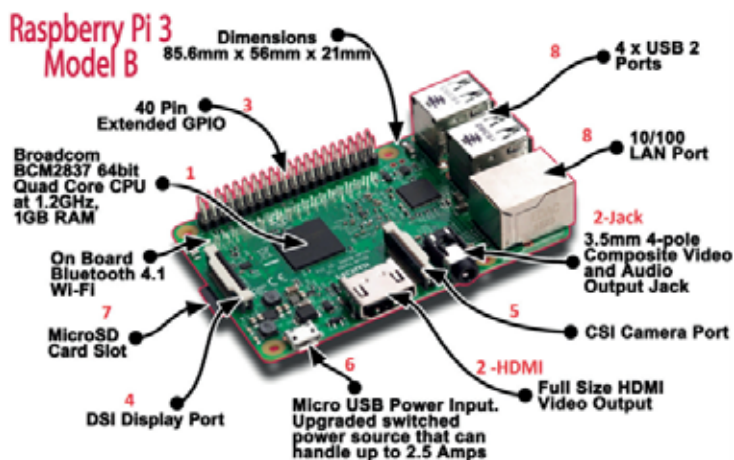
Saída de vídeo: localizada abaixo do SoC, é utilizada como sugere o nome, para saída de vídeo. Ela possui um conector High-Definition Multimedia Interface (HDMI), o mesmo que é utilizado por diversos reprodutores de mídia, como televisores, por exemplo. Possui também uma porta de vídeo para conexão com aparelhos que não possuem HDMI.

Display Serial Interface (Porta DSI): usado para conectar a sistemas de monitor de plano acionados digitalmente. Raramente utilizados, porque a porta HDMI é mais flexível. Um exemplo de uso comum desta porta é para o acessório de touchscreen oficial do Raspberry. Essa porta não está disponível para o Pi Zero.

- Câmera Serial Interface (porta CSI): fornece uma conexão de alta velocidade com o módulo de câmera.
- Soquete de energia: soquete micro USB, similar ao utilizado em smartphones. Conectando um cabo USB a uma fonte de energia, o Raspberry estará energizado.
- Entrada para cartão micros: fornece, através do cartão micros, armazenamento para o sistema operacional, programas, dados e tudo aquilo que for não volátil.
- Conectores Ethernet e USB: localizados na borda direita da placa, são utilizados respectivamente para Ethernet e para entrada de dados via USB.

A Figura 9 apresenta a placa em sua totalidade. Subsequentemente, vamos apresentar cada um dos elementos.

FIGURA 9 – PLACA RASPBERRY PI 3



FONTE: Adaptado de Mundo Eletrônica (c2020)

Um elemento de grande importância que merece destaque é o Header General-purpose input/output (GPIO): localizado na parte superior esquerda da placa, o GPIO é o elemento central de comunicação entre o Raspberry Pi e outros dispositivos de hardware programáveis. Ele é estruturado como uma sequência de diversos pinos, sendo que qualquer um dos pinos do GPIO pode ser designado (no software) como um pino de entrada ou saída e usado para uma ampla variedade de finalidades.

Na Figura 10 é possível ver o mapa dos pinos e a localização na placa, e a própria GPIO em destaque.

FIGURA 10 – GPIO. 5v (EM VERMELHO) E 3.3v (EM LARANJA) REPRESENTAM AS VOLTAGENS QUE O PINO SUPORTA COMO SAÍDA DE ENERGIA. AS PORTAS QUE SÃO TERRA ESTÃO EM PRETO; EM AMARELO SÃO OS PINOS GPIO QUE SERVEM PARA ENTRADA E SAÍDA DIGITAL DE DADOS E, EM BRANCO, DOIS PINOS EEPROM

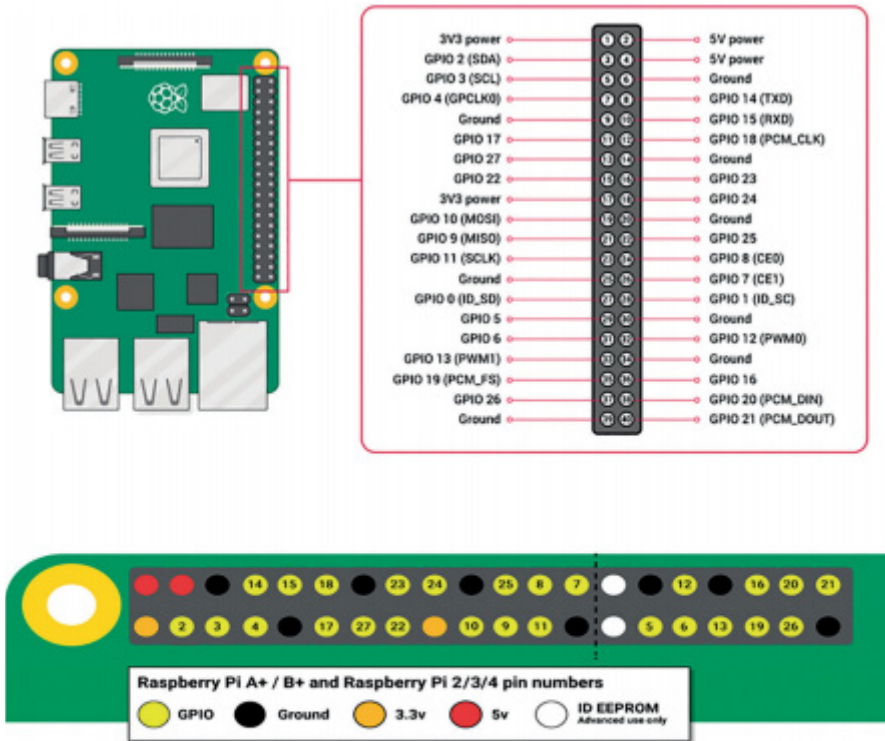


Figura 2. GPIO. 5v (em vermelho) e 3.3v (em laranja) representam as tensões que o pino suporta como saída de energia. As portas que são terra estão em preto; em amarelo são os pinos GPIO que servem para entrada e saída digital de dados e, em branco, dois pinos EEPROM.

Fonte: Raspberry Pi foundation ([2019]a, documento on-line).

FONTE: Raspberry Pi foundation (2019, s.p.)

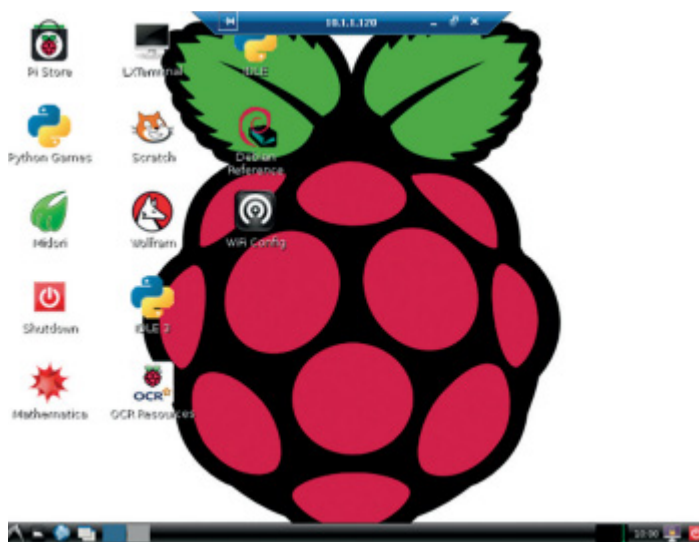
Para que você possa programar em seu Raspberry, ou mesmo inserir dados nele, é preciso instalar e inicializar o sistema operacional. O principal sistema operacional para Raspberry é o Raspbian. No Raspberry o sistema operacional é instalado diretamente no cartão microSD. Para que isso seja possível, são necessários dois passos para essa instalação, feitos em um computador qualquer: formatar o cartão e fazer a gravação do sistema operacional (EBERMAM *et al.*, 2017).

Com o sistema operacional instalado no cartão SD, o próximo passo é inicializar o Raspberry Pi. Para isso, são necessários: o cartão SD inserido, um monitor (para que você possa acompanhar o passo a passo) e uma fonte de energia. Na primeira vez em que for inicializado, o Raspberry exibirá a ferramenta Raspi-

config. Ao finalizar suas configurações, se o sistema operacional não se reiniciar sozinho, utilize a tecla TAB e selecione Finish.

A Figura 11 mostra a tela inicial do Raspbian. No desktop já encontramos as ferramentas de programação Scratch e Python, além do navegador Midori e do LXTerminal (EBERMAM *et al.*, 2017).

FIGURA 11 – ÁREA DE TRABALHO DO RASPBERRY



FONTE: Goulart (2014, s.p.).

3 COMUNICAÇÃO DO RASPBERRY COM O MUNDO EXTERIOR

Uma das principais formas de comunicação do mundo exterior com a placa Raspberry é através da GPIO (generated-purpose input-output). Essa porta possui duas fileiras com 20 pinos e pode ser utilizada tanto para entrada quanto para saída de dados. Entre estes pinos encontram-se oito pinos para uso geral que podem operar em três estados: estado alto com tensão positiva de 3,3V; estado baixo em que são terra (0v) ou como entrada. Além desses pinos de uso geral, há pinos dedicados a barramentos, sendo eles os barramentos: UART (Universal Asynchronous Receiver/ Transmitter), SPI (Serial Peripheral Interface) e I²C (Inter-Integrated Circuit).

- UART fornece uma interface serial com dois fios, esse barramento é utilizado como porta para mensagens e quando conectado a um dispositivo capaz de exibir dados, por exemplo, um monitor é capaz de exibir mensagens do núcleo o Linux sendo uma ferramenta muito útil para o diagnóstico de problemas (UPTON; HALFACREE, 2017). A comunicação neste barramento ocorre através do protocolo UART, que é um protocolo assíncrono em que existe qualquer

signal de relógio que marque a cadência a que os bits são enviados/recebidos (MENDONÇA, 2015).

- I²C estabelece a comunicação entre vários circuitos integrados, sendo que, um desses circuitos é o processador Soc. Esses pinos se conectam a resistores de pull-up do próprio Pi, não sendo necessário resistores externos. Ele é acessado nos pinos 3 e 5 (UPTON; HALFACREE, 2017).
- SPI é um barramento serial síncrono, full duplex, com um desempenho superior ao I²C, possui quatro fios e várias linhas que permitem se comunicar com mais de um dispositivo de destino. Está disponível nos pinos 19, 21 e 23. Este barramento trabalha em uma estrutura mestre escravo onde o gerador do sinal de sincronismo é definido como o Mestre (Master) da comunicação e os dispositivos que utilizam do sinal de sincronismo chamados de Escravo (Slave). Cada pino neste barramento tem um papel específico, o pino 19 fornece sinal MOSI (Master Output, Slave Input), o pino 21 oferece o sinal MISO (Master input, Input output) pino 23 oferece o SLCK (serial clock) usado para sincronizar a comunicação. Os pinos 24 e 26 fornecem os sinais chip select para até dois escravos independentes (UPTON; HALFACREE, 2017).



O Raspberry Pi não tem um interruptor de energia, para desligá-lo utilize o botão de logout ou o comando `pi@raspberrypi ~ $ sudo shutdown -h now`. Faça o desligamento corretamente, pois, se desligar brutalmente tirando da tomada, o cartão SD pode ser corrompido.

4 APLICAÇÕES DE IoT NO RASPBERRY PI

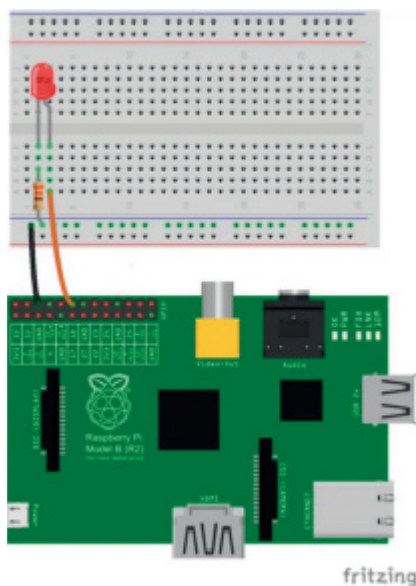
A Internet das Coisas se caracteriza como uma revolução tecnológica que tem por objetivo colocar literalmente todas as coisas conectadas na internet, permitindo, por exemplo, que sua geladeira se comunique com o seu celular. E como será que o Raspberry Pi pode ser utilizado neste contexto? É sobre isso que vamos estudar nesta seção.

O Raspberry Pi, por ser uma placa que permite a criação de circuitos eletrônicos mas que se assimila muito a um computador, por ter um sistema operacional, processamento próprio e armazenamento, pode ser utilizado para realização da comunicação entre dispositivos e para a automação de tarefas. Neste sentido, faz-se necessário desenvolver software específicos, que podem ser desde software simples com comandos lógicos - por exemplo, uma ação ou outra — até software mais complexos que envolvem comandos encadeados e loopings.

Vamos conhecer como é desenvolvido um sistema em Python e Raspberry para o acionamento de um light emitting diode (LED), que significa “diodo

emissor de luz”. Primeiramente, analisaremos o hardware. É necessário um LED, um resistor, uma protoboard e, claro, uma placa de Raspberry. O primeiro fio na imagem da Figura 12 está conectado ao pino 3 (GND), mas poderia ser conectado a qualquer outro pino GND. O segundo fio na imagem da Figura 12 está conectado ao pino 18, mas poderia estar conectado a outro pino GPIO. A partir do pino 18 que vamos controlar e definir se o LED está aceso ou apagado. O LED deve ser conectado com a sua parte maior (a perna curvada) no lado energizado, ou seja, na mesma linha vertical que o cabo que está ligado ao pino 18 quando estiver conectado. O outro lado do LED deve ser conectado alinhado verticalmente com o resistor, que, por sua vez, deverá ter uma ponta conectada logo abaixo do LED e outra ponta conectada na linha (-) da placa.

FIGURA 12 – CIRCUITO PARA ACENDIMENTO DE UM LED



FONTE: Tecnotronics (2017, s.p.)

Depois, considerando que o seu Raspberry já tem o Python instalado, você criará um arquivo com o código a seguir, Figura 13, em que, nas linhas 1 e 2, são feitas as importações das bibliotecas; na linha 3 é criada uma variável que é atribuída a um pino; na linha 4 é iniciado um laço de repetição; na linha 5 acendido o LED; na linha 6 aguardado 1 segundo; na linha 7 desligado o LED; na linha 8 aguardado um segundo; e então, como o código está dentro de um laço, o fluxo se repete e o LED fica piscando.

FIGURA 13 – CÓDIGO DE ACENDIMENTO DO LED

```
from gpiozero import LED
from time import sleep

led = LED(17)

while True:
    led.on()
    sleep(1)
    led.off()
    sleep(1)
```

FONTE: Raspberry Pi Foundaion (2019, s.p.)

Alternativamente, você poderia utilizar o comando `blink()`, que faz com que o LED pisque, reduzindo o tamanho do seu código. Utilizando este projeto simples como exemplo, você pode dar o primeiro passo para a construção de muitos outros projetos para a Internet das Coisas. Além disso, na página oficial do Raspberry, você pode visualizar muitos outros projetos para que você possa explorar a sua criatividade.



RESUMO DO TÓPICO 3

Neste tópico, você aprendeu que:

- Raspberry Pi é uma placa de microntrolador que tem função de minicomputador. Nela é possível instalar um sistema operacional, criar e executar programas como em um computador normal, contudo com um custo muito mais acessível.



- 1 Diversos são os elementos que formam as placas Raspberry, cada um com uma função específica. Sobre esses componentes, analise as afirmativas a seguir e assinale aquela que contém o nome e a descrição correta de um desses componentes.
 - a) () A saída de vídeo utilizada pelo Raspberry é exclusivamente HDMI.
 - b) () A porta DSI fornece uma conexão de alta velocidade com o módulo de câmera.
 - c) () Micro SD é a parte fundamental do Raspberry, pois é nele que acontece todo o processamento envolvido nesse tipo de computador.
 - d) () Circuito integrado ou chip é onde estão armazenados os programas e os dados utilizados pelo computador.
 - e) () Soquete de energia é um soquete micro USB que, quando conectado a uma fonte de energia, fornece energia para o computador.

- 2 Raspberry é um tipo de computador de baixo custo que foi criado para fins educacionais e se popularizou, permitindo inclusive realizar programação diretamente no Raspberry quando conectado a um dispositivo de vídeo e a periféricos, como mouse e teclado. Diversas são as versões de Raspberry Pi disponíveis. Sobre essas versões, analise as afirmativas a seguir e assinale a afirmativa correta.
 - a) () Todos os modelos de Raspberry Pi até a versão Raspberry Pi 4 têm GPIO de 40 pinos.
 - b) () O modelo Raspberry Pi 2 utiliza o SoC BCM2837.
 - c) () O modelo Raspberry Pi 4 pode ter até 4GB de memória RAM.
 - d) () O modelo Raspberry Pi Zero tem duas saídas USB.
 - e) () O modelo Raspberry Pi Zero não tem GPIO.

- 3 Para o Raspberry se comunicar com o mundo exterior, uma das formas mais comuns é por meio da utilização da GPIO (generated-purpose input-output). Sobre a comunicação por meio desse componente, analise a afirmativa que apresenta corretamente a sigla e a descrição barramento desse componente.
 - a) () UARB - Universal Asynchronous Receiver/Bus.
 - b) () PPI - Parallel Peripheral Interface.
 - c) () SPI - Sistem Peripheral Interface.
 - d) () I²C - Integrated Circuit.
 - e) () UART - Universal Asynchronous Receiver/Transmitter.

- 4 As placas Raspberry têm uma estrutura chamada GPIO, que é utilizada para interação com dispositivos externos programáveis. Uma das principais linguagens utilizadas em desenvolvimento para Raspberry é a linguagem

Python, em conjunto com a biblioteca GPIO Zero. Sobre desenvolvimento em Python e a biblioteca GPIO Zero, analise as afirmativas a seguir e classifique em verdadeiro ou falso.

- I. Para identificar qual pino da GPIO está sendo utilizado em programa que visa ao acendimento de um LED, utiliza-se o comando variável = LED (número do pino).
- II. Uma alternativa para fazer um LED piscar em Python é utilizando o comando Blink, que substitui a necessidade de escrever códigos para acender, pausar e desligar.
- III. O comando Sleep, utilizado da linguagem de programação Python e parte da biblioteca time.h, tem como finalidade exclusiva a utilização em programação para Raspberry.
- IV. Se remover o comando Sleep utilizando Python e a biblioteca GPIO Zero, o acendimento do LED não irá funcionar, porque não existirá tempo hábil para efetuar o processamento de acender e apagar.
- V. Mesmo utilizando o comando Blink, é necessário utilizar um laço de repetição para ver o efeito do LED acender e apagar múltiplas vezes. Caso contrário o LED irá piscar apenas uma vez.

- a) () Estão corretas as afirmativas I e II.
- b) () Estão corretas as afirmativas I, II e IV.
- c) () Estão corretas as afirmativas I e V.
- d) () Estão corretas as afirmativas I, II, III e IV.
- e) () Estão corretas as afirmativas I e IV.

5 O Arduino e o Raspberry têm características similares que os tornam tecnologias concorrentes no mercado de IoT. Sobre essas duas tecnologias, analise as afirmativas a seguir e assinale a afirmativa correta.

- a) () O Arduino é mais indicado para a execução de softwares complexos, por exemplo, com estruturas de decisão aninhadas.
- b) () O Arduino tem maior adaptabilidade para a instalação de sistemas operacionais diversos.
- c) () O Raspberry tem como vantagens, em relação ao Arduino, o fato de não necessitar de protoboard e por ser utilizado em circuitos mais simples.
- d) () O Raspberry tem como vantagem, em relação ao Arduino, o fato de ter sistema operacional, o que torna o desenvolvimento mais simples.
- e) () O Raspberry tem como vantagem, em relação ao Arduino, o fato de existirem mais shields compatíveis.

RASPBERRY PI E SUAS APLICAÇÕES

1 INTRODUÇÃO

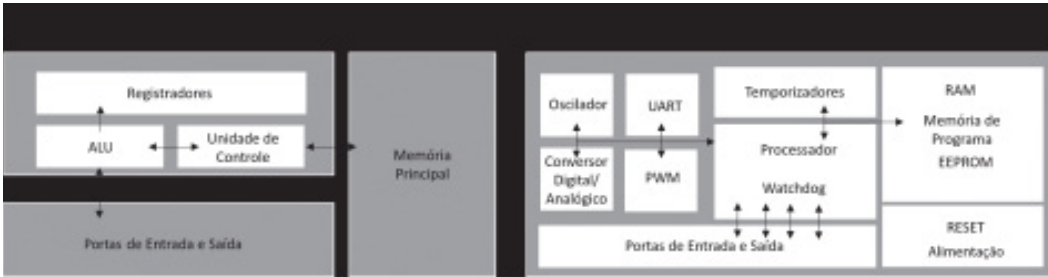
Muito associados aos microprocessadores, os microcontroladores são bem mais que uma mera unidade central de processamento, pois contêm em todo seu invólucro periféricos que lhes permitem efetuar muitas funções sem depender de outros componentes a eles conectados. Um microcontrolador é um circuito versátil em aplicações de sistemas digitais, havendo no mercado um grande número de fabricantes e famílias, com suas especificidades e características, para as mais diversas aplicabilidades. Dessa forma, a escolha do circuito integrado que irá compor “o coração” do seu projeto é de grande importância e varia de aplicação para aplicação.

Neste tópico, você conhecerá as principais características das placas Raspberry Pi. Além disso, verá como configurá-las para diferentes aplicações e encontrará exemplos de sua utilização.

2 PLACAS RASPBERRY PI

Sistemas embarcados difundiram-se em meados da década de 1970, devido a diversos avanços tecnológicos, como a substituição das válvulas por transistores. Consequentemente, microcontroladores tornaram-se altamente aceitos pela comunidade tecnológica, principalmente por hobbistas, uma vez que microcontroladores são chips que contêm em seu invólucro os componentes básicos, como processador, memória RAM, memória ROM, periféricos de entrada e saída, dentre outros, exigindo somente energia para seu funcionamento, ao contrário dos microprocessadores, que requerem componentes externos para funcionar, conforme ilustrado Figura 14. Com isso, a utilização de microcontroladores torna-se tão fácil quanto dispositivos plug-and-play.

FIGURA 14 – MICROPROCESSADOR *VERSUS* MICROCONTROLADOR



Atualmente, há no mercado diversas opções de microcontroladores, também conhecidos como System on Chip (SoC), para as mais variadas aplicações. Eles tendem a apresentar um poder de processamento limitado, como palavras de 8 bits, assim como baixa frequência. Tal limitação abre espaço para placas que possuem microprocessadores mais velozes, como aqueles das famílias x86 e ARM.

Dentre esse universo de opções, um módulo que tem se destacado em aplicações maiores e mais robustas é o conhecido como Raspberry Pi. Trata-se de um projeto de hardware aberto, ou seja, o projeto está livre para que as pessoas da comunidade possam construir, modificar, distribuir e utilizar esses artefatos, que utilizam processadores da família ARM. De acordo com o site oficial da Raspberry Foundation, as placas Raspberry foram desenvolvidas com o intuito de fomentar o ensino da ciência da computação básica em escolas, promovendo a inclusão e empoderamento social.

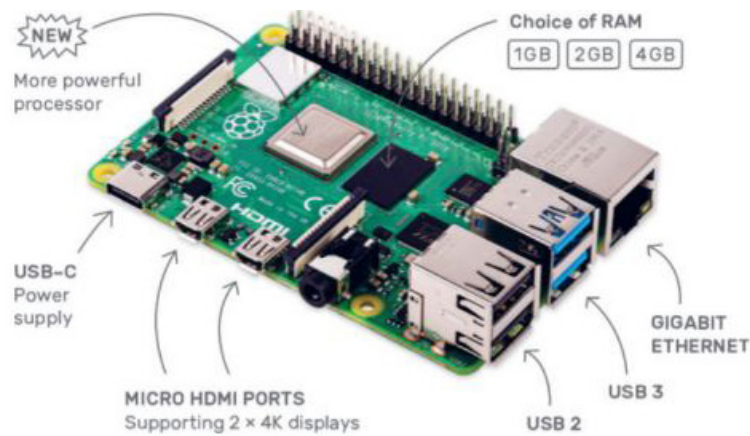


Você pode acessar e conferir o site oficial da Raspberry Foundation pelo link a seguir.

<https://qr.go.page.link/9W9Yd>

O projeto é viabilizado devido ao fato do Raspberry Pi ser capaz de funcionar como um “minicomputador”, trazendo em seu invólucro uma entrada HDMI para se conectar a um monitor e, em certos modelos, uma conexão do tipo flat para acoplar módulos de telas sensíveis ao toque (touch), entradas USB para conectar dispositivos de entrada e saída, como mouse e teclado, ou até mesmo pendrive e HD externo para armazenamento de dados (OLIVEIRA, 2017). Há modelos com memória RAM que varia de 1 a 4 GB e conexão Ethernet para conectar-se à Internet, suprimindo, dessa forma, as configurações necessárias para executar funções básicas em um computador, como editar textos e planilhas, navegar na Internet e elaborar códigos simples. Tais características podem ser observadas na Figura 15.

FIGURA 15 – IMAGEM PROMOCIONAL DIVULGADA PELA RASPBERRY FOUNDATION PARA A PLACA RASPBERRY PI 4



FONTE: Raspberry Pi Foundation (2019a, s.p.).

No mercado atual, é possível encontrar oito modelos de placas Raspberry Pi. A Tabela 1 traz um comparativo entre elas.

TABELA 1 – COMPARATIVO ENTRE OS MODELOS DE PLACAS RASPBERRY PI

Modelo	Processador	Núcleos	Clock CPU	RAM	Wireless e Bluetooth
Raspberry Pi A+	ARM1176JZF-S	1	700 MHz	256 MB	Não
Raspberry Pi Model B	ARM1176JZF-S	1	700 MHz	512 MB	Não
Raspberry Pi 2	Cortex-A7	4	900 MHz	1 GB	Não
Raspberry Pi Zero	ARM1176JZF-S	1	1 GHz	512 MB	Não
Raspberry Pi Zero W	ARM1176JZF-S	1	1 GHz	512 MB	Sim
Raspberry Pi 3	Cortex-A53 64 bits	4	1.2 GHz	1 GB	Sim
Raspberry Pi Model B+	Cortex-A53 (ARMv8) 64 bits	4	1.4 GHz	1 GB	Sim
Raspberry Pi 4	ARM Cortex-A72	4	1.5 GHz	1 a 4 GB	Sim

FONTE: Adaptado de Raspberry Pi Foundation (2019b)

De acordo com o site oficial da Raspberry Foundation, os sistemas operacionais disponíveis para as placas são: Risc OS, Windows IoT Core, Ubuntu Core, Linutop, Raspbian, dentre outros. O sistema operacional oficial das placas Raspberry é o Raspbian. Além da possibilidade de instalação de sistemas operacionais “convencionais”, ainda é possível transformar a placa Raspberry em entretenimento, executando sistemas operacionais como o projeto Retropie, uma biblioteca baseada em Debian que permite emular jogos em Raspberry, tendo até a possibilidade da utilização de joystick, uma vez que a placa disponibiliza entradas USB. Há também o OpenElec, um projeto baseado em Linux que permite que o usuário transforme sua placa em uma central de mídia. Além disso, as placas Raspberry oferecem portas configuráveis para que possam ser desenvolvidos projetos de controle e automação. Para a programação das portas General Purpose Input/Output (GPIOs), ou até mesmo para exercitar a programação, o Raspberry oferece ambientes de desenvolvimento para linguagem Python, C, Scratch, Java, QTCreator, Node-RED e Mathematica (similar ao WolframAlfa).

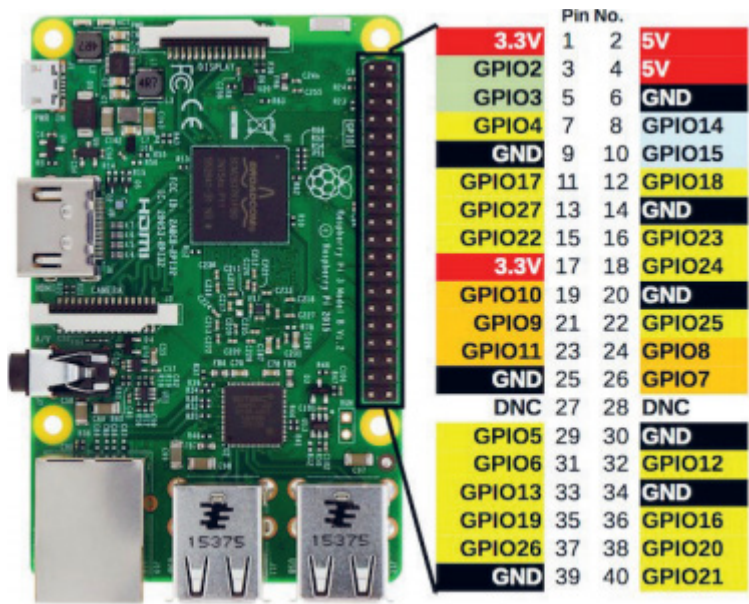


Ao iniciar um projeto, busque uma placa de acordo com o seu escopo, e não somente por ser a mais atual ou considerada como a que possui a “melhor” configuração. Isso pode custar caro em um projeto, pois se os requisitos forem simples e você optar pela placa mais completa, terá um alto custo energético e manterá grande parte de seus componentes ociosos, podendo trazer desvantagens para seu produto final.

3 RASPBERRY PI: COMO USAR

Como mencionado na seção anterior, as placas Raspberry oferecem pinos que podem ser programados de acordo com a necessidade do projeto. Na Figura 16, é possível observar o esquema de pinos configuráveis da placa Raspberry Pi 3 Model B.

FIGURA 16 – RASPBERRY PI 3 MODEL B



FONTE: Raspberry Pi Robotics (2019, s.p.).

Os pinos funcionam como interface entre a placa e outros módulos. Nesse caso, a placa Raspberry Pi 3 Model B possui 26 pinos GPIOs, ou seja, que podem enviar e receber mensagens de outros módulos; quatro pinos de energia, sendo dois de 5 V e dois de 3,3 V; oito pinos-terra (GND); e algumas placas trazem as portas 27 e 28 como do not connect (DNC) ou como ID_SC, que permite alterações direto na memória Electrically-Erasable Programmable Read-Only Memory (EEPROM) do dispositivo, por meio de pulsos elétricos internos ou externos. Possui também portas RS-232 para envio e recebimento de sinal digital e algumas GPIOs que permitem a comunicação Serial Full Duplex Síncrono, ou seja, com envio e recebimento de dados de outros dispositivos de forma simultânea, desde que se implemente o protocolo necessário (UPTON; HALFACREE, 2014).



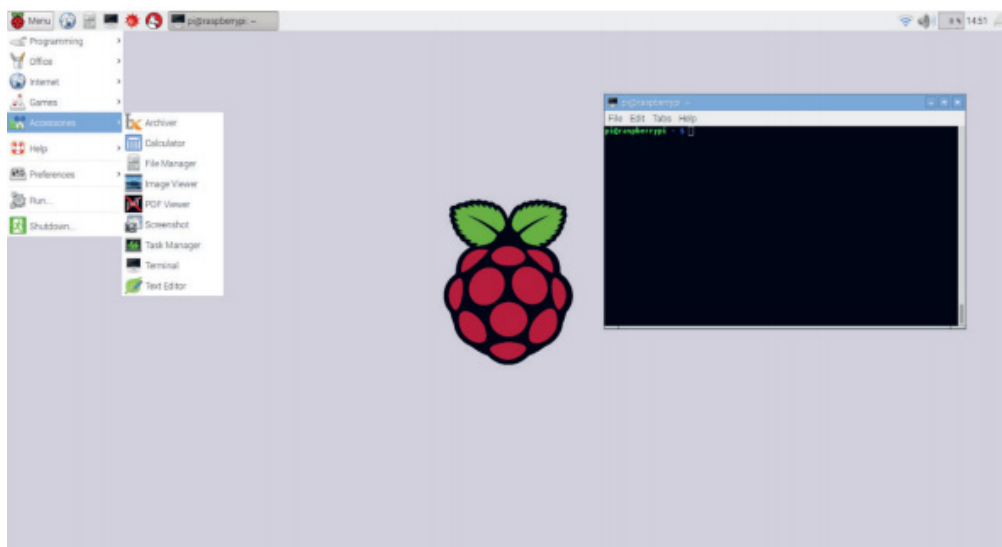
É necessário tomar um certo cuidado com as saídas de alimentação com tensão de 5 V, uma vez que as GPIOs não possuem um sistema de proteção como as utilizadas em placas Arduino, em que lógica digital TLL com 5 V representa o nível lógico alto. Para o Raspberry, o nível lógico alto é de 3,3V; portanto, se o curto for fechado entre a porta com 5 V e as demais GPIOs, aplicando uma tensão maior do que o esperado, isso pode vir a danificar não apenas o pino como a placa inteira.

Atualmente, em projetos de automação residencial, tem-se buscado conectar o objeto foco de automação à Internet, visando proporcionar praticidade e conforto ao executar certas tarefas, como acionar lâmpadas, monitorar câmeras, travar portas, dentre outras, por meio de dispositivos celulares. Para isso, o Raspberry possui a vantagem de oferecer em seu encapsulamento conectividade Wi-Fi, Ethernet e, em alguns módulos, até Bluetooth, o que facilita o desenvolvimento de projetos, uma vez que não é necessário comprar módulos à parte para conectividade.

Para desenvolver projetos utilizando as placas Raspberry, inicialmente necessário instalar um sistema operacional como o mencionado na seção anterior. Aqui, iremos exemplificar o uso com o sistema operacional oficial, Raspbian. O sistema operacional pode ser instalado via imagem do Raspbian ou pela imagem Noobs, que baixa o Raspbian diretamente no Raspberry.

Na Figura 17, é possível observar a área de trabalho do sistema operacional Raspbian.

FIGURA 17 – ÁREA DE TRABALHO RASPBIAN



FONTE: Henrique (2016, s.p.).



No link disponível a seguir, você pode aprender um pouco mais sobre o padrão de comunicação RS-232, atualmente utilizado em diversos dispositivos para enviar e receber dados.

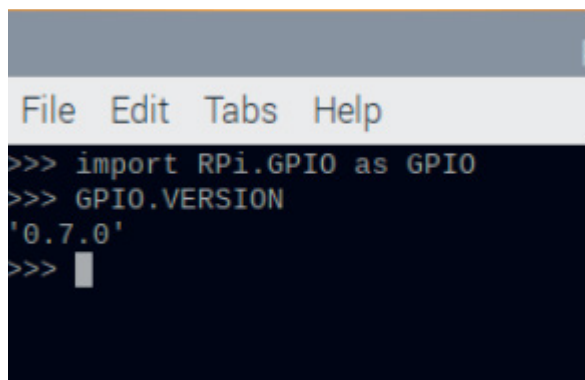
<https://qrگو.page.link/kHQLt>

O sistema operacional cumpre com seu objetivo de oferecer um “minicomputador” de baixo custo, pois com ele é possível executar funções computacionais básicas como: navegar na Internet (possui o navegador Chromium); editar planilhas, texto, slides, dentre outros, por meio do pacote LibreOffice; reproduzir áudio e vídeo; aceitar conexões de teclado e mouse; rodar alguns jogos; e apresentar por padrão alguns ambientes de desenvolvimentos instalados, como o IDLE para Python. Após a instalação do sistema operacional, é importante executar o comando `apt-get update` e `apt-get upgrade` para atualizar o sistema e a lista de pacotes instalados (RICHARDSON; WALLACE, 2013).

4 PROJETOS COM RASPBERRY

Uma vez instalado o sistema operacional, para começar a programar as GPIOs, primeiramente é necessário verificar se o Python está instalado e se a biblioteca `RPi.GPIO` está instalada. Caso não esteja, basta digitar o comando `pip install RPi.GPIO`. Na Figura 18, é possível observar a importação dessa biblioteca.

FIGURA 18 – IMPORTAÇÃO DA BIBLIOTECA `RPi.GPIO`



```
>>> import RPi.GPIO as GPIO
>>> GPIO.VERSION
'0.7.0'
>>> 
```

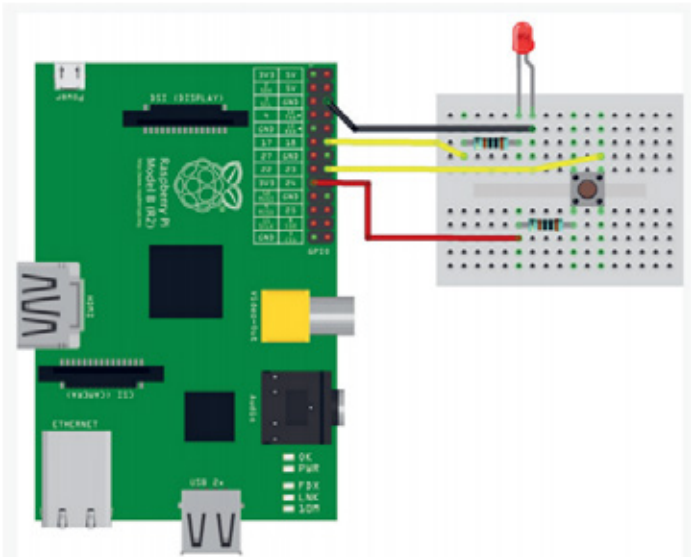
FONTE: O autor

Cumprida essa etapa, a biblioteca `RPi.GPIO` permitirá escrever nas portas do Raspberry Pi.

Acendendo um LED

Vamos agora criar o projeto de um circuito para acender e apagar uma luz de LED. Para isso, serão necessários uma luz de LED, dois resistores de 1 K, um push button, alguns jumpers e um Raspberry Pi. Na Figura 19, é possível observar o esquema do projeto.

FIGURA 19 – ESQUEMA DO PROJETO PARA ACENDER E APAGAR UMA LUZ DE LED



FONTE: ARAÚJO (2014, s.p.).

Para criar a codificação na linguagem Python, o Raspbian oferece o ambiente de desenvolvimento IDLE, mas é possível instalar outros ambientes de desenvolvimento ou até mesmo codificar pelo terminal. Para codificação deste projeto, foi utilizado o editor Mu.

FIGURA 20 – CÓDIGO DO PROJETO

```

Mu 1.0.2 - teste.py
File Edit View Help
New Load Save Run Debug REPL Plotter Zoom-in Zoom-out Theme
teste.py
1 # Write your code here :-)
2 import RPi.GPIO as GPIO
3
4 GPIO.setmode(GPIO.BOARD)
5 # GPIO.setmode(GPIO.BCM)
6
7 GPIO.setup(12, GPIO.OUT)
8 GPIO.setup(16, GPIO.IN)
9
10 while(True)
11     if GPIO.input == False
12         GPIO.output(12,1)
13     if GPIO.output == True
14         GPIO.output(12,0)
15
16 saved file: /home/pi/mu_code/teste.py
```

FONTE: O autor



Para acessar o Mu (code with Mu), um editor simples de Python para programadores iniciantes, basta acessar o link a seguir.

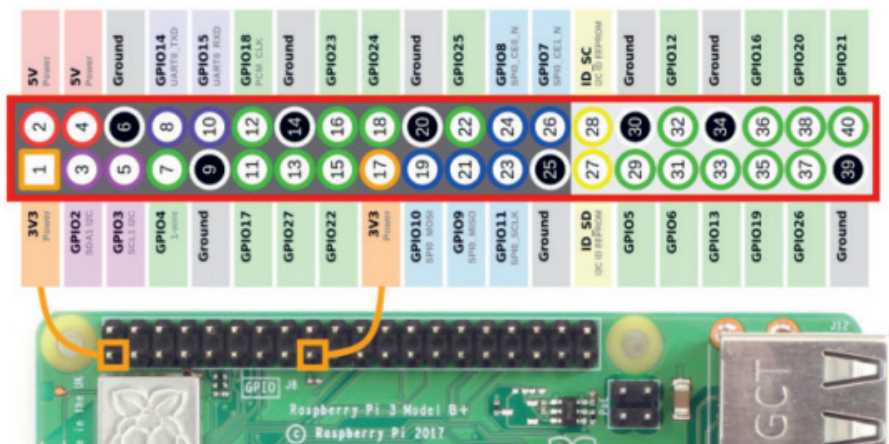
<https://codewith.mu/>

Ao contrário de outras linguagens, o Python utiliza o caractere “#” para iniciar um comentário, como é exposto na linha 1. Na linha 2, é feita a importação da biblioteca responsável por controlar as GPIOs. Caso a biblioteca não esteja instalada no Raspbian, ao ser executado, o script apontará um erro nessa linha. Nas linhas 4 e 5, é especificado para a biblioteca o modo como os pinos do Raspberry serão programados. A diferença entre ambas (UPDOWN; HALFWAVE, 2014) são:

- GPIO.BOARD: quando selecionada esta opção, fica determinado que a numeração que vem descrita/impressa na placa será utilizada como referência para codificação, sendo mais fácil de visualizar e localizar ao montar um projeto.
- GPIO.BCM: BMC é a sigla de Broadcom SOC Channel; assim, quando esta opção é selecionada, fica determinado que será utilizada a numeração interna da pinagem. A desvantagem de se utilizar esta opção é que em cada modelo das placas Raspberry a pinagem é diferente, sendo sempre necessário atentar para o circuito exposto em seu respectivo datasheet.

Na Figura 21, é possível observar a diferença de numeração das duas opções de manipulação das GPIOs.

FIGURA 21 – PINAGEM DA PLACA RASPBERRY PI 1 MODEL B REVISÃO 2.0



FONTE: Hawkins (2012, s.p.).

Tomando como exemplo o pino com numeração 16 dentro do círculo, tem-se a numeração 16 para a opção GPIO.BOARD e 23 para a opção GPIO.BCM. Dessa forma, é preciso examinar com atenção a opção selecionada no código e a pinagem da placa, pois descuidos podem causar danos à placa, uma vez que não possui proteção.

Para o código do exemplo (linha 4), foi selecionada a opção GPIO.BOARD. Nas linhas 7 e 8, são feitas as configurações dos pinos que serão utilizados, sendo o pino 12 para saída, que será responsável por acender o LED, e o pino 16 para entrada, que será responsável por ler a ação no botão. Na linha 10, é iniciado um loop, para que a placa sempre repita o código que vem logo abaixo. Na linha 11, é feita a verificação de se o botão, que está conectado no pino de entrada, não está pressionado; caso não esteja pressionado, o LED será aceso na linha 12. O parâmetro "12.1" significa que está sendo enviado o sinal 1 para o pino 12, ou seja, sinal alto. Nas linhas 13 e 14, é feita a verificação oposta. A lógica estudada pode ser utilizada para projetos maiores, como os de automação residencial.

5 ESTAÇÃO METEOROLÓGICA

Como já foi mencionado, a Raspberry Foundation está constantemente incentivando a difusão da ciência da computação. Um exemplo disso foi sua parceria estabelecida com a Oracle em 2014, em que juntas desenvolveram um kit de estação meteorológica, com um programa de treinamento para escolas, para que pudessem criar suas próprias estações meteorológicas. Esse projeto pode ser observado na Figura 21.

Há também a possibilidade de criar um servidor BitTorrent a partir de um Raspberry Pi. Para isso, basta instalar um sistema operacional, de preferência o Raspbian, e, em seguida, instalar o acesso SSH. As etapas passo a passo são as seguintes:

- digite no terminal: `sudo raspi-config`;
- selecione a opção Interface Options e pressione Enter;
- selecione a opção SSH;
- aparecerá duas janelas; basta confirmar com Yes e OK;
- digite no terminal: `sudo systemctl enable ssh`;
- digite no terminal: `sudo systemctl start ssh`.

Com o SSH habilitado, crie um arquivo `setup.sh` e insira as informações a seguir (SNAPDRAGON TECH BLOG, 2012):

```
[cc lang="bash" width="100%" height="600" noborder="1" line _
umbers="on" theme="dawn"]

#!/usr/bin/env bash

Installs all components needed for a nice seedbox on your new
```

raspberrypi.

Base image: <http://www.linuxsystems.it/2012/06/debian-wheezy-raspberrypi-minimal-image/>

Prepared by manu (at) snapdragon.cc

echo "[+] Updating packages" apt-get update ; apt-get -y upgrade

echo "[+] Installing Samba and Transmission packages" apt-get -y install transmission-daemon samba avahi-daemon

echo "[+] Configuring Transmission"

service transmission-daemon stop sed -i -re 's/(rpc-authentication-required\":\)([a-z]+)*\/\1false/g' /etc/transmission-daemon/settings.json

sed -i -re 's/(rpc-whitelist-enabled\":\)([a-z]+)*\/\1false/g' /etc/transmission-daemon/settings.json

sed -i -re 's/(download-dir\":\)([a-z]+)*(.*)\/\1\"\/srv\/media\"/,g' /etc/transmission-daemon/settings.json service transmission-daemon start

echo "[+] Setting up public Samba share"

mkdir /srv/media

chown debian-transmission /srv/media

echo "[public]

comment = Public Shares

browsable = yes

path = /srv/media

public = yes

writable = yes

quest ok = yes" >> /etc/samba/smb.conf service samba restart [/cc]

Salve o arquivo, execute com o comando `./setup.sh` e desfrute de seu servidor.

6 FLIPERAMA

Para passar o tempo e se divertir, é possível também construir um fliperama com o Raspberry. Inicialmente, é necessário baixar a imagem do Retropie, o sistema operacional para executar os emuladores de games antigos. Após instalar, é necessário fazer a configuração do sistema operacional cumprindo os seguintes passos:

```

sudo raspi-config;
selecione Advanced Options;
selecione Expand Filesystem e aguarde o final da configuração;
selecione Advanced Options e dentro dessa opção selecione SSH,
depois
ENABLE;
selecione Overclock e configure para Medium;
selecione Finish;

```

reinicie o Raspberry para atualizar as configurações.

Realizadas essas configurações, seu RetroPie estará pronto. Basta inserir as ROMS dos jogos, por meio do próprio cartão SD com o sistema operacional, pendrive ou até mesmo pela rede. Após inserir as ROMS, é importante reiniciar o Raspberry para que ele possa reconhecer os jogos, e conforme os jogos de diversos consoles forem sendo inseridos, a capa referente a cada um deles surgirá na tela para o usuário selecionar. Dentre outras configurações que podem ser feitas está a configuração de áudio:

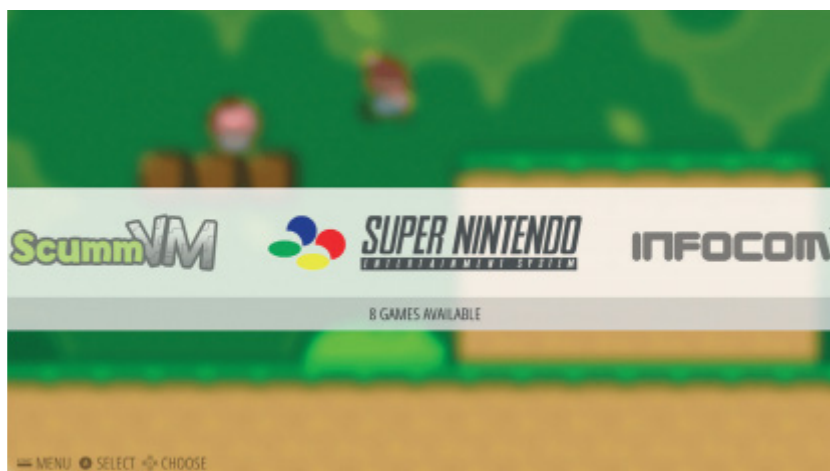
```

amixer cset numid=3 1 — para ligar o áudio pelo fone;
amixer cset numid=3 2 — para ligar o áudio por HDMI.

```

Para configurar os controles do teclado, basta manter pressionado qualquer tecla que aparecerá uma tela para efetuar a configuração; posteriormente basta configurar como desejar. Na Figura 22, é possível observar a tela inicial do RetroPie. Além do RetroPie, há outras opções, como o RetroArch.

FIGURA 22 – RETROPIE



FONTE: Pipplware (2015, s.p.).

RESUMO DO TÓPICO 4

Neste tópico, você aprendeu que:

- Os sistemas embarcados difundiram-se em meados da década de 1970, graças aos avanços tecnológicos e com a substituição das válvulas por transistores.
- Hoje temos no mercado diversas opções de microcontroladores, também conhecidos como System on Chip (SoC), um módulo que tem se destacado em aplicações maiores e mais robustas é o conhecido como Raspberry Pi.
- Nos projetos de automação residencial, tem-se buscado conectar o objeto foco de automação à Internet, visando proporcionar praticidade e conforto ao executar certas tarefas, como acionar lâmpadas, monitorar câmeras, travar portas, dentre outras, por meio de dispositivos celulares. Para isso, o Raspberry possui a vantagem de oferecer em seu encapsulamento.
- Como criar um projeto para acender e apagar uma luz de led, codificando em Python.



1 Para que as placas Raspberry Pi possam ser utilizadas, é necessário que seja instalado um sistema operacional. Assinale a alternativa que apresenta as opções de sistemas operacionais disponíveis para instalação no Raspberry Pi.

- a) () Raspbian, MacOS e Ubuntu Core.
- b) () Windows IoT Core , Ubuntu Core e Raspbian.
- c) () Android, Linutop e Risc Os.
- d) () CyanoGen, Ubuntu e Windows 10.
- e) () Windows 7, Ubuntu Core e Raspbian.

2 Para que seja possível programar os pinos do Raspberry, é necessário importar uma biblioteca nativa e, ainda, selecionar seu modo de operação. Selecione a alternativa que apresenta a biblioteca que deve ser importada, bem como o modo de operação.

- a) () Biblioteca Python.GPIO. Modos Board e BCM.
- b) () Biblioteca RPi.GPIO. Modos Board e BCM.
- c) () Biblioteca RPi.Numpy. Modos Board e BCM.
- d) () Biblioteca Django. Modos Board e BCM.
- e) () Biblioteca Selenium. Modos Board e BCM.

3 No sistema operacional oficial do Raspberry, o Raspbian, são disponibilizadas algumas linguagens para exercitar programação ou até mesmo programar as GPIOs da placa. Assinale a alternativa que represente as linguagens de programação pré-instaladas no Raspbian.

- a) () Python e Java.
- b) () Scratch e NodeJs.
- c) () Php e Python.
- d) () Angular e C.
- e) () Fortran e Assembly.

4 Em sistemas IoT, um fator importante é obter conectividade com a Internet. De que forma, quando oferecido, as placas Raspberry conectam-se à Internet?

- a) () Fonte de alimentação e USB.
- b) () Bluetooth e USB.
- c) () Ethernet e bluetooth.
- d) () Wi-Fi e bluetooth.
- e) () Wi-Fi e Ethernet.

- 5 Diferente de outras placas, como Arduino, há alguns cuidados que se deve tomar ao manusear as placas Raspberry Pi. Dentre eles, destaca-se o cuidado ao trabalhar com as GPIOs. Selecione a alternativa que explique o motivo desse cuidado.
- a) () As GPIOs não têm proteção contra curto, o que pode queimar a placa caso uma tensão de 2V seja aplicada.
 - b) () As GPIOs podem ser manuseadas facilmente, pois são altamente protegidas contra curto.
 - c) () As GPIOs não têm proteção contra curto, o que pode queimar a placa, caso uma tensão um pouco acima do necessário seja aplicada.
 - d) () As GPIOs são frágeis e podem facilmente se quebrar.
 - e) () As GPIOs não têm compatibilidade com os módulos do Arduino.

CONECTANDO A INTERNET DAS COISAS - IoT

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, você deverá ser capaz de:

- definir o que são redes de computadores;
- reconhecer o breve histórico das redes de computadores;
- descrever as topologias de redes de computadores;
- identificar os meios de transmissão como equipamentos de interconexão;
- relacionar equipamentos de redes com fios;
- reconhecer equipamentos de redes wireless;
- analisar os protocolos da camada de internet: IP, ICMP, ARP e RARP;
- descrever o cabeçalho IP e sua função;
- explicar a fragmentação de datagramas IP. Identificar as principais tecnologias de comunicação sem fio para IoT e suas especificações;
- listar as aplicações de tecnologias de comunicação sem fio para IoT;
- analisar o padrão Ethernet;
- identificar as características do padrão Fast Ethernet;
- diferenciar os padrões Giga Ethernet de 10 Giga Ethernet;
- caracterizar a comunicação via Bluetooth;
- reconhecer os componentes que possibilitam a comunicação do Arduino via Bluetooth;
- analisar as aplicações do Bluetooth com Arduino;
- identificar os principais problemas na segurança de redes sem fio para IoT (Internet of Things);
- enumerar as técnicas de segurança em redes sem fio para IoT;
- aplicar técnicas para garantir a segurança em redes sem fio para IoT.

PLANO DE ESTUDOS

Esta unidade está dividida em três tópicos. No decorrer da unidade você encontrará autoatividades com o objetivo de reforçar o conteúdo apresentado.

TÓPICO 1 – TOPOLOGIAS E PROTOCOLOS DE COMUNICAÇÃO

TÓPICO 2 – TECNOLOGIAS PARA IoT

TÓPICO 3 – CONEXÃO DE EQUIPAMENTOS E NOÇÕES DE SEGURANÇA



Preparado para ampliar seus conhecimentos? Respire e vamos em frente! Procure um ambiente que facilite a concentração, assim absorverá melhor as informações.

TOPOLOGIAS E PROTOCOLOS DE COMUNICAÇÃO

1 INTRODUÇÃO

As redes de computadores estão intensamente presentes no dia a dia das pessoas — quando elas enviam mensagens por meio de seus aplicativos, acessam as redes sociais ou assistem a um vídeo estão usando a internet (ou redes de computadores) mundial, a qual conecta computadores ao redor do mundo inteiro.

Existem redes de computadores de diferentes tamanhos e com diferentes características, mas, neste tópico, você aprenderá a identificar o que é uma rede de computador, compreender como as redes de computadores surgiram e as diferentes maneiras de organizar os elementos que compõem uma rede de computadores.

Neste tópico, você conhecerá também os meios de transmissão como elementos de interconexão e as tecnologias utilizadas para redes, bem como o seu princípio de funcionamento e suas aplicações. Além disso, conhecerá os equipamentos utilizados em redes com fio, como hubs, repetidores, switches e roteadores, bem como a camada na qual eles operam, os benefícios e as limitações de cada equipamento. Por fim, verá quais são os elementos de rede necessários para a construção de uma rede wireless e suas características de operação.

A comunicação entre computadores é imprescindível para o funcionamento das tecnologias de hoje, especialmente da internet. Para proporcionar essa comunicação entre computadores, especifica-se a camada de internet, que funciona acima da camada de rede e abaixo da camada de transporte e garante a comunicação ponto a ponto de computadores de uma rede. A ideia é permitir a transferência de datagramas entre computadores de diferentes redes. Um datagrama nada mais é que um pacote na camada de internet que contém os dados a serem transferidos e um cabeçalho com informações gerais, como destino e tamanho da mensagem.

Neste tópico, você ainda vai aprender sobre a camada de internet e como computadores que estão a milhares quilômetros de distância podem trocar mensagens. Além disso, verá os principais protocolos utilizados para garantir o funcionamento da rede entre os equipamentos envolvidos. Por fim, vai estudar detalhes sobre como essas mensagens são construídas e alguns casos especiais de como enviar grandes quantidades de dados num mesmo datagrama.

2 DEFINIÇÃO DE REDES DE COMPUTADORES

As redes de computadores são hosts conectados entre si para trocar informações, compartilhar recursos e aplicativos, comunicação que tem diversos conceitos por trás, envolvendo hardware e software trabalhando em conjunto. Os protocolos de rede, por exemplo, são muito importantes para que os hosts compreendam as mensagens trocadas, definindo o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento (KUROSE; ROSS, 2007).

Para compreender o conceito de protocolos, utilizaremos a analogia de duas pessoas se comunicando ao encontrar-se na rua, cujo protocolo consiste basicamente em:

- Pessoa 1: “Oi”;
- Pessoa 2: Ouve a mensagem e responde “Oi”;
- Pessoa 1: Ouve a resposta e pergunta “Como vai?”;
- Pessoa 2: Ouve a pergunta e responde “Vou bem, e você?”;
- Pessoa 1: Ouve a resposta e responde “Vou bem também. Até mais”;
- Pessoa 2: Ouve a resposta e responde “Até mais”.

Resumidamente, as duas pessoas seguiram um protocolo de aguardar uma “solicitação” e respondê-la, conceito também seguido nas redes de computadores. Utilizando como exemplo um usuário que deseja acessar o Google, temos:

- Usuário: solicita a conexão TCP;
- Servidor: responde à conexão TCP;
- Usuário: acessa www.google.com;
- Servidor: devolve a página do Google;
- Usuário: faz uma pesquisa;
- Servidor: devolve a página de resultados.

Com esses exemplos, podemos notar que existem mensagens específicas que são enviadas e ações específicas realizadas em reação às respostas recebidas, satisfazendo ao conceito de protocolo de redes. Uma rede deve atender a alguns critérios, sendo os mais importantes segundo Forouzan (2008):

- **Desempenho:** pode ser medido de diversas maneiras, inclusive pelo tempo necessário para uma mensagem trafegar de um dispositivo a outro. Ainda, o desempenho depende de alguns fatores, como meios de transmissão, capacidades de hardware conectados e eficiência do software. Assim, tem-se a avaliação do desempenho por meio da vazão (throughput) e do atraso (delay);
- **Confiabilidade:** medida pela frequência de falhas, tempo que um link demora para recuperar-se de uma falha e robustez de uma rede em caso de catástrofe;
- **Segurança:** envolve proteção ao acesso não autorizado de dados, proteção de dados contra danos, implementação de políticas e procedimentos para recuperação de violações e perdas de dados etc.

Ainda, alguns atributos de redes são imprescindíveis para que consigamos compreender sua estrutura, por exemplo, o tipo de conexão, que pode ser ponto a ponto, na qual há um link dedicado entre dois dispositivos, e multiponto, em que, como o próprio nome sugere, vários hosts compartilham um único link. Existem também as categorias de redes ou abrangência de redes (Figura 1), que se referem até onde o sinal será distribuído.

FIGURA 1 – ABRANGÊNCIA DE REDES

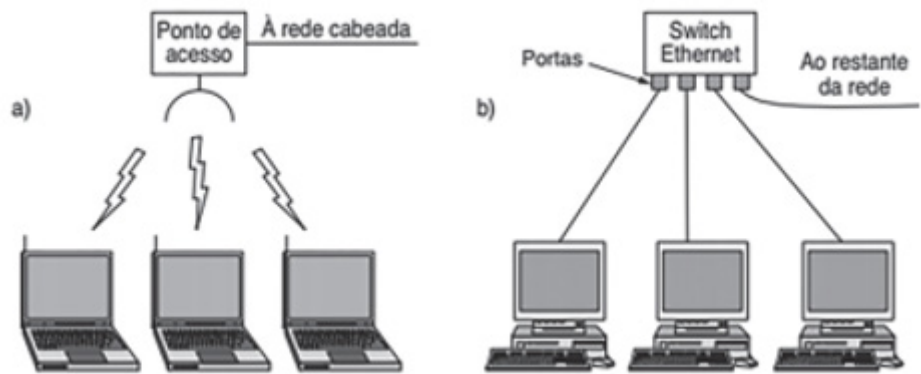
Distância do interprocessador	Processadores localizados no mesmo	Exemplo
1 m	Metro quadrado	Área pessoal
10 m	Cômodo	
100 m	Prédio	Rede local
1 km	Campus	
10 km	Cidade	Rede metropolitana
100 km	País	Rede a longas distâncias
1.000 km	Continente	
10.000 km	Planeta	A Internet

FONTE: Tanenbaum e Wetherall (2011, p. 11)

Conforme Forouzan (2008) e Tanenbaum e Wetherall (2011), a localização geográfica de redes, ou seja, sua abrangência, é categorizada em:

- **Personal area network (PAN):** rede privada menor que a rede LAN, tendo como alcance até 10 m, é utilizada, por exemplo, para conexões bluetooth e USB.
- **Local area network (LAN):** rede privada capaz de conectar diversos dispositivos em um prédio, um escritório, uma escola ou um campus. Como exemplos, têm-se uma rede simples em um escritório que conecta apenas dois computadores e uma impressora e uma rede mais complexa, que envolve um escritório com diversos funcionários e compartilhamento de diversos recursos, sendo hardware, software ou dados. Um exemplo real refere-se a uma empresa X que utiliza um software Y pago: em vez de a gerência adquirir uma licença para cada funcionário, adquire-se somente uma licença, que é armazenada no servidor local e disponibilizada para todos os funcionários acessarem. As redes LAN podem ser cabeadas (Figura 2, item a) ou sem fio (Figura 2, item b) e têm abrangência limitada.

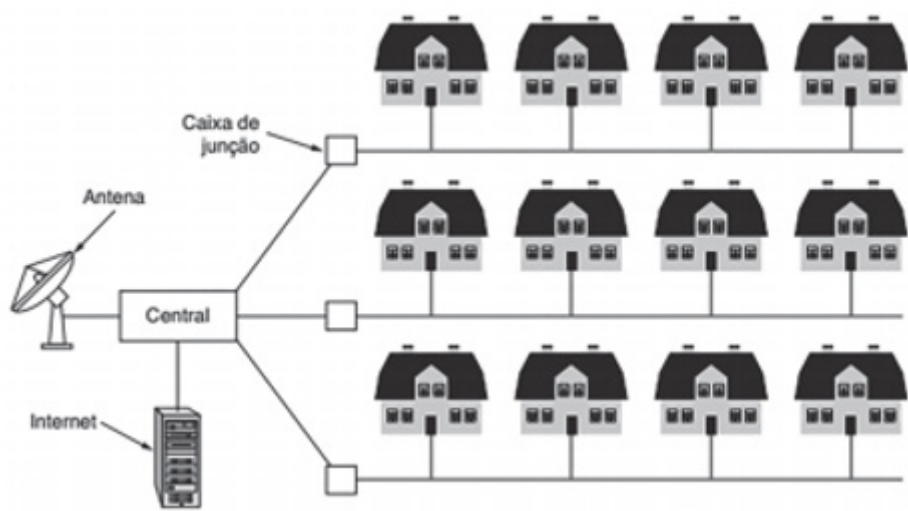
FIGURA 2 – REDE LAN (a)WI-FI E (b) CABEADA



FONTE: Tanenbaum e Wetherall (2011, p. 12)

- **Metropolitan area network (MAN):** rede de tamanho intermediário comparada com a LAN e WAN, cobre uma área dentro de um município e é projetada para clientes que precisam de conectividade de alta velocidade (ex., telefonia e redes de TV fechada, como exemplificado na Figura 3).

FIGURA 3 – EXEMPLIFICAÇÃO DA REDE MAN



FONTE: Tanenbaum e Wetherall (2011, p.14)

- **Wide area network (WAN):** possibilita que dados sejam transmitidos a longas distâncias, correspondentes a um país, a um continente ou até mesmo o mundo todo. Pode ser exemplificada quando o usuário final se conecta a um provedor de internet ou, ainda, no caso de uma empresa que dispõe de diversas filiais, porém precisa que elas estejam interconectadas, como exemplificado na Figura 4.

FIGURA 4 – EXEMPLIFICAÇÃO DA REDE WAN

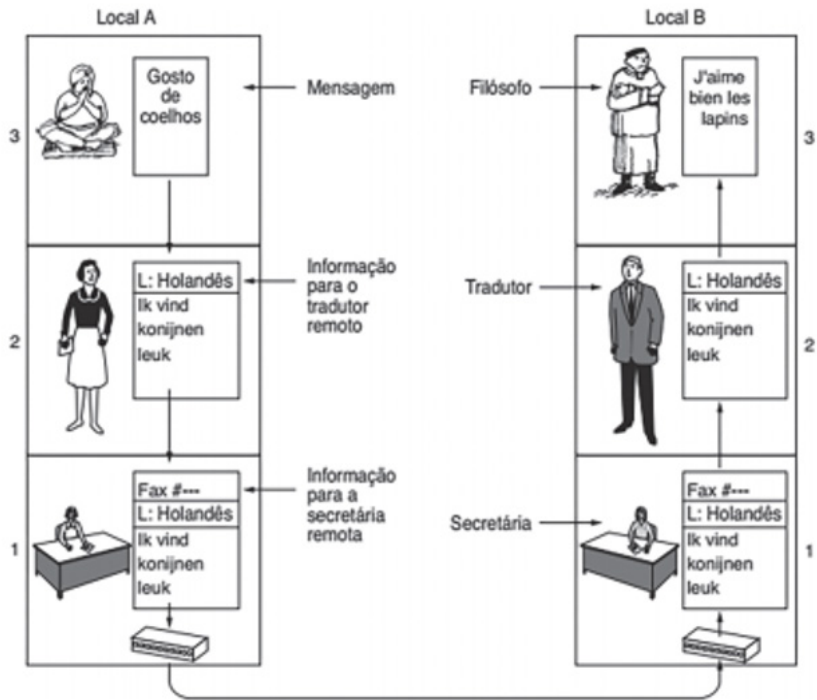


FONTE: Tanenbaum e Wetherall (2011, p. 15)

Além disso, há o conceito de topologias de redes, discutido no próximo capítulo, e os modelos arquiteturais de redes (ou, como também são conhecidos, os softwares de redes). Como mencionado anteriormente, para que dois dispositivos possam se comunicar, ambos precisam estejam atuando sobre o mesmo protocolo; caso contrário, não haverá compreensão. Os modelos arquiteturais de rede trabalham sob uma hierarquia de protocolos, em que há várias camadas, cada uma das quais responsável por uma tarefa no processo de entregar e receber uma mensagem.

Analogamente, imaginemos um brasileiro tentando conversar com um holandês, sem que nenhum saiba falar a língua do outro (Figura 5). Nesse exemplo, há três camadas: a 3ª a pessoa de origem e destino da mensagem; a 2ª a pessoa responsável por traduzir a mensagem para uma linguagem que as pessoas de origem e destino compreendem; e a 1ª, os secretários responsáveis por enviar as mensagens. Se a mensagem é enviada do local A para o local B, no local A a pessoa falará a mensagem, o tradutor a traduzirá e a secretária a enviará, e, no local B, o secretário receberá a mensagem, o tradutor a traduzirá e a pessoa a compreenderá — e mesmo ocorre para o inverso. Com isso, é possível notar que ambos os lados, na mesma camada, atuam sob o mesmo protocolo, arquitetura que possibilita que diversos dispositivos se comuniquem entre si na rede.

FIGURA 5 – EXEMPLO GENÉRICO DE HIERARQUIA DE PROTOCOLOS



FONTE: Tanenbaum e Wetherall (2011, p. 19)



As empresas responsáveis por produzir um componente de rede devem estar atentas aos protocolos, para que seu dispositivo esteja disponível para fazer operações na rede. Para a definição dos protocolos, existem documentos técnicos mantidos por empresas de tecnologias, como no link a seguir:

<https://qrqo.page.link/Wm2MR>

3 BREVE HISTÓRICO SOBRE REDES DE COMPUTADORES

Uma das principais necessidades da sociedade sempre foi a comunicação, a qual era impedida, antigamente, pela distância. Tentando mitigar a distância geográfica entre os povos, nossos ancestrais utilizavam sinais de fumaça ou pombo-correio para realizar tais comunicações.

Com a evolução das tecnologias e da sociedade, essas soluções foram aprimoradas, como em meados de 1838, em que o pintor e inventor Samuel Finley Breese Morse desenvolveu um sistema binário de representação da

distância de números, letras e sinais gráficos, que utilizava sons curtos e longos, traços e pontos para transmitir mensagens, nomeado Código Morse e que, no século XIX, foi muito utilizado por marinheiros para comunicação em alto-mar. Em 1865, esse código chegou a ser regulamentado internacionalmente a partir de sua utilização no telégrafo, proporcionando maior dinamismo às comunicações (TANENBAUM; WETHERALL, 2011).

Após a invenção do telefone em meados de 1876, o Código Morse caiu em desuso, pois passou-se a haver uma tecnologia que permitia às pessoas se comunicarem por meio de som e em tempo real. Avançando um pouco mais na história, tivemos a criação do rádio e da televisão (respectivamente, em 1902 e 1927), que proporcionou a propagação de informações e a transmissão de som e imagem por meio de ondas eletromagnéticas.

E, quando se pensou que as formas de comunicação não poderiam mais evoluir, iniciaram-se estudos e descobertas acerca do conceito de redes, como o de Leonard Kleinrock, em 1962, sobre a teoria das filas, conceito utilizado como base matemática para a comutação de pacotes, a tecnologia-base por trás do que hoje conhecemos como internet.

Por volta de 1960, o Departamento de Defesa dos Estados Unidos fez um acordo com a RAND Corporation buscando uma solução em meio à Guerra Fria, para construir uma rede de controle de comando capaz de sobreviver a uma guerra nuclear. Paul Baran, que trabalhava naquela empresa, apresentou um projeto em que aplicava a teoria de Leonard Kleinrock na transmissão de voz em redes militares, que atribuída maior segurança para a comunicação, uma vez que o projeto apresentou uma solução altamente distribuída e tolerante a falhas, visto que o temor dos Estados Unidos estava em sofrer ataques na central de comunicação e perder todos os seus dados. Com o projeto de Baran, as mensagens agora tinham vários caminhos para percorrer entre a origem e o destino.

Nesse período, os Estados Unidos até tentaram uma parceria com a American Telephone and Telegraph Company (hoje AT&T Corporation), empresa que dispunha do monopólio da indústria de telecomunicações, buscando um patrocínio na construção de um protótipo, porém a empresa se negou a fazê-la, desacreditando do potencial do projeto.

Em 1967, o então diretor da Advanced Research Projects Agency (ARPA), uma organização centralizada de pesquisa de defesa construída pelos Estados Unidos para desenvolver pesquisas tecnológicas, Larry Roberts, estava procurando um meio de oferecer acesso remoto aos computadores e, mais tarde, após juntar várias teorias, criou uma sub-rede para conectar computadores, em que havia interface message processors (IMP) para conectar cada nó.

Com isso, Larry e sua equipe de pesquisa desenvolveram a ARPANET, inicialmente com experimentos com quatro nós, conectando universidades, e, depois, com as pesquisas sobre os protocolos utilizados no ARPANET, chegando

à conclusão de que, com o aumento de dispositivos conectados a essa rede, poderia haver falhas.

Assim, por volta de 1978, criou-se o protocolo TCP/IP, utilizado até os dias atuais em redes de computadores, a partir do qual a ARPANET foi expandindo seus nós até se transformar na internet como conhecemos atualmente (TANENBAUM; WETHERALL, 2011).

Então, o que são as redes de computadores?

Partindo do conceito de redes, que define um conjunto de entidades interligadas entre si, em informática, redes de computadores compreendem um conjunto de hosts conectados entre si com a finalidade de trocar informações, compartilhar recursos e aplicativos.

Atualmente, essa nomenclatura não define somente a conexão em computadores, mas também celulares, tablets, televisões, carros, videogames ou qualquer outro dispositivo capaz de se conectar à rede. Com vários dispositivos podendo se conectar à rede, as redes de computadores passaram a ter uma vasta aplicação, como: aplicações comerciais, com o compartilhamento de recursos, servidores, banco de dados, correio eletrônico, videoconferência, e-commerce etc.; e aplicações domésticas, como bate-papo, jogos, vídeo por demanda, ensino a distância, redes sociais etc.

Partindo de tal pressuposto, têm-se como vantagens o compartilhamento de arquivos e programas, uma vez que empresas podem adquirir apenas uma licença de determinado produto, instalá-lo em rede e vários funcionários acessarem, o compartilhamento de impressoras, a agilidade nos processos, uma vez que não é preciso esperar muito para trocar informações, a redução de custos, com compartilhamento de recursos, como dispositivos de armazenamento, o aumento de segurança etc.

No entanto, também há desvantagens quanto ao uso de redes de computadores, como a própria segurança, pois, ao mesmo tempo que há níveis de acesso e histórico entre os funcionários, também são possíveis ataques de vírus e invasões hackers, problemas generalizados (ex., falhas em concentradores ou servidor que pode parar a rede) e também questões sociais, como roubo de identidade etc.

4 TOPOLOGIAS DE REDES

Topologia de redes refere-se à configuração física em que uma rede será organizada (KUROSE; ROSS, 2007), compreendendo uma representação geométrica da relação de todos os links e nós de uma conexão (FOROUZAN, 2008) que pode se conectar a vários pontos (multiponto) ou a apenas um ponto (ponto a ponto). Existem, ainda, tipos de topologia:

- **Malha:** cada host tem um link ponto a ponto dedicado a cada um dos outros dispositivos; para suportar esse tipo de rede, cada dispositivo deve conter $n-1$ portas de entrada e saída, em que “n” representa a quantidade de hosts conectados à rede. Na Figura 6, pode-se observar um exemplo dessa topologia.

FIGURA 6 – TOPOLOGIA MALHA

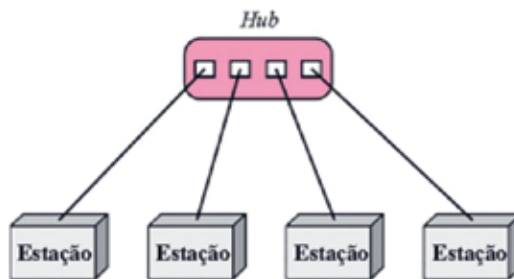


FONTE: Forouzan (2008, p.10)

Uma das vantagens do uso da topologia malha consiste em sua robustez, uma vez que, se um link é danificado, não afeta o sistema como um todo, pois uma estação tem outros caminhos para os dados percorrerem, o que auxilia na segurança, pois facilita a detecção de falhas. As desvantagens estão relacionadas à quantidade de recursos físicos necessários, quantidade de cabeamento e quantidade de portas de entrada e saída.

- **Estrela:** nessa topologia (Figura 7), cada host tem um link ponto a ponto dedicado, conectado apenas com o controlador central, e os hosts não são interconectados entre si, diferentemente da topologia malha; assim, é necessária somente uma porta de entrada e saída.

FIGURA 7 – TOPOLOGIA ESTRELA

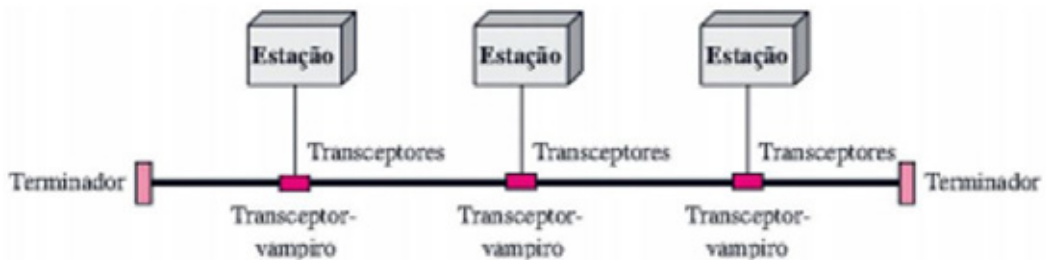


FONTE: Forouzan (2008, p. 11).

- **Barramento:** essa topologia atua como multiponto, com um longo cabo atuando como um backbone entre os hosts. Apresenta transceptores, os cabos que ligam o host ao cabo principal, e o transceptor-vampiro, o conector que

une o cabo principal aos hosts. As desvantagens relacionadas a essa topologia são as limitações quanto à distância, pois o sinal tende a ficar fraco conforme a distância do cabo central e a dificuldade de isolamento de falhas, e uma falha no cabo central atinge toda a rede (Figura 8).

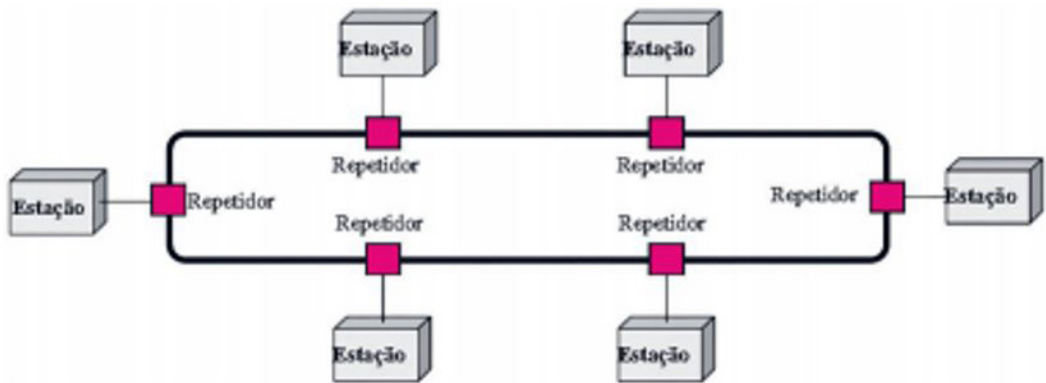
FIGURA 8 – TOPOLOGIA BARRAMENTO



FONTE: Forouzan (2008, p. 11).

- **Anel:** nessa topologia (Figura 9), cada dispositivo dispõe de uma conexão ponto a ponto dedicada com outros dois dispositivos conectados lado a lado e o sinal percorre somente uma direção. Então, se o computador A for enviar um dado para o computador D, o dado passará por B e C. Além disso, a falha em qualquer host pode danificar a rede inteira.

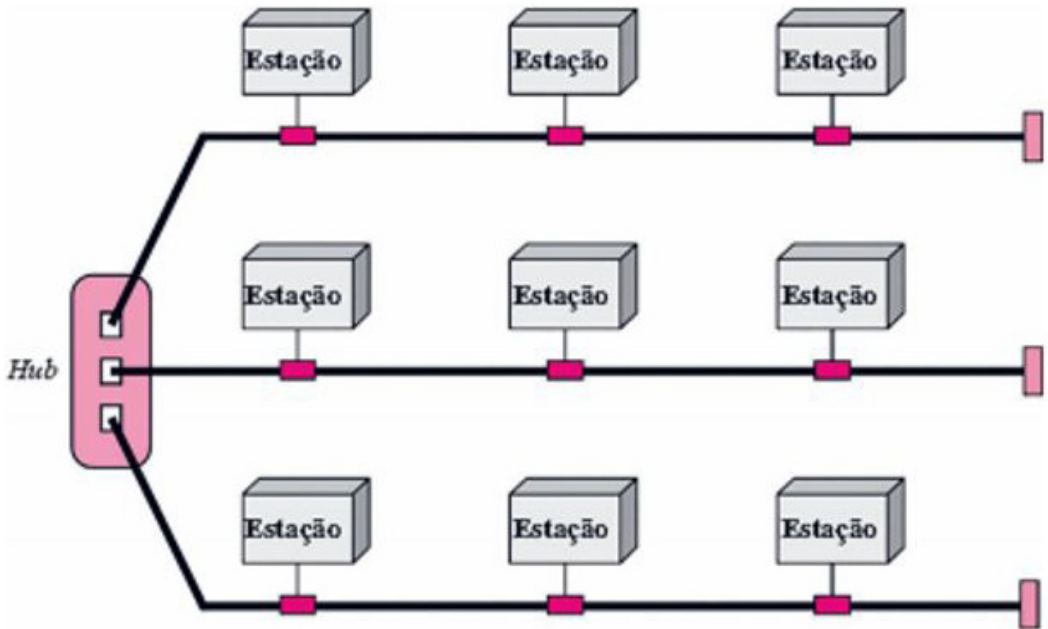
FIGURA 9 – TOPOLOGIA ANEL



FONTE: Forouzan (2008, p. 12).

Além dessas topologias mais conhecidas, há a topologia híbrida, que pode utilizar duas ou mais topologias distintas, como a mencionada na Figura 10, que apresenta uma topologia estrela, do hub ao cabo central, e uma barramento, que conecta todas as estações ao hub.

FIGURA 10 – TOPOLOGIA HÍBRIDA



FONTE: Forouzan (2008, p. 13).

Até agora, observamos o conceito de topologias físicas de redes, porém há também o conceito de topologias lógicas, que estão relacionadas ao percurso das mensagens entre hosts e o comportamento de uma rede. A topologia física não está ligada à topologia lógica, ou seja, uma rede pode ter topologias distintas, como Token Ring (IEEE 802.5) e Ethernet (IEEE 802.3).

5 OS MEIOS DE TRANSMISSÃO

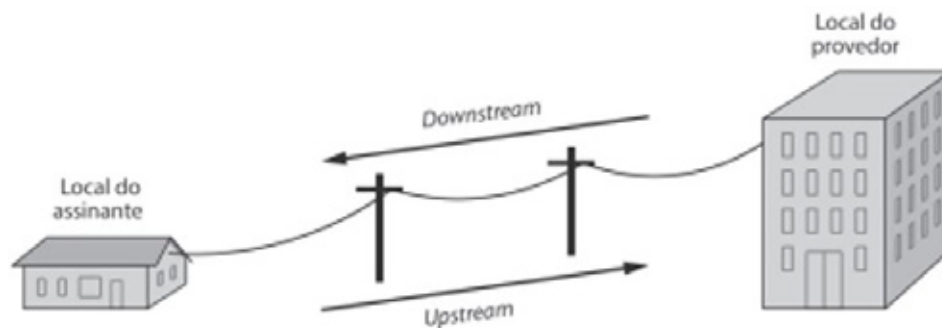
A teoria de comunicação define um meio de transmissão como um objeto capaz de transportar informações de uma origem para um destino. Os meios de transmissão utilizados em comunicação de dados podem ser os seguintes: espaço livre, cabo metálico ou fibra óptica. Ao analisar o modelo de camadas de redes, os meios de transmissão se situam abaixo da camada física, sendo controlados por ela.

Os meios de transmissão podem ser classificados em duas categorias: meios guiados, com fios, e meios não guiados, wireless. Os meios de transmissão guiados utilizam cabos de par trançado, cabos coaxiais e cabos de fibra óptica. Já os meios de transmissão não guiados são o espaço livre.

Em geral, um assinante residencial de internet recebe muito mais informações do que envia. Assim, as tecnologias de acesso à internet são projetadas para transferir mais dados em uma direção do que na outra. A Figura 11, a seguir, ilustra as definições de downstream e upstream. A indústria de redes

usa o termo *downstream* (ou download) para se referir aos dados que trafegam de um prestador de serviços na internet para um assinante, e *upstream* (ou upload) para se referir aos dados que trafegam de um assinante para um provedor de serviços.

FIGURA 11 – DEFINIÇÕES DAS DIREÇÕES *UPSTREAM* E *DOWNSTREAM* UTILIZADAS NAS TECNOLOGIAS DE ACESSO À INTERNET



FONTE: Comer (2016, p.172).

Existem tecnologias de acesso à internet de banda larga (*broadband*) e de banda estreita (*narrowband*). O termo tecnologia de banda estreita refere-se às tecnologias que entregam dados com uma taxa de transferência de até 128 kbit/s. Por exemplo, a taxa máxima de dados que pode ser atingida por meio de uma ligação telefônica analógica, com a mais sofisticada tecnologia de modem e com linhas telefônicas menos ruidosas, é de 56 kbit/s. São exemplos de tecnologia de banda estreita: conexões telefônicas discadas, circuito alugado que usa modems e rede digital de serviços integrados (RDSI ou ISDN, do inglês *Integrated Services Digital Network*).

A linha telefônica do assinante, ou *local subscriber line*, descreve a conexão física entre o escritório central (CO, do inglês *central office*) de uma empresa telefônica e o local do assinante. As companhias telefônicas desejavam fornecer um serviço de dados de alta velocidade ao assinante por meio da linha telefônica. Uma das primeiras ações que as companhias telefônicas realizaram foi a rede digital de serviços integrados (ISDN). Esse serviço possuía três canais digitais, denominados B, B e D, ou 2B+D. Os canais B tinham velocidade de 64 kbits/s, sendo utilizados para transporte de dados, ao passo que o canal D tinha capacidade de 16 kbits/s, sendo utilizado para controle. Além disso, era possível combinar os canais B para fornecer uma velocidade de 128 kbits/s, muito superior à dos modems de conexão discada.

Já as tecnologias de banda larga oferecem taxas de dados mais altas, porém há uma fronteira determinada entre banda estreita e banda larga. Muitos provedores, como empresas telefônicas, utilizam o termo banda larga para se referirem a qualquer serviço que oferece uma taxa mais elevada do que a oferecida pela internet discada. São exemplos de tecnologias de banda larga: tecnologias

DSL, tecnologias *cable* modem (modem a cabo) e tecnologias de acesso sem fio (*wireless*). A linha digital de assinante (DSL, do inglês *Digital Subscriber Line*) é uma das principais tecnologias utilizadas para oferecer serviços de comunicação de dados de alta velocidade através de uma linha do assinante (*loop local*). Existem muitas variantes da DSL, e a ADSL é a variante mais difundida e utiliza pela maioria dos clientes residenciais.

Inicialmente, foi utilizada a fiação da linha telefônica para conexão à internet. Entretanto, a falta de blindagem torna a fiação suscetível a interferências, que degradam substancialmente o desempenho para alguns assinantes. Como houve demanda crescente de taxas de bits, foi necessário o desenvolvimento de esquemas de fiação alternativos, e, conseqüentemente, uma variedade de tecnologias sem fio e com fio foi desenvolvida para uso nas linhas de assinantes.

Uma tecnologia de acesso alternativa que se destaca como particularmente atraente usa a fiação já existente para televisão a cabo. O meio utilizado em sistemas a cabo é o cabo coaxial, o qual possui banda larga e é menos suscetível a interferências eletromagnéticas do que o par trançado. Como os sistemas a cabo usam a multiplexação por divisão de frequência (FDM, do inglês *Frequency Division Multiplexing*), um *cable* modem pode ser ligado diretamente à fiação a cabo existente, sem a necessidade de um divisor de frequências.

A tecnologia de interconexão que possui taxas de dados mais altas e não necessita da alteração de todo o cabeamento é conhecida como *Hybrid Fiber Coax* (HFC), ou cabo coaxial de fibra híbrida. Esse sistema combina fibra óptica, utilizada na instalação central, e cabo coaxial, para assinantes individuais. Com isso, a fibra óptica é utilizada nas partes da rede que requerem as maiores larguras de banda, ao passo que o cabo coaxial é utilizado para usuários que toleram taxas de dados mais baixas. Para a implementação desse sistema, um provedor coloca dispositivos em cada bairro, os quais se convertem entre cabo coaxial e óptico. Cada dispositivo se conecta novamente ao provedor, através de uma fibra óptica, e às casas na vizinhança, via cabo coaxial. Se os cabos coaxiais utilizados para a TV a cabo já estão no local, o custo é minimizado, conforme ilustrado na Figura 2.

FIGURA 12 – SISTEMA DE ACESSO HYBRID FIBER COAX



FONTE: Comer (2016, p.179).

6 TIPOS DE EQUIPAMENTOS DE REDES COM FIO

As redes locais (LANs, do inglês *Local Area Network*) não trabalham isoladamente, pois se conectam entre si e à internet. Para a implementação física da rede local, são utilizados dispositivos de interconexão, visando à interligação das estações de trabalho. Esses equipamentos trabalham em diferentes camadas do modelo de internet e serão apresentados em três grupos: repetidores e *hubs*, que atuam na camada física; pontes (*bridges*), *switches* ou comutadores da camada 2; e roteadores ou comutadores da camada 3. Os repetidores e *hubs* trabalham na camada física, ou camada 1, os *switches* e as *bridges* trabalham na camada de enlace, ou camada 2, e os roteadores operam na camada de rede, ou camada 3.

A escolha do equipamento depende de alguns fatores, como: a máxima distância entre duas estações, a utilização de comunicação *full-duplex*, a necessidade de definição de sub-redes, a realização de difusão (*broadcast*) e a definição de domínios de colisão.

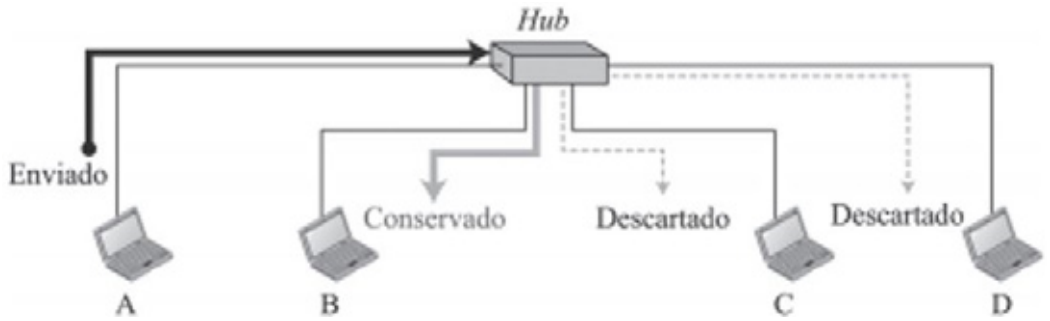
6.1 REPETIDORES E HUBS

O **repetidor** recebe um sinal e o regenera, antes que ele fi que muito fraco ou possa ser corrompido. Posteriormente, o repetidor encaminha o sinal regenerado. Um repetidor pode estender o alcance físico de uma LAN e conectar dois trechos de uma mesma LAN, mas não pode interligar duas LANs.

É possível aumentar o comprimento máximo do cabeamento por meio da divisão do cabo em segmentos, com repetidores entre eles. Um repetidor encaminha todos os *frames* de entrada para a saída, porém ele não tem capacidade de filtragem. É importante destacar que um repetidor não tem a função de amplificar o sinal, mas sim de regenerá-lo. Quando recebe, na entrada, um sinal de baixa amplitude ou corrompido, ele cria uma réplica, bit a bit, do sinal original.

Um **hub** é um repetidor com múltiplas portas, geralmente utilizado para conectar estações na topologia física estrela. A Figura 3, a seguir, ilustra o funcionamento de um hub ou roteador. Quando um pacote que tem como origem a estação A e como destino a estação B alcança o hub, o sinal é regenerado, para a retirada de possíveis ruídos que transformem os dados, e o hub o encaminha para todas as portas de saída, com exceção da porta pela qual os dados foram recebidos.

FIGURA 13 – HUB OU ROTEADOR



FONTE: FOROUZAN E MOSHARRAF (2013, P. 454).

6.2 PONTES (BRIDGES) E SWITCHES DE CAMADA 2

Devido ao crescimento do número de equipamentos interligados em uma rede estruturada com *hubs*, houve um aumento da probabilidade de ocorrência de colisão de pacotes, o que afeta diretamente o desempenho da rede em relação a atraso e velocidade de transmissão. Uma solução para esse problema é obtida por meio de pontes, ou *bridges*, em inglês, que definem diferentes domínios de colisão em uma rede, promovendo a sua segmentação (i.e., divisão da rede em vários domínios de colisão).

Uma ponte tem como função a interconexão de duas ou mais redes físicas, mantendo a abstração de uma única rede, composta pelos equipamentos dessas redes físicas. Entretanto, cada rede física obtém um domínio de colisão próprio. Para efetuar o redirecionamento de quadros de um segmento a outro, uma ponte necessita saber quais equipamentos estão conectados a cada segmento, o que é feito por meio de um software. O software de uma ponte realiza três tarefas básicas: aprendizado de endereços, envelhecimento e filtragem e redirecionamento de quadros.

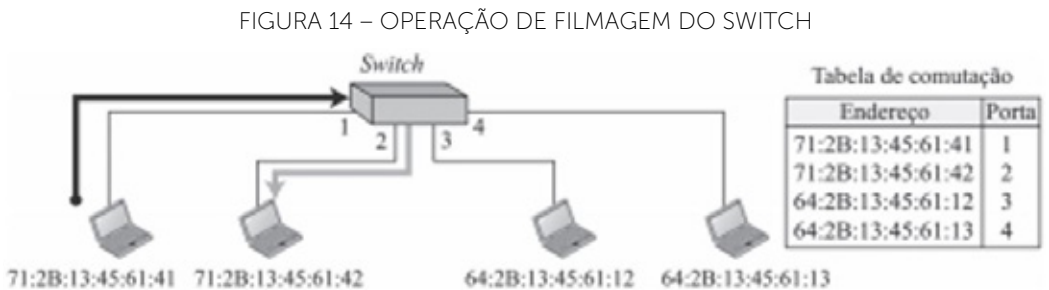
Existem vantagens na utilização de uma ponte de interconexão: aumento da confiabilidade, aumento do diâmetro da rede, desempenho e segurança. Com a isolamento dos diferentes segmentos de redes, os problemas físicos que eventualmente ocorrerem em um segmento não afetarão o comportamento global da rede, aumentando o seu nível confiabilidade. Como cada porta define um domínio de colisão isolado, garantindo o tempo de propagação dentro dele e o correto funcionamento do acesso múltiplo com detecção de portadora (CSMA, do inglês *Carrier Sense Multiple Access*), é possível concatenar diversos domínios de colisão por sucessivas pontes. À medida que o tráfego interno de um segmento deixa de ser propagado para os demais segmentos, o número de prováveis colisões é reduzido, sendo permitido que comunicações ocorram simultaneamente no interior de cada segmento. Assim, ocorre um aumento do desempenho global da rede. Além disso, uma ponte permite maior segurança, ao limitar o alcance de certas transmissões dentro de um segmento de rede.

Já o funcionamento de um *switch* ou comutador pode ser explicado como um conjunto de múltiplas pontes. Em relação aos aspectos físicos, o *switch* possui uma certa quantidade de portas, geralmente 24 ou 48 portas. Cada porta é utilizada para conectar um computador ou outro equipamento de rede, como *hub*, outro *switch* ou um roteador.

O *switch* de camada 2 trabalha tanto na camada física como na camada de enlace. Na camada física, o equipamento regenera o sinal recebido. Já na camada de enlace, sua função é a verificação dos endereços de controle de acesso ao meio (MAC, do inglês *Media Access Control*), tanto da origem como do destino, presentes no quadro. Pode ser considerado como uma *bridge* com muitas portas, visando ao melhor desempenho. Não existe tráfego de disputa, de modo que, ao contrário do que ocorre nas redes padrão Ethernet, não ocorrem colisões.

Tanto o *switch* de camada 2 como a *bridge* realizam uma decisão de filtragem no endereço físico MAC ou do *frame* que ele recebeu. A filtragem pode ser mais sofisticada no *switch* de camada 2, pois ele pode possuir um *buffer*, para armazenar os *frames* para processamento, ou ter um fator de comutação, que encaminha os *frames* de forma mais rápida.

A Figura 4, a seguir, mostra o princípio de operação da filtragem em uma rede LAN de quatro estações que deseja enviar dados da estação A para a B.



FONTE: FOROUZAN E MOSHARRAF (2013, P. 455).

6.3 ROTEADORES

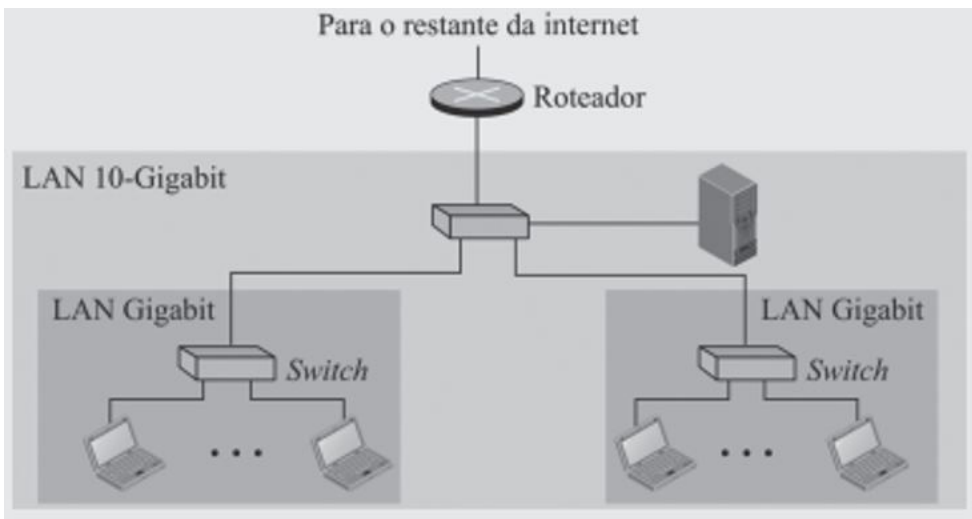
Um roteador é um dispositivo que opera em três camadas (física, enlace de dados e redes), transmitindo os pacotes baseados em endereços lógicos no endereçamento *host-host*. Por operar em camada física, ele regenera o sinal que recebe, ao passo que, por trabalhar na camada de enlace, ele verifica os endereços físicos tanto da origem como do destino que estão contidos nos dados. Como dispositivo da camada de rede, o equipamento verifica os endereços de camada de rede.

Um roteador é utilizado para interligar LANs e WANs (do inglês *Wide Area Network* [rede de longa distância]) na internet e possui uma tabela de roteamento,

base para a tomada de decisões de roteamento. As tabelas de roteamento são dinâmicas, e a sua atualização ocorre por meio dos protocolos de roteamento. Além do endereço físico, o roteador possui um endereço lógico (IP) para cada uma de suas interfaces. Ele atua apenas sobre os pacotes nos quais o endereço da camada de enlace de destino equivale ao endereço da interface de chegada do pacote. Além disso, o roteador altera o endereço da camada de enlace do pacote, tanto da origem quanto do destino, no momento de seu encaminhamento.

A Figura 5, a seguir, apresenta um exemplo que retrata a rede de uma corporação que possui dois prédios comerciais. Em cada prédio, há uma rede local do tipo LAN Ethernet Gigabit, para interconectar todas as estações de trabalho, sejam *notebooks* ou *desktops*, ao *switch*. Os *switches* de cada uma das LANs são interligados juntamente ao servidor da empresa, o que permite que haja uma rede de alta velocidade do tipo LAN 10-Gigabit. Com a inclusão do roteador, é possível conectar o sistema da empresa à internet. O roteador é responsável por alterar o endereço MAC que ele recebe, uma vez que os endereços MAC possuem apenas jurisdição local. Além disso, a camada de rede é responsável pelo encaminhamento do pacote da origem até o destino, sendo que a rede física é uma combinação de redes (LANs e WANs) e dos roteadores que as conectam

FIGURA 15 – EXEMPLO DE INTERCONEXÃO DE REDES



FONTE: FOROUZAN E MOSHARRAF (2013, P. 458).

6.4 PATCH PANELS

Os *patch panels* são equipamentos que organizam as conexões de rede, para assegurar que as ligações sejam montadas e desmontadas corretamente, e facilitam a identificação dos pontos de rede no *rack*. O número de portas em um patch panel pode variar entre 24, 48 e 96 portas no padrão RJ45.

Com o *patch panel*, é possível alterar as entradas e saídas do *rack* sem alterar o cabeamento horizontal, compreendido entre as tomadas de telecomunicações nas áreas de trabalho (ATR) até o *patch panel*. Os cabos são conectados na parte traseira do *patch panel* e, na parte frontal, são conectadas cada uma das portas utilizando-se cordões de manobra (*patch cords*). O *patch panel* fica localizado nos armários de telecomunicações. A Figura 6, a seguir, apresenta um exemplo de *patch panel* de par trançado.

FIGURA 16 – PATCH PANEL COM UTILIZAÇÃO DE CABOS DE PAR TRANÇADO



FONTE: Adaptado de Schutterstock (2020)

7 EQUIPAMENTOS DE REDES *WIRELESS*

As redes sem fio, ou redes *Wireless*, representam um sistema de comunicação de dados alternativo a redes locais cabeadas e combinam conectividade de dados com mobilidade através de tecnologia de radiofrequência (RF). Suas vantagens são as facilidades de uso e de instalação, que permitem a mobilidade do usuário, cada vez mais frequente desde o advento de *notebook*, *tablets* e *smartphones*, além de existirem situações em que é inviável a instalação de cabos.

Entretanto, para o funcionamento correto de uma rede *wireless*, existem fatores críticos para a escolha de tecnologia, tais como imunidade a interferências, segurança de dados, compatibilidade, custo acessível e gerenciamento de redes. Um fator determinante para a escolha da tecnologia é a faixa de frequência na qual será realizada a operação, pois as características de propagação podem variar muito com a frequência. Assim, existem algumas frequências que possuem características mais adequadas que outras. A frequência de 2.4 GHz, por exemplo, apresenta um bom nível de propagação. Em geral, quanto maior a frequência, maior o consumo de energia e menor o alcance.

Para cada país, há uma alocação diferente do espectro eletromagnético que é controlado pelo governo. No Brasil, a agência responsável pelo controle é a Agência Nacional de Telecomunicações (Anatel). O Quadro 1, a seguir, apresenta as designações, os comprimentos de onda e as aplicações de bandas de frequências de RF.

QUADRO 1 – DESIGNAÇÕES, COMPRIMENTOS DE ONDA E APLICAÇÕES DE BANDAS DE FREQUÊNCIAS DE RF

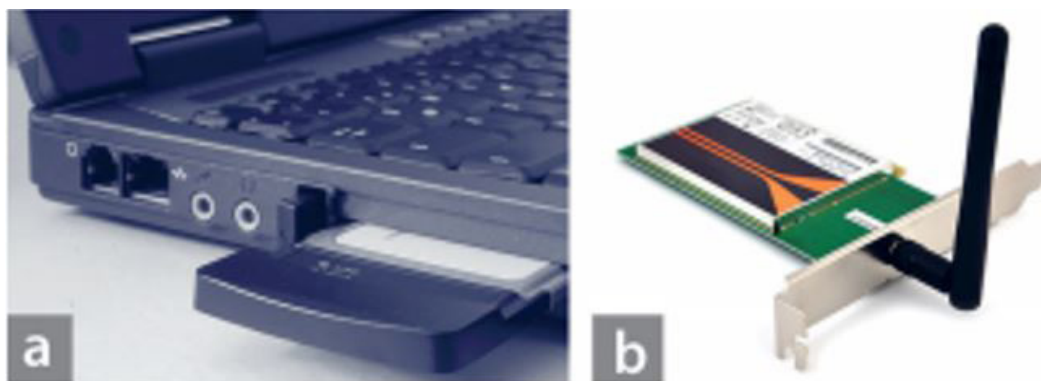
Banda de frequências	Frequências	Comprimentos de onda	Aplicações
Muito baixa frequência (VLF)	3–30 kHz	10–100 km	Navegação; meteorologia
Baixa frequência (LF)	30–300 kHz	1–10 km	Navegação; comunicação marítima Sistemas de informação e meteorologia; sistemas de padrão de tempo
Média frequência (MF)	0,3–3 MHz	0,1–1 km	Navegação Rádio AM Rádio móvel
Alta frequência (HF)	3–30 MHz	10–100 m	Banda do cidadão (CB) Rádio em ondas curtas Rádio móvel Rádio marítimo
Muito alta frequência (VHF)	30–300 MHz	1–10 m	Radioamadorismo Rádio FM Satélite móvel Rádio móvel Rádio fixo
Ultra-alta frequência (UHF)	0,3–3 GHz	0,1–1 m	Satélite de micro-ondas TV UHF Telefonia sem fio Telefonia celular LAN sem fio
Superalta frequência (SHF)	3–30 GHz	1–10 cm	Satélite de micro-ondas LAN sem fio
Extremamente alta frequência (EHF)	30–300 GHz	1–10 mm	Satélite de micro-ondas Localização via rádio

FONTE: Adaptado de Visser (2015).

Outro ponto a ser observado são os sinais refletidos, em que um sinal de rádio sai de um transmissor e chega ao receptor por vários diferentes caminhos, fenômeno conhecido como *multipath*. Esses sinais refletidos podem trazer relevante interferência ao sinal original.

Para implementar uma rede local sem fio (WLAN), são necessários diversos elementos de rede, tais como: placas de rede *wireless*, *access point*, antenas. As placas de rede *wireless* são adaptadores utilizados nas estações, instaladas em *notebook* ou *desktop*. O barramento dessas placas pode ser PCI e PCMCIA, comuns em *notebooks*. A Figura 7, a seguir, ilustra esses tipos de placa de rede.

FIGURA 17 – (a) PLACA DE REDE PCMCIA. (b) PLACA DE REDE PCI



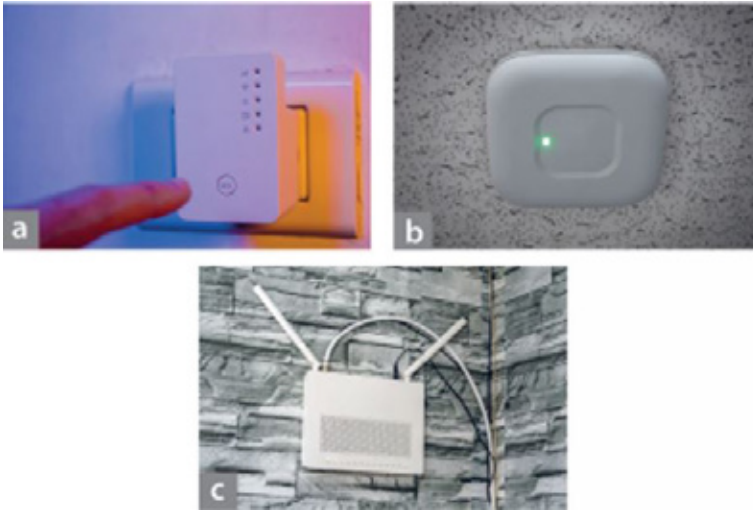
FONTE: Adaptado de Shutterstock (2020)

O adaptador *wireless* também funciona como placa de rede, mas utiliza interface USB. É adotado quando não é possível a conexão de placas PCI e PCMCIA. Já o *access point*, ou ponto de acesso, é uma estação na rede *wireless* responsável pelo gerenciamento das conexões dos usuários com a rede. Além disso, serve como ponto de interligação entre a rede cabeada e a rede wireless.

A área de cobertura do sinal do *access point* é da ordem de 100 metros, e cada *access point* pode atender diversos usuários na mesma rede. Quando a distância entre o usuário e o *access point* é maior que 100 metros, faz-se necessária a colocação de mais *access points* para esse local. O dispositivo funciona conectado via cabo a um roteador ou *switch* e distribui o sinal Wi-Fi na outra extremidade. Pode-se entender o funcionamento de um *access point* de modo similar a um repetido Wi-Fi que utiliza cabeamento e não pode ser substituído por um roteador.

A Figura 18, a seguir, apresenta diferentes tipos de *access point*. O primeiro deles é um repetidor de Wi-Fi (Figura 18a), que tende a ser mais barato e simples de usar, em relação às versões cabeadas. Entretanto, com ele, há uma relevante perda de desempenho. Outros tipos de *access point* Wi-Fi são o fixado no teto (Figura 18b), para maximizar o alcance, e o em formato de caixa fixado em uma parede (Figura 18c).

FIGURA 18 – DIFERENTES TIPOS DE ACCESS POINT: (A) EXTENSOR DE SINAL DE WI-FI; (B) ACCESS POINT WI-FI FIXADO NO TETO; (C) ACCESS POINT SEM FIO EM FORMATO DE CAIXA FIXADO NA PAREDE



FONTE: Adaptado de Shutterstock (2020)



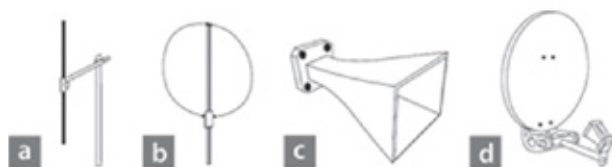
Para conhecer os critérios de escolha de um roteador para um ambiente doméstico, leia o artigo “Saiba como escolher o roteador Wi-Fi ideal para a sua casa”, disponível no link a seguir:

<https://qrqo.page.link/jwtdW>

Outro dispositivo que pode, eventualmente, ser utilizado em redes sem fio é o *wireless print server*, que permite o compartilhamento de impressoras para a rede *Ad-hoc*. Esse dispositivo possui uma antena para recebimento/envio dos dados das estações e, para se conectar às impressoras da rede, utiliza uma conexão USB ou paralela.

As antenas representam um elemento fundamental para o sistema de redes sem fio, e podem ser definidas com um dispositivo para a radiação ou recepção de ondas de rádio. Uma classificação de antenas é omnidirecional, quando irradiam o sinal de forma igualitária em todas as direções, e direcional, quando concentram e irradiam o sinal para uma única direção. Existem diversos tipos de antenas em relação à construção, como: antena dipolo, antena de quadro, antena corneta e antena parabólica (Figura 19).

FIGURA 19 – TIPOS BÁSICOS DE ANTENAS: (A) ANTENA DIPOLO; (B) ANTENA DE QUADRO; (C) ANTENA CORNETA; (D) ANTENA REFLETORA PARABÓLICA



FONTE: Visser (2015, p. 8).

Outros tipos de antenas podem ser vistos como uma combinação dessas antenas básicas (p. ex., antenas Yagi-Uda, combinações de antenas dipolos ativos e curto-circuitadas em paralelo) ou derivadas de uma das antenas básicas (p. ex., uma antena de plaqueta de microfita, que consiste em duas antenas de abertura retangulares).

Outra forma de transmissão sem fio é o sinal óptico sob forma de *laser* (Figura 20). Não é um tipo de rede muito frequente, e a principal aplicação desse tipo de enlace é a conexão de LANs situadas em prédios diferentes, porém com linha de visada. Uma das vantagens desse tipo de transmissão é prescindir da licença de um órgão regulador.

FIGURA 20 – ENLACE PONTO A PONTO UTILIZANDO TECNOLOGIA A LASER



FONTE: Moraes (2014, p. 106).

8 PROTOCOLOS DA CAMADA DE INTERNET

A comunicação entre computadores interconectados é o que garante o funcionamento da internet e de todas as suas tecnologias. Assim, para prover uma organização e garantir o bom funcionamento da rede, diversos protocolos foram propostos, ainda na década de 1980. O principal protocolo nessa camada é o IP (*Internet Protocol*), que é responsável por transferir datagramas entre computadores de redes interconectadas. Esses computadores são identificados por endereços virtuais únicos de tamanho fixo, e as redes estão interconectadas por meio de roteadores ou computadores que pertencem a mais de uma rede.

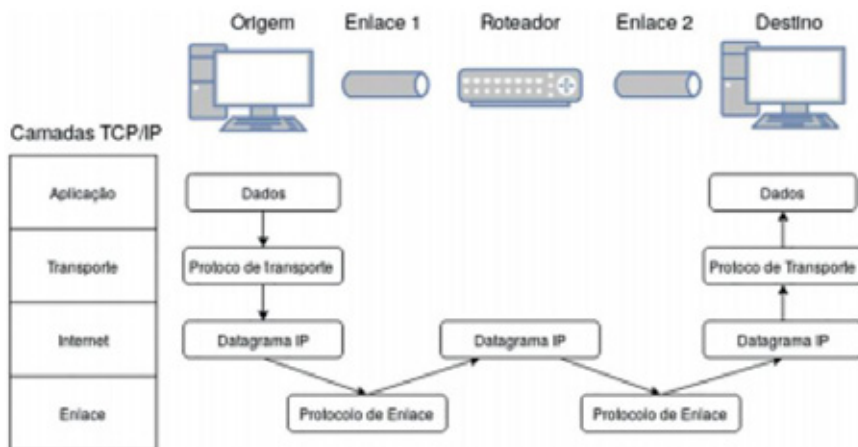
Quando um computador deseja mandar uma mensagem para um computador de outra rede, ele encapsula a sua mensagem em um datagrama,

que é um pacote contendo informações gerais e a mensagem a ser enviada. Esse datagrama contém um cabeçalho de informações, como o endereço de destino, e o corpo contendo os dados, ou seja, a mensagem original a ser enviada.

A comunicação começa quando o computador de origem envia o datagrama para o próximo ponto na rede responsável pelo redirecionamento de mensagens (chamado de *gateway*). Esse ponto pode ser tanto um roteador quanto outro computador na rede. O roteador analisará o endereço de destino e verificará em qual rede ele está conectado e se possui um caminho para o destino, utilizando-o para enviar a mensagem ao próximo roteador.

Esses encaminhamentos ocorrem até um roteador que está diretamente conectado ao destino. Durante os encaminhamentos, os roteadores ou computadores devem apenas ler as informações gerais do datagrama contidos no seu cabeçalho, sem precisar analisar a mensagem original que foi enviada, isto é, não é necessário analisar as informações das camadas de transporte e aplicação. A Figura 21 mostra um exemplo de comunicação entre computadores que estão em redes diferentes, os quais estão interconectados por um roteador. Veja o encapsulamento dos dados originais nas diferentes camadas TCP/IP.

FIGURA 21 – EXEMPLO DE COMUNICAÇÃO ENTRE COMPUTADORES DE REDES DIFERENTES, INTERCONECTADOS POR UM ROTEADOR



FONTE: Os autores

Imagine o funcionamento da transferência de datagramas como a transferência de cartas no sistema de correios. Um datagrama é uma carta, e os computadores são locais. Um endereço IP é equivalente a um endereço físico de um local (como uma cidade, rua e número). Quando uma carta chega a um centro de processamento de cartas, o carteiro olha o endereço dela e sabe o próximo ponto para o qual ela deve ser encaminhada — que não é necessariamente o destino. Esses locais intermediários funcionam como os roteadores entre redes. Uma carta com origem na cidade de São Paulo e destino na cidade do Rio de Janeiro deve ser, primeiramente, transferida para o estado do Rio de Janeiro, para depois ir à cidade e, por fim, ao endereço mais específico.

O protocolo IP é especificado pelo RFC 791, sendo a versão **IPv4** ainda muito difundida. Essa versão tem o **formato de endereçamento x.x.x.x**, em que x é um byte que pode ter valor entre 0 e 255. Um exemplo de endereço no IPv4 é 192.168.0.2. Com a explosão de dispositivos conectados à internet e a utilização de diversas tecnologias, como IoT (*Internet of Things* ou, em português, internet das coisas), os endereços de IPv4 acabaram. Para solucionar esse problema, uma nova versão do protocolo foi desenvolvida: o **IPv6**. Essa versão contém algumas novas funcionalidades e um novo tipo de **endereçamento no formato hh:hh:hh:hh:hh**, em que h é um valor em hexadecimal.

Outra característica do protocolo IP é que ele não garante a entrega dos datagramas. Se ocorrer alguma situação, durante a comunicação, que implique o descarte do datagrama, ele não será reenviado automaticamente. Isso é tratado normalmente pelos protocolos da camada de transporte, como o TCP.

Durante a comunicação de datagramas, várias situações podem ocorrer e, como o protocolo IP não garante a confiabilidade da entrega e não informa se ela aconteceu, um protocolo de controle é necessário para prover informações sobre o estado da rede e da entrega dos datagramas. Dessa forma, o ICMP (*Internet Control Message Protocol*), especificado pelo RFC 792, é um protocolo utilizado para monitorar a rede e prover informações sobre a sua saúde. Tipicamente, o ICMP é utilizado para informar quando houve falhas na entrega do datagrama para o computador de origem.

O datagrama ICMP segue o datagrama IP, e possui sete tipos diferentes de mensagens. Exemplos de mensagens de erros do ICMP são as seguintes:

- Destino inacessível – quando um roteador não possui informação sobre para onde enviar o datagrama.
- Tempo para envio do datagrama excedido – quando o roteador percebe que o pacote já passou por muitos outros roteadores e passou do limite de tempo estabelecido para o envio.
- Erro nos parâmetros do datagrama – quando um roteador encontrou um problema no cabeçalho do datagrama.

Ainda, uma clássica aplicação ping e pong utiliza o protocolo ICMP para verificar se um nó responde na camada de internet. O Quadro 1 mostra mais códigos de erros, indicando o tipo da mensagem, o código a ela relacionado e a sua descrição prática.

TABELA 1 – TIPOS DE MENSAGEM ICMP

ICMP - Tipo	Código	Descrição
0	0	Resposta eco (<i>ping</i>)
3	0	Rede de destino inacessível
3	1	Nó de destino inacessível
3	2	Protocolo de destino inacessível
3	3	Porta de destino inacessível
3	6	Rede de destino desconhecido
3	7	Nó de destino desconhecido
4	0	Abaixar fonte (Controle de congestionamento)
8	0	Pedido eco (<i>ping</i>)
9	0	Anúncio de rota
10	0	Descobrir rota
11	0	TTL expirada (tempo de vida do datagrama)
12	0	Erro de cabeçalho IP

FONTE: Adaptado de Kurose, Ross e Zucchi (2013).

A comunicação entre dois computadores utilizando o protocolo IP deve passar pela camada de rede, em que é necessário conhecer também o endereço físico (MAC) da interface física de destino. Em algumas situações, quando computadores da mesma rede precisam se comunicar e têm endereços IP, o computador de origem precisa descobrir o endereço MAC do seu destino (de modo a ser utilizado na camada de rede).

Para solucionar esse problema, o protocolo ARP (*Address Resolution Protocol*) foi especificado pelo RFC 826. O seu funcionamento basicamente ocorre de forma reativa dos equipamentos que estão na rede. Isso significa que, quando um dos equipamentos precisa de um MAC de outro computador do qual ele só tenha o IP, é realizada uma consulta na rede.

A consulta é essencialmente na forma da pergunta “Quem é o equipamento que possui o IP x.x.x.x?”. Então, a máquina de destino responde “Eu sou o equipamento de IP x.x.x.x e tenho MAC x”. Assim, para evitar a necessidade de fazer consultas a todo tempo, cada equipamento possui uma tabela ARP correlacionando IPs e MACs.

De forma similar ao ARP, em algumas situações, é necessário descobrir o endereçamento IP de máquinas vizinhas na rede quando somente se conhecem os seus endereços MAC. Para utilizar o protocolo IP, é necessário descobrir o endereço IP dessas máquinas.

Assim, no protocolo RARP (*Reverse Address Resolution Protocol*), especificado pelo RFC 903, a máquina interessada em descobrir o endereço IP

de uma máquina na mesma rede realiza uma consulta enviando um pacote em broadcast para determinar o IP da máquina alvo.



O termo broadcast refere-se a comunicações endereçadas a todos os equipamentos de uma rede específica. Dessa forma, um pacote é enviado para vários destinos ao mesmo tempo.



O protocolo RARP foi substituído, na maioria dos sistemas, pelo protocolo DHCP (Dynamic Host Configuration Protocol), especificado pelo RFC 2131 (TANENBAUM; WETHERALL, 2011).

9 DATAGRAMA IP

O datagrama IP (ou diagrama, conforme alguns autores) é efetivamente a mensagem trocada entre os computadores utilizando o protocolo IP na camada de internet.

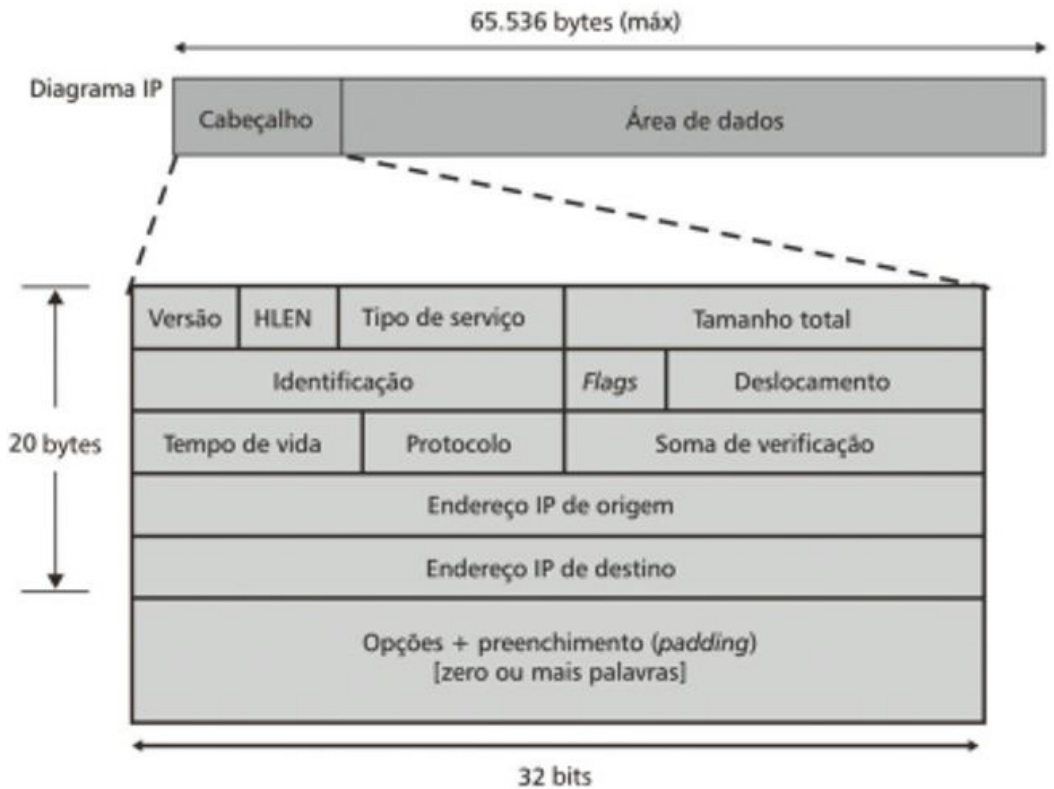
O datagrama IP é constituído de um cabeçalho e de uma área de dados, e o seu tamanho total é de 65.536 bytes.

Se considerarmos um cabeçalho sem opções adicionais de apenas 20 bytes, restam 65.515 bytes para dados.

Se considerarmos ainda o cabeçalho de transporte do protocolo TCP, que também possui 20 bytes sem opções extras, o espaço máximo para a área de dados fica em 65.495.

Na Figura 22, você pode ver a representação da versão 4 do protocolo IP (IPv4).

FIGURA 22 – DATAGRAMA IP VERSÃO 4 E OS SEUS ELEMENTOS



FONTE: Carissimi, Rochol e Granville(2009, p. 234).

O cabeçalho do datagrama IPv4 é constituído por 13 campos, que possuem informações diferentes, conforme descrito a seguir.

- **Versão:** indica a versão do protocolo IP a ser utilizada. Isso permite que múltiplas versões possam ser usadas ao mesmo tempo. Atualmente, está ocorrendo a transição da versão IPv4 para a IPv6. Apesar de, na versão IPv6, ser utilizado outro formato de cabeçalho, os primeiros quatro bits da mensagem são dedicados a isso, permitindo aos roteadores processarem o restante do diagrama.
- **HLEN:** informa o tamanho do cabeçalho, já que este pode variar, pois o campo de opções pode ficar em branco. Na maioria dos casos, é isso que acontece, e o cabeçalho tem tamanho de 20 bytes (KUROSE; ROSS; ZUCCHI, 2013).
- **Tipo de serviço:** pode ser utilizado por roteadores para identificar o tipo do pacote e ter certa flexibilidade quanto à prioridade ou não dele. Indicar se o pacote pertence a um serviço que requer baixa latência seria um exemplo de utilização desse campo.
- **Tamanho total:** indica o tamanho total do datagrama, considerando o cabeçalho e os dados, tendo no máximo 65.536 bytes, já que esse é um campo de 16 bits. Entretanto, a maioria dos datagramas são menores que 1.500 bytes (KUROSE; ROSS; ZUCCHI, 2013).

- **Identificação:** utilizado para identificar fragmentos de um mesmo datagrama IP. Nesse caso, todos os fragmentos do mesmo datagrama IP possuem a mesma identificação, enquanto datagramas diferentes têm identificadores diferentes.
- **Flags:** dois bits são utilizados para marcar duas flags relacionadas à fragmentação de datagramas — isto é, um sinalizador para certo comportamento. O primeiro bit é utilizado para informar os roteadores para não fragmentar o pacote. O segundo bit é utilizado para marcar que o datagrama é um fragmento com um fragmento subsequente, e somente o último fragmento (ou datagramas não fragmentados) deve desativar o bit.
- **Deslocamento:** utilizado para informar qual parte do fragmento do datagrama IP esses dados representam, o que permite a reconstrução do datagrama.
- **Tempo de vida:** utilizado para limitar a vida dos datagramas, ou seja, quantas vezes o datagrama pode ser processado por roteadores. Todo roteador, quando redireciona um datagrama IP, deve decrementar o tempo de vida, de modo a evitar que esse datagrama fique na rede para sempre. Se um roteador receber um datagrama com o campo zerado, esse datagrama deve ser descartado, e um ICMP de aviso é enviado à origem.
- **Protocolo:** indica de qual protocolo esse datagrama faz parte, como ICMP, TCP ou UDP. Esse campo é essencialmente utilizado para ligar a camada de internet com a camada de transporte.
- **Soma de verificação:** utilizado para verificar a integridade do cabeçalho do datagrama. Essencialmente, é realizada a soma de dois em dois bytes do cabeçalho IP, a qual é armazenada neste campo, utilizando a regra de complemento de 1s quando o valor estourar. Assim que um datagrama chega a um roteador, a soma é realizada e comparada com o valor desse campo. Datagramas com um valor inválido são descartados.
- **Endereço IP de origem e de destino:** são os endereços de origem e destino do datagrama. Quando um datagrama é criado, o criador insere o seu próprio endereço no campo de origem e informa o endereço de destino. O endereço IP é constituído de 32 bits, sendo usualmente representado numa quadrupla x.x.x.x.
- **Opções:** é um campo opcional para descrever opções adicionais do datagrama. São raramente utilizadas e, por isso, foram removidas no IPv6.

De forma similar, o cabeçalho do datagrama IP para a versão 6 é mostrado na Figura 22. A grande diferença dessa versão para o IPv4 é a remoção de diversos campos, o tamanho do campo dos endereços e a criação de cabeçalhos adicionais. Veja a explicação de cada campo:

- **Versão:** igual ao IPv4, com quatro bits utilizados para informar a versão do datagrama IP a ser utilizada.
- **Classe de tráfego:** equivalente ao tipo de serviço do IPv4.
- **Identificador de fluxo:** novo campo para identificar datagramas do mesmo fluxo de comunicação.
- **Tamanho dos dados:** equivalente ao tamanho total do IPv4; porém, como o cabeçalho do IPv6 tem tamanho fixo, esse tamanho é apenas dos dados do datagrama.

- **Próximo cabeçalho:** utilizado para indicar o próximo cabeçalho. Como vários parâmetros do cabeçalho IPv4 acabavam não sendo utilizados, foi acrescentada a ideia de múltiplos cabeçalhos. Caso os campos adicionais sejam utilizados, um novo cabeçalho específico é criado, e esse campo indica o próximo tipo a ser lido.
- **Limite de encaminhamento:** equivalente ao tempo de vida do IPv4.
- **Endereço de origem e destino:** equivalente aos do IPv4, mas agora com tamanho de 128 bits, possibilitando $3,4 \times 10^{38}$ endereços.

FIGURA 23 – CABEÇALHO DO DATAGRAMA IP VERSÃO 6 E SEUS ELEMENTOS

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)		
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				

FONTE: Adaptado de IPv6 (2012)

10 FRAGMENTAÇÃO DE DATAGRAMAS IP

A camada de internet utiliza a camada de rede para enviar os seus datagramas. Isso significa que um datagrama IP, quando enviado à camada de rede, será novamente encapsulado em pacotes do protocolo, sendo utilizado nessa camada. Até aqui, tudo parece correto e não há nenhum problema à vista. Entretanto, o que acontece se o protocolo da camada de rede tiver um limite de dados a serem transferidos inferior ao de um datagrama IP?

Esse problema na verdade é mais recorrente do que parece. O datagrama IP, por exemplo, possui limite de 65.536 *bytes*. No entanto, um dos protocolos mais utilizados na camada de rede — o ethernet — tem um limite de 1.500 *bytes*. Então, surge o problema de como dividir os dados do datagrama IP para que sejam adequados aos requerimentos de tamanho das camadas menores.

O tamanho de dados máximo que pode ser enviado por um enlace na camada de rede é chamado de MTU (*Maximum Transmission Unit*). Quando um datagrama for transferido por um enlace, ele estará limitado pelo MTU dele. Assim, a solução mais simples é limitar todo o datagrama para o menor MTU. Entretanto, entre uma origem e um destino, pode haver várias rotas com MTUs diferentes.

Para solucionar esse problema, foram criados os fragmentos do datagrama IP, com o objetivo de reduzir o tamanho do datagrama de forma a se adequar aos tamanhos requeridos na camada de rede. Após a fragmentação de um datagrama em um roteador, ele deverá ser reconstruído corretamente antes de ser enviado para a camada de transporte, já que os protocolos nessa camada esperam que os dados estejam completos.

Isso significa que, em algum momento, os fragmentos devem ser reconstituídos no datagrama original. Imagine que, após passar por um enlace com baixo MTU e chegar a um roteador em que o próximo enlace da rota tem um MTU maior, seria possível reconstruir o datagrama e enviar menos fragmentos. No entanto, os criadores do IPv4 decidiram que essa reconstrução poderia ser custosa demais nos roteadores — afinal, implicaria mais latência nesse datagrama e possivelmente em todos os subsequentes (KUROSE; ROSS; ZUCCHI, 2013). Então, essa responsabilidade foi atribuída ao destino do datagrama.

No IPv4, os fragmentos podem ter tamanhos diferentes, o que gera certa dificuldade extra na reconstrução dos datagramas originais. Para realizar a reconstrução de um datagrama, são utilizados os campos do cabeçalho IPv4 identificação, *flags* e deslocamento. Quando o destino recebe datagramas de um mesmo local, ele deve separar os fragmentos e esperar até o último fragmento. Isso pode ser feito verificando datagramas recebidos com a mesma origem e o mesmo identificador, e com a *flag* indicando que ainda há um novo fragmento, isto é, não é o último fragmento.

Quando o destino recebe o último fragmento, isto é, a *flag* indicando se existe um fragmento subsequente está zerada, ele poderá reconstituir o datagrama original. Para realizar isso, o roteador avalia o campo deslocamento para reconstruir o pacote. O roteador, então, seleciona todos os fragmentos com a mesma origem e o mesmo deslocamento, e analisa o valor de deslocamento de cada fragmento para posicionar os dados no local correto.

Na versão IPv6, a especificação da fragmentação acontece de forma levemente diferente da IPv4. No IPv6, as especificações de se um datagrama é fragmento é feita nos cabeçalhos estendidos. Nesse caso, o ID do cabeçalho estendido é o 44. A Figura 24 apresenta o cabeçalho de extensão, que tem campos similares ao IPv4. O campo “Próximo cabeçalho” é igual ao do cabeçalho original no IPv6, indicando se existe próximo cabeçalho e qual é. O campo “Reservado” é uma zona de dados não utilizada, e o campo “Deslocamento do Fragmento” equivale ao deslocamento do IPv4. “Res” é outro espaço reservado sem uso

no momento, e M é a *flag* de se existe um fragmento subsequente. Por fim, a identificação é equivalente ao IPv4.

FIGURA 24 – CABEÇALHO DE EXTENSÃO DE FRAGMENTAÇÃO
DO IP VERSÃO 6 E SEUS ELEMENTO

Próximo Cabeçalho	Reservado	Deslocamento do Fragmento	Res	M
Identificação				

FONTE: Adaptado de IPv6 (2012)



RESUMO DO TÓPICO 1

Neste tópico, você aprendeu que:

- Uma rede de computadores é um conjunto de componentes de hardware e de software que interliga equipamentos, como computadores, impressoras e celulares, tornando possível que estes sejam capazes de compartilhar recursos e de trocar mensagens. Existem diferentes tipos de redes que se adequam a diferentes contextos. Por exemplo, quando uma pessoa conecta o seu celular a um fone de ouvido por meio de bluetooth, ela está utilizando uma rede do tipo PAN (Personal Area Network) sem fio, chamada de WPAN (Wireless Personal Area Network).
- Os endereços de IP identificam computadores e equipamentos em redes locais e na Internet. O número de dispositivos conectados na Internet já ultrapassa a quantidade de IPs que a versão 4 desse protocolo contém. Devido a isso, a versão 6 do IP surge com um número de endereços milhões de vezes maior.



- 1 Existem diferentes arquiteturas de rede ou topologias. Cada topologia de rede se enquadra em um contexto específico. Suponha um cenário em que foi necessário escolher uma topologia física que permitisse que pessoas conectadas não dependessem de um servidor sempre funcionando. Assim, pares arbitrários de hosts se comunicam diretamente. Que topologia foi utilizada nesse caso? Marque a alternativa CORRETA.
 - a) ☐ Par-a-par.
 - b) ☐ Cliente-servidor.
 - c) ☐ De barramento.
 - d) ☐ Híbrida.
 - e) ☐ Estrela.

- 2 A topologia da rede representa como os nós de uma rede estão conectados e organizados fisicamente. Existem diferentes topologias que se adequam a cenários específicos. Nesse contexto, marque a alternativa que descreve as topologias físicas de redes.
 - a) ☐ Malha, estrela e barramento.
 - b) ☐ Malha, half-duplex e barramento.
 - c) ☐ Estrela, malha e MVC.
 - d) ☐ Par-a-par, anel e full-duplex.
 - e) ☐ Half-duplex, par-a-par e malha.

- 3 Um papel fundamental em redes de computadores é prover comunicação entre os hosts. Para que seja possível essa comunicação, existem alguns pré-requisitos que devem ser respeitados na implementação da rede. No contexto de topologias lógicas, assinale a alternativa que apresenta corretamente uma condição para que dois dispositivos em uma rede possam se comunicar.
 - a) ☐ Para que dois hosts possam se comunicar, é necessário que ambos estejam na mesma rede LAN.
 - b) ☐ Para que dois hosts possam se comunicar, é necessário que ambos estejam atuando sobre o mesmo protocolo.
 - c) ☐ Para que dois hosts possam se comunicar, é necessário que ambos implementem um protocolo broadcast.
 - d) ☐ Para que dois hosts possam se comunicar, é necessário que ambos estejam atuando sobre protocolos diferentes.
 - e) ☐ Para que dois hosts possam se comunicar, é necessário que ambos possuam uma topologia par-a-par.

4 Considerando as características dos vários elementos de interconexão de redes de computadores, identifique a alternativa que corresponda especificamente a esses equipamentos conforme a sequência a seguir:

- I- Pode ser usado para interligar vários hubs, ou mesmo para interligar diretamente as estações, substituindo com vantagens o hub.
- II- É possível aumentar o alcance, ou extensão, de uma rede wireless utilizando esses elementos de interconexão.
- III- Serve para conectar duas redes distintas, de mesmo protocolo, permitindo comunicações entre elas.
- IV- Pode ser utilizado para unir duas redes que usam protocolos de rede distintos.

- a) () I – Repetidor; II – Hub; III – Bridge; IV – Switch.
- b) () I – Switch; II – Repetidor; III – Bridge; IV – Roteador.
- c) () I – Switch; II – Bridge; III – Repetidor; IV – Roteador.
- d) () I – Repetidor; II – Hub; III – Switch; IV – Roteador.
- e) () I – Roteador; II – Bridge; III – Repetidor; IV – Switch.

5 Uma rede wireless pode trazer diversos benefícios em relação às redes cabeadas. Considere as características a seguir:

- I. Mobilidade.
- II. Maior segurança.
- III. Custos reduzidos de instalação.
- IV. Rápida e simples instalação.

Assinale a alternativa que indica corretamente os benefícios.

- a) () Somente I, II e IV.
- b) () Somente I e III.
- c) () Somente I, III e IV.
- d) () Somente I e IV.
- e) () Somente III e IV.

6 Na Internet, este elemento encaminha os pacotes que são gerados por um sistema final e os entrega a seu destino, ou seja, é o responsável por entregar a requisição de um usuário ao servidor que a possui. Está interligado a vários outros e conhece o caminho para diversas redes no mundo. Que elemento é esse?

- a) () Switch.
- b) () Placa de rede.
- c) () Modem.
- d) () Roteador.
- e) () Hub.

7 Suponha que o host A, de endereço IP 143.54.10.140, envie ao host B, endereço de IP 143.54.10.202, um segmento TCP encapsulado em um

datagrama IPv4. Quando o host B receber esse datagrama, qual campo do cabeçalho ele vai verificar para decidir para qual protocolo da camada de transporte ele deve passar a carga útil do datagrama?

- a) () Tipo de serviço.
- b) () Identificação.
- c) () Protocolo.
- d) () Identificador de fluxo.
- e) () Classe de tráfego.

8 O protocolo IPv6 surgiu porque os endereços do IPv4 estavam acabando. Nesse sentido, quantos bits são utilizados para o IPv4 e o IPv6? E para o endereço MAC?

- a) () 32, 64 e 16.
- b) () 16, 64 e 32.
- c) () 48, 128 e 32.
- d) () 32, 128 e 48.
- e) () 32, 128 e 128.

TECNOLOGIAS PARA IoT

1 INTRODUÇÃO

O padrão Ethernet lida com a estrutura física da rede e os meios pelos quais a rede se comunica. Esse padrão, criado em 1976, é líder de mercado desde o princípio, superando — e praticamente extinguindo — seus concorrentes, como o Token Ring e o FDDI. Duas características possibilitaram a conservação do padrão Ethernet por mais de 30 anos: a flexibilidade e a simplicidade. Essas características possibilitam que, na prática, o padrão seja confiável, seguro, de fácil manutenção e barato de se manter.

Assim, neste tópico, você vai estudar o padrão Ethernet, suas características e seus diferentes padrões

Neste tópico, você vai estudar também os conceitos do que é considerado no mercado como uma das tecnologias disruptivas da área tecnológica. A IoT, ou simplesmente Internet das Coisas, conecta máquinas em uma rede que permite o compartilhamento de dados, para que estes possam ser compartilhados de forma a complementar as atividades de cada um dos dispositivos da rede.

É a partir desse conceito que você vai aprender como, na prática, a tecnologia da IoT propõe esses serviços e transforma o modo como o mundo se conecta. Você também vai verificar as aplicações da IoT. Ainda, você vai conferir as tecnologias envolvidas na comunicação dos equipamentos que compõem a IoT e vai poder refletir sobre a situação do mercado atual.

2 O PADRÃO ETHERNET

As duas primeiras camadas do modelo *Open Systems Interconnection* (OSI) lidam com a estrutura física da rede e os meios pelos quais os dispositivos de rede podem enviar informações de um dispositivo em uma rede para outra. Tanenbaum (1997) destaca que o protocolo mais popular para as camadas físicas e o enlace de dados é o padrão Ethernet, superando tecnologias como Token Ring, Token Bus, FDDI e LANs ATM.

O padrão Ethernet foi criado em 1976 pela Xerox, no Palo Alto Research Center. Conforme leciona Comer (2016), esse padrão se mantém em uso até hoje,

mesmo que os hardwares, os cabos e os meios usados com o padrão tenham mudado ao longo de sua existência. Sua evolução e sobrevivência aos avanços da tecnologia se deve a alguns fatores, dentre eles a interoperabilidade das diferentes versões do padrão.

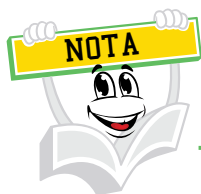
As terminologias básicas usadas na Ethernet são: nó, meio, segmento e quadro. Os nós são dispositivos como computadores, roteadores e dispositivos periféricos que se comunicam pela Ethernet. O meio é o caminho usado pelos dispositivos para se comunicar. Na Ethernet, o meio pode ser um cabo coaxial, um cabo de par trançado ou um cabo de fibra ótica. O segmento é o meio compartilhado (ou seja, o caminho ou cabo único) que está ligando os dispositivos de rede. O quadro é a mensagem curta compartilhada pela rede. Quando os dispositivos Ethernet estão conectados, eles formam uma rede de área local (LAN, do inglês *Local Area Network*).

Vários padrões de Ethernet operam em velocidades distintas, usando diferentes meios físicos; no entanto, são compatíveis entre si. Dessa forma, é possível combiná-los na mesma rede, usando dispositivos como *hubs* e *switches*, para vincular segmentos de rede que usam tipos diferentes de meios.

Tanenbaum (1997) destaca outros fatores que fazem o padrão Ethernet ser popular.

- **Economia:** os dispositivos de rede e o meio físico de transmissão (par trançado) são de baixo investimento.
- **Manutenção:** não há necessidade de software para usar o padrão, nem de configurações adicionais para gerenciá-lo.
- **Facilidade de expansão de rede:** para adicionar nós na rede, basta plugar.
- **Interoperabilidade:** como já mencionado, os diferentes padrões Ethernet são compatíveis entre si.
- **Evolução:** o padrão conseguiu evoluir com mais velocidades e mantendo as mesmas características, sem necessidade de mudanças na infraestrutura das organizações.

A Ethernet foi originalmente padronizada como IEEE 802.3, com uma taxa de transmissão de dados de 10 Megabits por segundo (Mbps). Outras versões de Ethernet foram introduzidas recentemente, para oferecer taxas de dados mais altas: Fast Ethernet e Gigabit Ethernet suportam taxas de dados de 100 Mbps e 1 Gbps (1.000 Mbps), respectivamente. Uma LAN Ethernet pode usar cabo coaxial (10Base2), cabeamento de par trançado não blindado (10Base-T, 100Base-T e 1000Base-T) ou cabo de fibra ótica.



O Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) é uma organização sem fins lucrativos, fundada nos Estados Unidos, que tem como objetivo promover conhecimento nas engenharias elétrica, eletrônica e da computação. Acesse o link a seguir para visitar o site da organização.

FONTE: <www.ieee.org>. Acesso em: 29 jun. 2020.

2.1 CONTROLE DE ACESSO AO MEIO

Ao usar um mesmo meio, diferentes dispositivos compartilham esse meio para enviar e receber dados. Segundo Tanenbaum (1997), por esse motivo, a Ethernet fornece um método para controlar a forma de os nós compartilharem o acesso ao meio: a tecnologia *carrier sense multiple access* (CSMA).

O processo CSMA é usado para detectar primeiro se o meio está em uso por outro dispositivo. Se um sinal de outro nó for detectado, isso significa que outro dispositivo está transmitindo. Quando o dispositivo que está tentando transmitir perceber que o meio está ocupado, ele aguardará e tentará novamente após um curto período de tempo. Se nenhum sinal for detectado, o dispositivo transmitirá seus dados. É possível que o processo CSMA falhe e dois dispositivos transmitam ao mesmo tempo. Isso é chamado de **colisão de dados**. Se isso ocorrer, os dados enviados pelos dois dispositivos serão perdidos e precisarão ser reenviados.

À medida que o uso e o número de nós aumentam, a probabilidade de acesso de meio bem-sucedido sem uma colisão diminui. Além disso, os mecanismos de recuperação necessários para corrigir erros devido a essas colisões diminuem ainda mais o rendimento da rede. O **CSMA/CD** (CSMA com detecção de colisão ou CD, do inglês *Collision Detection*) é o protocolo Ethernet mais utilizado nesse sentido. A finalidade desse protocolo é manipular os pacotes descartados, perdidos ou corrompidos. Na Ethernet, como mencionado anteriormente, se dois dispositivos transmitem mensagens ao mesmo tempo, ocorre uma colisão, e as mensagens (quadros) são descartadas. O protocolo CSMA/CD é usado para evitar a perda de dados de tais colisões.

A popularização de tecnologias comutadas em redes, como o *switch*, substituiu amplamente a necessidade original de CSMA/CD em LANs. Quase todas as conexões com fio entre dispositivos em uma LAN hoje são conexões *full-duplex*, em que um dispositivo é capaz de enviar e receber simultaneamente. Isso significa que, embora as redes Ethernet sejam projetadas com a tecnologia CSMA/CD, usando dispositivos como o *switch*, as colisões não ocorrem. Já os *hubs* não fazem o controle de acesso ao meio, fazendo uso do CSMA/CD.



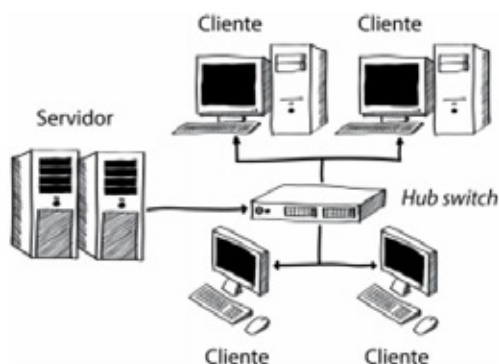
Para exemplificar o CSMA, suponha uma reunião com várias pessoas (nós), todas em volta de uma mesa (LAN), em que cinco pessoas falam (segmento) ao mesmo tempo sobre seus relatórios (quadro). Fica impossível compreender qualquer uma dessas informações. Cabe a quem conduz a reunião (CSMA) dar a palavra a cada um dos membros da reunião, um por vez.

3 O PADRÃO FAST ETHERNET

Conforme leciona Tanenbaum (1997), em 1992, a IEEE se reuniu para produzir uma LAN mais rápida, já que o padrão Ethernet de 10 Mbps já não atendia à demanda necessária. Em 1995, foi oficialmente aprovado o padrão 802.3U, conhecido como **Fast Ethernet**. Ele não é necessariamente um novo padrão, mas apenas um aprimoramento do padrão 802.3. Por trás do aprimoramento, tecnicamente, apenas se reduziu o tempo de bit de 100 para 10 ns (nano segundos). Além disso, os padrões de conexão com cabos multipontos, com conectores de pressão ou BNC (Bayonet Neill–Concelman) não podem mais ser utilizados.

A Fast Ethernet usa o mesmo mecanismo de controle de acesso à mídia CSMA/CD que as tradicionais redes Ethernet de 10 Mbps. As implementações Fast Ethernet são coletivamente conhecidas como tecnologias 100Base-T. Os dispositivos geralmente são conectados em uma topologia em estrela, usando *hubs* e *switches*. A especificação, conforme Tanenbaum (1997), inclui mecanismos de autonegociação de velocidade de quadro, permitindo que os fornecedores de hardware produzam dispositivos de rede duplos de 10/100 Mbps para incorporar a Fast Ethernet às redes 10Base-T legadas.

FIGURA 25 – ESTRUTURA DE UMA LAN EHERNET



FONTE: Adaptado de Shutterstock (2020)

A Fast Ethernet pode ser implementada em três diferentes esquemas de transmissão ou opções de cabeamento, conforme descritos a seguir.

- **100Base-TX:** é a implementação mais popular de Fast Ethernet. O 100Base-TX usa dois pares de fios no cabeamento da categoria 5; isto é, o mesmo cabeamento da popular variedade de Ethernet 10Base-T de baixa velocidade. Sua conexão é *full-duplex* e a distância do segmento do meio não deve ultrapassar 100 m.
- **100Base-FX:** utiliza um cabo de fibra ótica multimodo *duplex* com conectores ST (straight tip), usado principalmente para fiação de *backbone*. Sua distância pode chegar a 2.000 m.
- **100Base-T4:** usa quatro pares de fios e permite que o Fast Ethernet seja usado em cabeamento de categoria 3 ou superior. Exige quatro pares trançados. Esse padrão perdeu a popularidade, pois sua distância máxima de segmento é de 100 m.

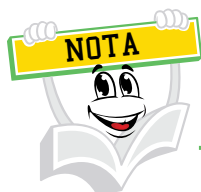
A atualização para Fast Ethernet é provavelmente a maneira mais fácil e barata de atualizar uma rede para atender às novas necessidades de largura de banda. Dentre as vantagens de atualizar redes Ethernet de 10 Mbps para Fast Ethernet, pode-se destacar as seguintes:

- integra-se facilmente às redes Ethernet de 10 Mbps existentes, sem exigir reinvestimento em novos softwares de gerenciamento de rede e solução de problemas;
- pode transportar voz, dados e vídeo a 100 Mbps, o que é 10 vezes mais rápido do que a Ethernet tradicional de 10 Mbps;
- pode operar com o mesmo meio instalado em uma rede Ethernet tradicional de 10 Mbps;
- a rede pode ser migrada lentamente para a Fast Ethernet, usando hubs 10/100 com detecção automática e placas de interface de rede (NICs).

O padrão 802.3u possibilita a interconexão por *hubs* e *switches* de dois tipos:

- **Repetidor classe I:** realiza a conversão de sinal interno, que introduz pequenos atrasos de propagação, mas permite que tipos diferentes de meios Fast Ethernet, como 100Base-TX e 100Base-FX, sejam conectados juntos.
- **Repetidor classe II:** envia os sinais recebidos imediatamente (sem conversão) para todas as portas de saída, minimizando, assim, a latência da porta. Os repetidores de classe II exigem que todas as portas se conectem à mesma mídia, como 100Base-TX.

Uma alternativa ao Fast Ethernet é o 100Base-VG (também chamado 100VG-AnyLan). Essa especificação IEEE 802.12 define transmissão de 100 Mbps, usando uma tecnologia de controle de acesso ao meio com prioridade de demanda, que a Hewlett-Packard originalmente desenvolveu para o transporte de quadros Ethernet e Token Ring. Entretanto, essa alternativa não teve sucesso.



Os switches Ethernet de 100 Mbps podem ser usados para segmentar a rede, para reduzir os gargalos causados pelos usuários que tentam acessar os principais servidores na rede. Basta conectar cada hub 10/100 da rede local (LAN) ao comutador Ethernet e conectar os servidores diretamente ao comutador.

4 GIGABIT E 10 GIGABIT

Em se tratando de conexão de rede, quanto maior a capacidade, melhor. Por isso, em 1999, a IEEE lançou o 802.3ab, popularmente conhecido como **Gigabit Ethernet**, conforme leciona Tanenbaum (1997). O padrão Gigabit Ethernet suporta uma taxa de dados máxima teórica de 1 Gbps (1.000 Mbps).

A princípio, alguns achavam que atingir velocidades de gigabit com Ethernet exigiria o uso de fibra ótica ou outra tecnologia de cabo de rede especial. No entanto, isso é necessário apenas para longas distâncias, mostrando a versatilidade da tecnologia Ethernet. Em condições normais, a efetiva transferência de dados pelo cabo ainda pode chegar a 900 Mbps.

Nos PCs, as unidades de disco podem limitar muito o desempenho de uma conexão Gigabit Ethernet. Os discos rígidos tradicionais giram a taxas que variam entre 5.400 e 9.600 rotações por segundo, o que pode suportar apenas uma taxa de transferência de dados entre 25 e 100 Megabytes por segundo, por exemplo. O Gigabit Ethernet é suportado por quatro padrões de camada física, usando cabos de cobre de par trançado (especificamente, os padrões de cabeamento CAT5e e CAT6) semelhantes aos Fast Ethernet de 100 Mbps mais antigos (que funcionam em cabos CAT5). Esses tipos de cabo seguem o padrão de cabeamento 1000Base-T. Esse padrão incorpora 1000Base-SX para transmissão de dados via fibra ótica multimodo. Além disso, inclui 1000Base-LX sobre fibra monomodo e 1000Base-CX via cabeamento de cobre para transmissão. O padrão Gigabit Ethernet possibilita, assim, operar em dois modos: *full-duplex* e *half-duplex*. O Quadro 3 sintetiza essas especificações.

QUADRO 3 – PADRÕES 802.3AB

Nome	Cabo	Distância máxima do segmento	Vantagens
1000Base-SX	Fibra óptica	550 m	Fibra multimodo (50, 62,5 micra)
1000Base-LX	Fibra óptica	5.000 m	Modo único (10micra) ou multimodo (50, 62,5 micra)
1000Base-CX	2 pares de STP	25 m	Par trançado blindado
1000Base-T	4 pares de UTP	100 m	UTP padrão da categoria 5

FONTE: Adaptado de Tanenbaum (1997)

O Gigabit Ethernet oferece os seguintes benefícios em relação à Ethernet comum de 10 a 100 Mbps:

- a taxa de transmissão é 100 vezes maior;
- reduz os problemas de gargalos e aumenta a capacidade de largura de banda, resultando em desempenho superior;
- oferece capacidade full-duplex, que pode fornecer largura de banda praticamente duplicada;
- oferece largura de banda cumulativa para maior velocidade, empregando adaptadores e switches de servidor gigabit;
- apresenta qualidade de serviço (QoS), reduzindo latência e oferecendo melhores serviços de vídeo e áudio;
- é compatível com o nós Ethernet existentes;
- transfere uma grande quantidade de dados rapidamente;
- tem valores acessíveis.

A IEEE, em 2002, levou muito a sério a frase “quanto mais velocidade melhor” e propôs o **10 Gigabit Ethernet**, que é uma tecnologia de telecomunicação que oferece velocidade de dados de até 10 bilhões de bits por segundo. O 10 Gigabit Ethernet também é conhecido como 10 GE, 10 GbE, 10 GigaE ou 803.ae.

Conforme leciona Tanenbaum (1997), o padrão 10 GbE é totalmente compatível com os protocolos Ethernet existentes. Ele difere da Ethernet tradicional por ser um protocolo *full-duplex*, o que significa que não precisa de protocolos de detecção de acesso múltiplo ou colisão (CSMA / CD). Em todos os outros aspectos, o 10 GbE é o mesmo que o protocolo Ethernet original. Isso é importante para os gerentes de rede, pois, à medida que a demanda por velocidade aumenta, a Ethernet de 10 Gb pode ser facilmente implantada nas redes existentes, fornecendo uma tecnologia econômica, que pode suportar requisitos de alta velocidade e baixa latência.

O 10 GbE é frequentemente descrito como uma tecnologia disruptiva, que oferece uma abordagem mais eficiente e menos dispendiosa para mover dados em conexões de *backbone* entre redes. O padrão IEEE 802.3ae permite distâncias

entre locais físicos de até 40 quilômetros em uma fibra monomodo. Ambos os sistemas de fibra monomodo e multimodo podem ser usados com aplicativos de 10 GbE. A tabela a seguir mostra os padrões aceitos pelo 10 GbE.

TABELA 2 – PADRÕES 10 GIGABIT EHERNET

Nome	Cabo	Distância máxima do segmento	Vantagens
10GBase-SR	Fibra óptica	Até 300 m	Fibra multimodo (0,85µ)
10GBase-LR	Fibra óptica	10 km	Fibra monomodo (1,3µ)
10GBase-ER	Fibra óptica	40 km	Fibra multimodo (1,5µ)
10GBase-CX4	4 pares de Twinax	15 m	Cobre twinaxial
10GBase-T	4 pares de UTP	100 m	UTP padrão da categoria 6a

FONTE: Adaptado de Tanenbaum (1997).

Os desafios para implantar o Ethernet de 10 Gb se baseiam principalmente nos custos de implantação *versus* benefícios recebidos, com problemas associados à possível substituição de tecnologias de rede legadas, como linhas privadas ponto a ponto e/ou comutação de rótulo multiprotocolo. Dentre as vantagens do 10 GbE, podemos destacar:

- largura de banda com menor custo.
- troca mais rápida — o 10 GbE usa o mesmo formato Ethernet, que permite a integração perfeita de LAN, SAN, WAN e MAN, o que elimina a necessidade de fragmentação de pacotes, remontagem, conversão de endereços e roteadores.
- escalabilidade — a atualização de 1 GbE para 10 GbE é simples, porque seus caminhos de upgrade são semelhantes.

O 10 GbE é otimizado para dados e, portanto, não fornece qualidade de serviço integrada, embora isso possa ser fornecido nas camadas superiores.

5 CONCEITO E APLICAÇÃO DA IoT

O futuro da internet não compreenderá apenas milhões de serviços realizados entre máquinas e software, mas abrangerá bilhões de pessoas e seus dispositivos, além de contar com sensores, equipamentos portáteis, antenas miniaturizadas, robôs e objetos digitalizados. A IoT, que cresceu rapidamente nos últimos anos e apresenta rápida evolução, influenciará a definição de novas estratégias de alto impacto, sustentadas com a adoção de medidas inteligentes em infraestrutura na área de **tecnologia da informação (TI)**.

Profissionais da área industrial e acadêmicos estão constantemente procurando casos técnicos e futuros negócios que poderão ser desenvolvidos com o conceito transformador da IoT, abrangendo cada vez mais empresários, cientistas, pesquisadores, empreendedores e usuários finais nesses projetos. Governos nacionais em todo o mundo estão criando grupos especiais para apresentar estratégias, políticas, práticas e procedimentos, para levar adiante as ideias inovadoras da IoT. Cada vez mais os governantes compreendem o significado estratégico dessa nova era, prevista para conceber serviços centrados no público-alvo, visando a garantir e aprimorar o conforto, a chance de escolha, o atendimento personalizado e a convivência das pessoas nessa nova sociedade.

A IoT foi abraçada por vários países do mundo, em especial da Ásia e da Europa. Por exemplo, ela é parte de uma estratégia nacional da China (CHEN *et al.*, 2018), o Japão vem promovendo feiras e eventos nessa área desde 2004, e a União Europeia tem como objetivo liderar o caminho da Web 3.0 com a IoT. A perspectiva da IoT aproxima as tecnologias de TI, como as plataformas M2M (*machine to machine*), os sistemas ciberfísicos (*cyber-physical systems*) e a rede elétrica inteligente (*smart grid*), conhecidas como **tecnologias emergentes para comunicação entre dispositivos inteligentes**. Essas tecnologias influenciam muitos aspectos da vida real e, portanto, têm maiores implicações sociológicas, especialmente em um mundo em que questões como aquecimento global, proteção do meio ambiente e busca por fontes de energias renováveis estão sendo cada vez mais debatidas.

6 DEFININDO TECNICAMENTE A IoT

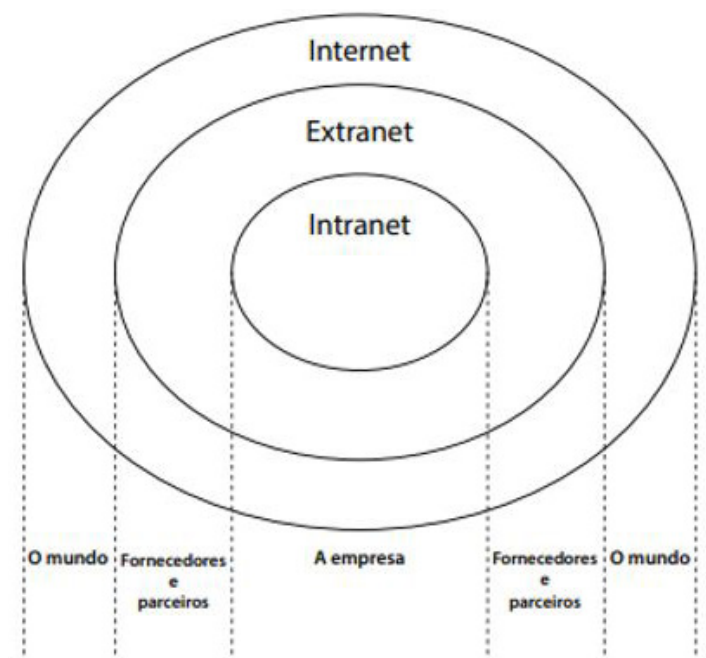
A definição de IoT depende mais dos aspectos e do ponto de vista adotado do que de outras variáveis. O que podemos considerar como unanimidade é o conceito de IoT como uma infinidade de tecnologias e seus aplicativos, que fornecem meios para acessarmos e controlarmos todos os tipos de dispositivos, instalações e ativos identificáveis em uma rede. Isso inclui equipamentos com inteligência inerente, como motores, sensores, atuadores, dispositivos móveis, controladores industriais, aparelhos domésticos, câmeras IP de segurança e também todo tipo de ativos marcados com identificação por radiofrequência (RFID, do inglês *Radio-Frequency Identification*).



A Web 3.0 é a terceira onda da internet, que abrange conceitos como a compreensão das máquinas e a semântica das redes. É a web inteligente, que é gerida por big data e datacenters (EL HAKIM, 2018). Já ICT é um termo utilizado para representar a evolução da internet e a sua modernização, que se refletem na disponibilização de novas tecnologias que transformam as formas de comunicação. A IoT, com a Web 3.0, estão inseridas na chamada terceira onda de ICT (ou terceira geração) (EL HAKIM, 2018). Por fim, RFID é uma tecnologia que usa campos eletromagnéticos para identificar objetos. Uma etiqueta RFID é composta por um pequeno rádio transponder, formado por um transmissor e um receptor. Por muitos anos, essa tecnologia foi considerada como uma das 10 maiores contribuições tecnológicas do século XXI (ADHIARNA; RHO, 2009).

Hoje, com a IoT, as comunicações são feitas com base em **todo tipo de alcance entre os dispositivos**, com ou sem fio, e **todo tipo de ambiente de rede**, como Intranet, Extranet e a própria internet. Esses ambientes são amparados por tecnologias de ponta, como *cloud computing*, *software as a service* e *service-oriented architecture*, e possuem medidas de segurança e privacidade adequadas, baseadas em formatos de dados regularizados e transmissão padronizada (ZHOU, 2013).

FIGURA 27 – VISÃO GERAL SOBRE O CONCEITO DE INTRANET, EXTRANET E INTERNET



FONTE: Adaptada de Zhou (2013).

O objetivo principal da IoT é alcançar uma maior conectividade e difusão em plataformas **M2M**, para prover segurança, disponibilidade, rapidez (*real-time*) e personalização de funcionalidades e serviços. Entre esses serviços e funcionalidades, estão: monitoramento remoto, detecção, rastreamento, alerta, programação, planejamento, manutenção, mineração de dados, tendências, relatórios, suporte a decisões, entre outros. A meta é construir um mundo universalmente conectado e altamente produtivo, seguro e sustentável.



O termo M2M, ou máquina a máquina, tem um significado literal: duas máquinas se comunicando. Ele se refere às tecnologias que permitem a sistemas tanto com fio quanto sem fio se comunicarem com outros dispositivos que possuem a mesma habilidade, sem intervenção ou interação humana (PERSIA; REA, 2016).

A internet (a rede física) e a web (as aplicações) são dois lados de uma mesma aplicação. A internet é a infraestrutura criada para fazer as interligações entre redes e dispositivos; já a web tem a ver com as aplicações usadas por todo mundo. Com a evolução da internet, na IoT, as aplicações e os softwares passaram a ser baseados na web. Os sistemas e aplicações baseados na web e os serviços de redes para sistemas inteligentes se expandem mais rapidamente do que os equipamentos e a infraestrutura (ZHOU, 2013). Essa é uma das razões pelas quais se acredita que, no futuro, as aplicações (software) desempenharão no mercado um papel central nos negócios envolvendo IoT.

Na evolução das aplicações para a internet, podemos citar a **Web 1.0**, caracterizada por publicações e envio de conteúdo para os usuários, em um **fluxo unidirecional**.

A **Web 2.0** é caracterizada por duas vias de fluxo de informações e está associada com aplicativos da web que facilitam a obtenção e o compartilhamento de informações, a interoperabilidade e a colaboração. Exemplos disso são os blogs, as redes sociais, o compartilhamento de vídeos, os jogos on-line, entre outros. Diz-se que a Web 1.0 e a Web 2.0 dizem respeito à Internet das Pessoas, enquanto a **Web 3.0** está relacionada à IoT.

Enterprise 2.0 é o nome dado ao uso de tecnologias da Web 2.0 dentro das empresas, para otimizar os processos de negócios, enquanto se aprimora a colaboração. É a extensão da Web 2.0 em aplicações corporativas. Sendo uma ferramenta já existente, é usada na integração do novo conceito de Web — a Web 3.0 — com as novas aplicações de IoT. Tecnologias baseadas na IoT podem ser integradas à Enterprise 2.0, em empresas que precisam monitorar e controlar equipamentos e instalações, integrando-os aos seus sistemas já existentes.

As definições de Web 3.0 variam bastante. Muitos argumentam que seus recursos mais importantes são a **Web Semântica** e a personalização; outros sugerem que a Web 3.0 é o ambiente no qual o computador está gerando novas informações, em vez do homem. O termo Web Semântica foi criada por Tim Berners-Lee, o inventor da World Wide Web, e é definido como sendo uma rede de dados que pode ser processada direta e indiretamente por máquinas (RAJ; RAMAN, 2017). Uma diferença fundamental entre a Internet das Pessoas (Web 1.0 e Web 2.0) e a Internet das Coisas (Web 3.0) é que, **na IoT, os dados são gerados por máquinas, e não por humanos.**

7 O ECOSSISTEMA DA INTERNET OF THINGS E O USO DE TECNOLOGIAS SEM FIO

A tecnologia M2M tem revolucionado as redes sem fio pelo mundo, conduzindo à criação e ao uso de uma grande quantidade de tecnologias e serviços de suporte. Os serviços M2M estão interligados ao mundo dos dispositivos IoT; portanto, as tecnologias de serviços móveis também evoluíram para dar suporte M2M e, por isso, fazem parte do ecossistema IoT. Veja, a seguir, algumas das principais tecnologias sem fio que evoluíram para dar suporte aos requisitos que são específicos para o sistema IoT.

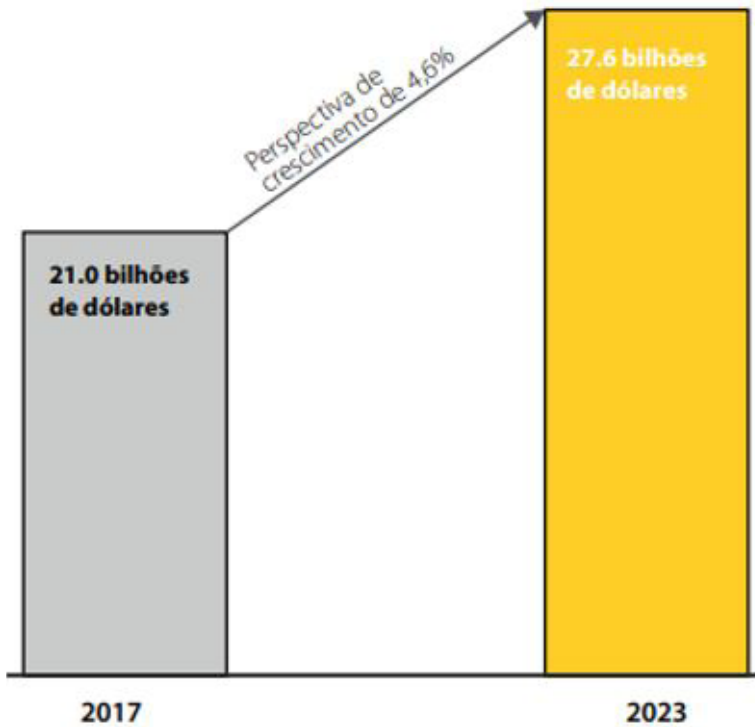
- **Redes celulares:** 4G e 5G são, respectivamente, a quarta e a quinta geração das redes de telefonia celular, dentro de sua evolução tecnológica nas últimas duas décadas.
- **LPWAN** (*low-power wide area network*): tecnologia utilizada para a comunicação entre dispositivos a longa distância com baixo consumo de energia.
- **WPAN** (*wireless personal area network*): rede sem fio para comunicação privada entre dispositivos.

Um dos principais desafios do mundo IoT é o gerenciamento de energia, pois, como proceder para fornecer energia para milhões de dispositivos que fazem parte de um mesmo ecossistema? Entre as tecnologias que despontam para tentar sanar esse problema estão a LPWAN e alguns dos protocolos (operadores) que serão abordados mais adiante neste capítulo, mais precisamente Sigfox, ZigBee, *Narrow Band IoT* (NB-IoT) e *Long Range WAN* (LoRaWAN).

As redes móveis já oferecem conectividade a uma ampla variedade de dispositivos, que abriram novas regiões de opção de serviço, tanto para provedores e operadoras quanto para usuários finais (RAJ; RAMAN, 2017). Um tipo de serviço que tem criado um impacto significativo no dia a dia das pessoas são os serviços da tecnologia M2M. Atualmente, os dispositivos móveis inteligentes são utilizados para interagir e controlar locais e máquinas e, portanto, são candidatos a fazer parte dos dispositivos que suportam M2M. As conexões M2M, como parte de um total de conexões móveis, são um forte indicador de mercado.

A agência de pesquisa de mercado MarketandMarkets, em uma publicação de 2016, estimou o crescimento de 27,62 bilhões de dólares do mercado de conexões M2M até 2023, chegando a uma quantidade de 3 bilhões de conexões M2M. No ano da pesquisa, o número de conexões M2M era de 1,47 bilhão, com valor de mercado de 19,31 bilhões de dólares.

FIGURA 28 – PERSPECTIVA DE CRESCIMENTO DE MERCADO DE CONEXÕES M2M



FONTE: Adaptado de Markets and Markets (2020).

O segmento de conectividade tecnológica detém a maior parte do mercado de conexões M2M, em termos de número de conexões. No entanto, é esperado que o mercado de tecnologia sem fio cresça em taxa mais alta no mercado de conexões M2M até 2023.

8 ARQUITETURA PARA IoT USANDO DISPOSITIVOS MÓVEIS

Não existe uma representação simples e genérica da arquitetura definitiva para IoT — e isso é uma unanimidade entre pesquisadores do mundo inteiro. Muitas arquiteturas diferentes têm sido propostas por pesquisadores. Alguns deles afirmam que a arquitetura deve ser composta por três camadas (*three-layers architecture*); outros defendem o modelo de arquitetura de quatro camadas (*four-layers architecture*). Eles acham que, devido à evolução e ao aprimoramento

da IoT, a arquitetura de três camadas não seria suficiente para atender aos requisitos dos aplicativos. Devido a um desafio na IoT com relação à segurança e à privacidade, a arquitetura de cinco camadas também foi proposta. Considera-se que essa arquitetura proposta por último tem a capacidade de atender a todos os requisitos com relação à segurança.

A figura a seguir mostra o modelo de arquitetura mais básico, que cumpre também as ideias básicas para a IoT. Ele foi proposto nas primeiras etapas do desenvolvimento da IoT. Essa arquitetura tem **três camadas**, conhecidas como **percepção, rede e aplicação** (BURHAN *et al.*, 2018):

- a camada de percepção é representada pelos dispositivos (sensores);
- a camada de rede indica qual tecnologia vai prover a comunicação entre esses dispositivos;
- por fim, a camada de aplicação representa a interação do usuário final com a tecnologia, por meio de aplicações (software).

FIGURA 27 – EXEMPLO DE ARQUITETURA DE TRÊS CAMADAS PARA IoT



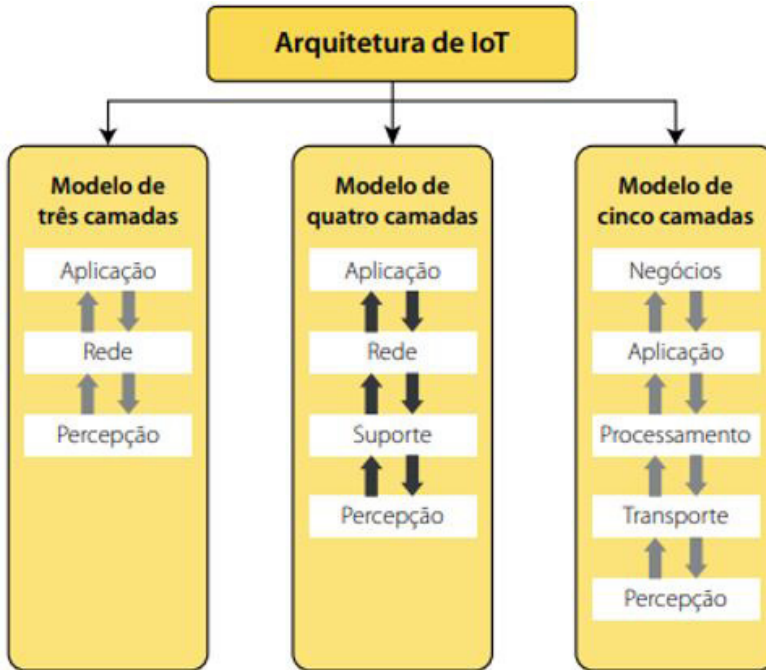
FONTE: Burhan *et. al* (2018)

A camada de percepção é também conhecida como camada dos sensores. Analogamente, ela funciona como os olhos, as orelhas e o nariz das pessoas. Ela tem a responsabilidade de identificar as “coisas” e coletar as informações delas. Existem inúmeros tipos de sensores anexados aos objetos para coletar essas informações, como RFID, códigos de barras e sensores. Esses sensores são escolhidos de acordo com a necessidade da aplicação, e as informações colhidas por eles podem ser sobre localização, mudanças no ar, ambiente, movimento, vibração, entre outros aspectos (ADHIARNA; RHO, 2009).

A criação da **arquitetura de quatro camadas** desempenhou um papel muito importante nas normas para desenvolvimento da IoT, já que apresentou a inserção da camada de suporte. Porém, havia também alguns problemas relacionados à segurança e ao armazenamento das informações nessa topologia.

Por isso, foi proposto o **modelo de cinco camadas**, com foco na segurança. Nessa arquitetura, as camadas de aplicação e percepção se mantiveram, e foram criadas as camadas de transporte, processamento e negócios.

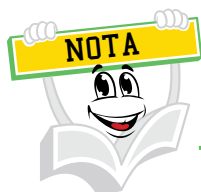
FIGURA 28 – AS ARQUITETURAS DE CAMADAS PARA IoT



FONTE; Burhan et. al (2018)

A seguir, a comunicação entre as camadas é apresentada de forma simplificada, como proposto por Raj e Raman (2017), destacando-se os principais componentes da arquitetura IoT.

- Os dados são coletados de uma grande quantidade de fontes e equipamentos, usando telefones móveis. Esses dados provêm de sensores remotos e outros dispositivos eletrônicos, sendo gerados a partir de vários componentes de infraestrutura, como edifícios, empresas, operadoras e sistemas de transportes.
- Esses dados são transferidos, usando-se várias opções de redes cabeadas e sem fio, para algum tipo de banco de dados, ou *data warehouse*, para serem coletados e armazenados. Ferramentas de análise são aplicadas nesses dados, para se obterem informações significativas, que definam as ações futuras.
- Esses dados servirão de entrada para as plataformas de prestação de serviços (SDPs, do inglês *Service Delivery Platforms*), que executarão inúmeras aplicações de serviços para IoT. Esses serviços abrangem todos os domínios, como transporte, saúde, operadoras, redes de comunicação, instituições financeiras etc. Essas SDPs fornecerão interfaces de programação de aplicações (APIs, do inglês *Application Programming Interfaces*) abertas, que ajudarão desenvolvedores a projetarem novos serviços, assim, agregando valor à plataforma.



SDP é uma plataforma de entrega de serviços que cria, hospeda e gerencia serviços em diferentes canais e dispositivos do usuário final. Essa plataforma de entrega inclui serviços de telecomunicações tanto com cabo quanto sem fio (RAJ; RAMAN, 2017).

9 TECNOLOGIAS MÓVEIS PARA SUPORTE AO ECOSISTEMA IoT

Uma máquina conectada não se torna “inteligente” a partir de um único sensor, *modem*, rede ou aplicativo (software) sozinho. É a combinação de todas essas peças que cria a inteligência adicional dos dispositivos. Há uma variedade de tecnologias sem fio que permitem a conectividade IoT, todas com benefícios e restrições. A escolha consciente da tecnologia sem fio deve ser feita de acordo com as aplicações. As opções mais comuns para conectividade IoT são:

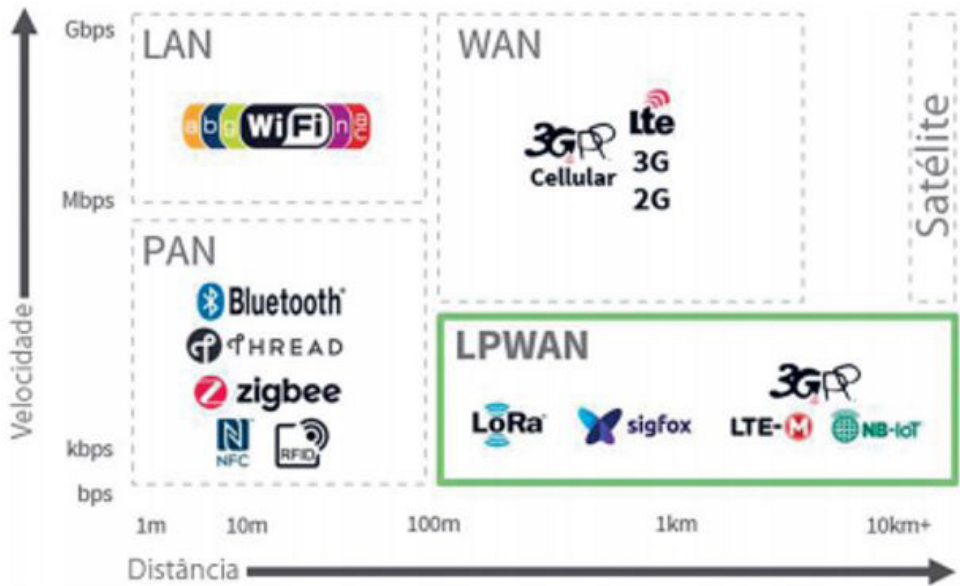
- por proximidade, como **RFID**;
- WPAN, como **Bluetooth**;
- Wireless LAN (WLAN), como **Wi-Fi**;
- LPWAN, como **LoRA** e **Sigfox**;
- por tecnologia celular, como **4G** e **5G** (padrões 3GPP).



3GPP (3rd generation partnership project) é um projeto que une sete organizações de desenvolvimento de padrões para as telecomunicações, conhecidas como parceiros organizacionais. O grupo foi criado nos anos 1990, com o intuito de focar na criação de padrões e especificações para sistemas de comunicação móveis. (3GPP, 2020)

Diversas tecnologias sem fio para IoT são mostradas na Figura 30, comparando a distância alcançada e a velocidade de transmissão dos dados.

FIGURA 30 – COMPARATIVO ENTRE TECNOLOGIAS SEM FIO COM SUPORTE PARA IoT



FONTE: Adaptada de Hayes (2019)



As siglas WAN e PAN, bastante utilizadas quando se trata de tecnologias de comunicação, correspondem, respectivamente, aos termos *wide area network*, que significa rede de longa distância, e *personal area network*, que significa rede de área pessoal. Já LAN se refere ao termo *local area network*, ou rede de área local. Por fim, MAN se refere à rede de área metropolitana, ou *metropolitan area network*, em inglês.

9.1 TECNOLOGIA CELULAR (4G/5G)

Redes celulares são exemplos de redes WAN com capacidade de longo alcance para conexão globalizada, usando ondas de radiofrequência para enviar e receber dados via torres de comunicação. Conexões robustas e confiáveis podem ser criadas entre dispositivos e torres de comunicação com até 16 km de distância, eliminando ainda mais as barreiras para a conectividade em áreas remotas (EL HAKIM, 2018).

A **família 3GPP** de tecnologia de redes celulares é a plataforma líder em comunicação sem fio em todo o mundo. O que começou como um padrão global único para telefonia móvel evoluiu para uma ampla gama de tecnologias de rede 2G, 3G e 4G, que operam em uma faixa cada vez maior de bandas de frequência, suportando altas taxas de transmissão de dados em alta velocidade. Dividimos a família de padrões 3GPP em quatro categorias principais (MEKKI et al., 2018):

- os padrões 2G, com o serviço GPRS (general packet radio service);
- os atuais 3G/4G, com as tecnologias high speed packet access (HSPA) e long-term evolution (LTE); e
- a emergente 4G-MTC, com os padrões LTE-M e NB-IoT, plataformas de tecnologias que vão conectar dispositivos IoT às redes de telefonia celular.

As primeiras especificações oficialmente reconhecidas para as comunicações 5G foram incluídas nos estudos da organização 3GPP e lançadas em 2018 no documento “3GPP Release 15”.

9.2 LOWER-POWER WIDE AREA NETWORK (LPWAN)

LPWANs são redes de telecomunicações do tipo WAN projetadas para permitir comunicação a longa distância, a uma baixa taxa de bits de transmissão (0.3 kbit/s a 50 kbit/s por canal), para dispositivos do tipo sensores, operados por bateria, que operam na faixa de frequência ISM (*Industrial, Scientific and Medical band*) (MEKKI *et al.*, 2018). A faixa ISM corresponde a bandas de frequências reservadas internacionalmente para o desenvolvimento industrial, científico e médico, que não possuem necessidade de licenciamento e são normatizadas para limitação de potência (*low power*). É uma tecnologia que poderá ser usada para criar uma rede privada sem fio para sensores.

As necessidades das aplicações para IoT e M2M deram origem a alguns requisitos específicos das tecnologias LPWAN, que têm o **padrão estrela** (*star-topology*) como modelo de topologia de rede, em vez de uma rede em malha. Os dispositivos da rede estrela são conectados diretamente nos *access-points*. Repetidores podem ser usados para cobrir áreas que possam apresentar perda de potência de sinal, devido a áreas de sombra. Os principais protocolos para a tecnologia LPWAN são apresentados a seguir.

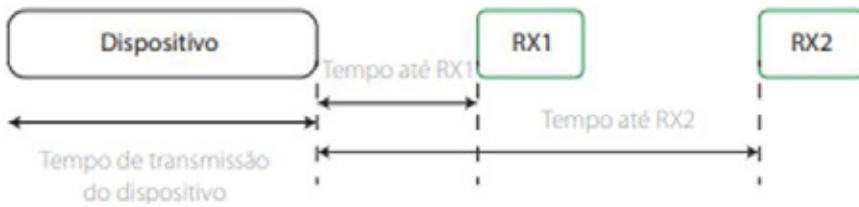
O **LoRaWAN** é um protocolo padrão LoRa com especificação para redes sem fio, baixo custo e operado por baterias. Foi padronizado pela LoRa-Alliance para atuar na camada física, usando uma técnica própria de espalhamento espectral (*spread spectrum*). Busca prover uma comunicação bidirecional por meio da modulação *chirp spread spectrum*, que espalha o sinal de banda estreita sobre um canal com maior largura de banda. Isso resulta em um sinal com baixo ruído, alta resistência a interferência e dificuldade para detecção (MEKKI *et al.*, 2018).

O LoRa tem uma taxa de transmissão de 300 bps a 50 kbps que depende da largura de banda do canal e do fator de espalhamento. Mensagens transmitidas usando diferentes fatores de propagação podem ser recebidas simultaneamente pelas estações-base LoRa.

Usando LoRaWAN, cada mensagem transmitida por um dispositivo é recebida por todas as estações-base LoRa vizinhas (RX1 e RX2). Ao explorar essa recepção redundante, LoRaWAN melhora a taxa de mensagens recebidas

com sucesso; porém, essa solução requer várias estações próximas, o que pode acarretar altos investimentos em recursos de implantação.

FIGURA 31 – COMUNICAÇÃO BIDIRECIONAL ENTRE DISPOSITIVO E ESTAÇÃO-BASE LORAWAN



FONTE: Adaptada de Mekki et al. (2018)

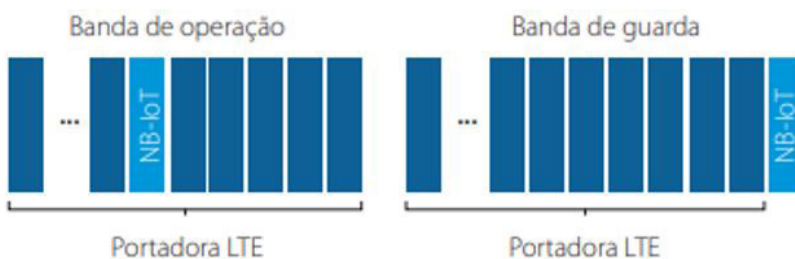
Sigfox, por sua vez, é o protocolo LPWAN mais comum em ambientes industriais. Possui parceria com muitos fornecedores de rádio, como Texas Instruments, Silicon Labs e Axom.

O Sigfox, diferentemente do LoRa, não suporta comunicação bidirecional na rede e oferece suporte apenas para aplicativos de sensores *uplink*. Isso impõe uma restrição ao usuário final, que transfere apenas 15 bytes de tráfego por vez, com uma média de apenas 10 mensagens por dia. Isso limita a usabilidade dessa tecnologia apenas para dispositivos muito simples.

O Sigfox usa antenas configuradas em torres para receber dados de dispositivos como sensores de estacionamento e sensores de água. As transmissões de dados usando a tecnologia Sigfox ocorrem em 868 MHz (na Europa) ou bandas de frequência de 915 MHz na América do Norte.

A **NB-IoT** é uma tecnologia considerada faixa estreita pelo 3GPP no Release 13, de 2016. Ela pode coexistir com o padrão LTE sobre uma faixa de frequência licenciada (700 MHz, 800 MHz e 900 MHz). O protocolo NB-IoT, quando implementado, ocupa uma largura de banda de 200 kHz, que corresponde a um bloco de recursos da transmissão LTE. É um protocolo que atua na interface aérea de transmissão de uma rede celular e é focado nos dispositivos alimentados por baterias (sensores).

FIGURA 32 – MODO DE OPERAÇÃO PARA NB-IOT.



FONTE: Adaptada de Mekki et al. (2018)

O protocolo de comunicação NB-IoT é baseado no protocolo LTE. De fato, o NB-IoT reduz as funcionalidades do protocolo LTE ao mínimo e as aprimora conforme necessário para as aplicações de IoT. Por exemplo, o sistema de *back-end* LTE é usado para transmitir informações válidas para todos os dispositivos de uma célula. Como o sistema de *back-end* de transmissão obtém recursos e consome energia da bateria de cada dispositivo final, ele é mantido no mínimo, tanto em tamanho quanto em sua ocorrência. Isso foi otimizado para mensagens de dados pequenas e pouco frequentes e evita o uso de recursos não necessários para a finalidade da IoT; por exemplo: medições e monitoramento da qualidade do canal, agregação de operadora e dupla conectividade. Portanto, os dispositivos requerem apenas uma pequena quantidade de bateria, tornando-os econômicos.

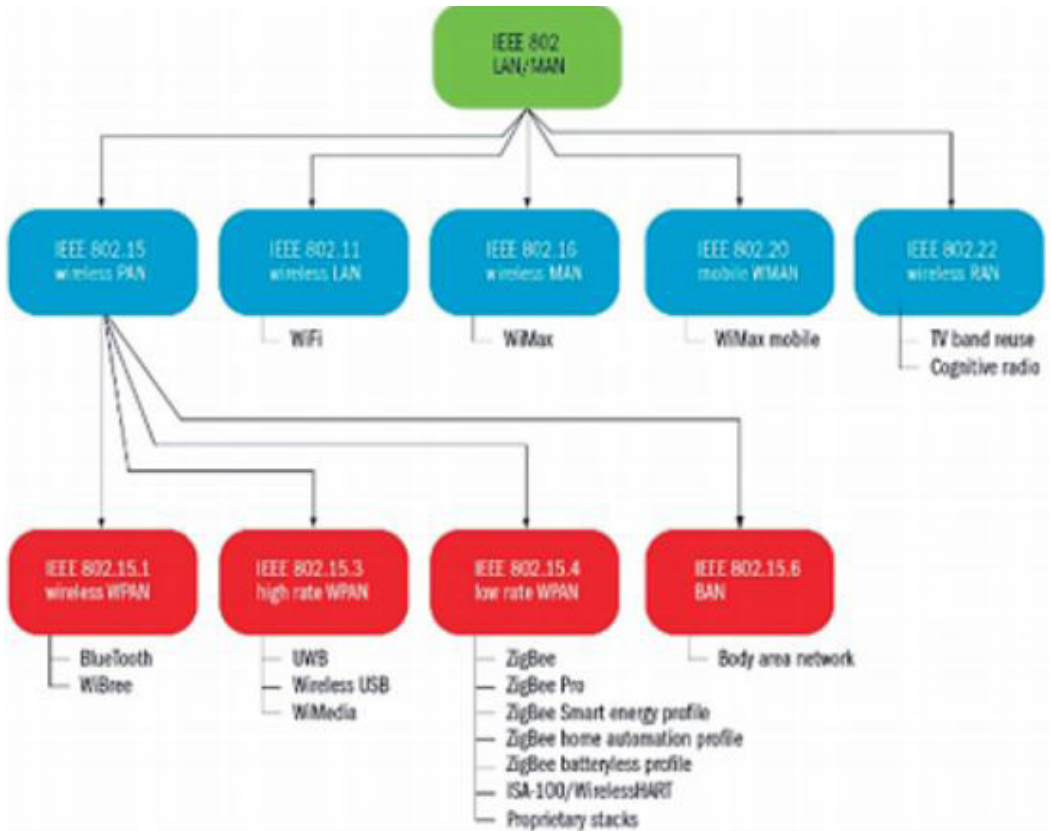
Consequentemente, a tecnologia NB-IoT pode ser considerada como uma nova interface aérea do ponto de vista das pilhas de protocolos. O NB-IoT é preferido para aplicações que requerem QoS (*Quality of Service*), pois atua em uma faixa de frequência licenciada, diferentemente das aplicações Sigfox e LoRa. Ele também provê baixa latência e possui maior escalabilidade, por permitir conexões superiores a 100 K por célula, em comparação aos 50 K suportados por Sigfox e LoRa.

Os fatores e as diferenças técnicas entre Sigfox, LoRa e NB-IoT determinarão sua viabilidade para aplicativos específicos. Conforme visto, uma tecnologia não pode igualmente atender e oferecer suporte a todas as aplicações em IoT

9.3 WIRELESS PERSONAL AREA NETWORK (WPAN)

WPAN é a designação para redes pessoais sem fio, regulamentadas pelo **padrão IEEE 802.15**, do Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE). A Figura 33 mostra a divisão do padrão IEEE 802, que regulamenta todas as tecnologias sem fio no mercado de telecomunicações. O foco deste tópico é o padrão que norteia os estudos e as aplicações para as redes sem fio PAN.

FIGURA 33 – PADRÃO IEEE 802 LAN/MAN



FONTE: Adaptado de Melo (2020c)

9.3.1 IEEE 802.15.1: Bluetooth e Bluetooth Low Energy

Bluetooth e Bluetooth Low Energy (também conhecido como Bluetooth Smart) são tecnologias sem fio usadas para transferência de dados a curtas distâncias. São usadas frequentemente para conectar dispositivos pequenos a telefones/*tablets* e também sistemas de alto-falante, como em *home-theaters*. Trata-se de um protocolo de comunicação de curto alcance a nível de camada física e enlace, que possui baixa energia, pode atingir 10 vezes menos que o Bluetooth clássico, enquanto sua latência pode atingir 15 vezes.

Ele segue a arquitetura cliente/servidor e oferece dois tipos de quadros (frames): *advertising* e *data*. O quadro *advertising* é usado para “descoberta” e é enviado por clientes em um ou mais canais dedicados. Os servidores detectam os canais para encontrar clientes e conectá-los. Após a conexão, o servidor informa ao cliente o seu ciclo de espera e a sequência de programação. *Nodes* geralmente ficam ativos apenas quando estão se comunicando e ficam em *stand-by* para economizar energia.

Dispositivos Bluetooth, quando se conectam e se comunicam por meio de uma rede *ad-hoc* (sem uma estação-base), formam um **Piconet**. Piconets são dinamicamente estáveis e automatizados para permitirem a dispositivos Bluetooth se comunicarem e ficarem próximos ao sinal de rádio. Suportam até oito dispositivos, sendo um master (principal) e sete clientes, com área de cobertura de até 10 m, e até 1 Mbps de taxa de transmissão. Dois ou mais Piconets formam uma rede chamada de **Scatternet**.

9.3.2 IEEE 802.15.4: ZigBee

A tecnologia **ZigBee** é mais simples e mais barata do que a Bluetooth (BUYYA; DASTJERDI, 2016). Os principais objetivos da categoria LR-WPAN (low-rate WPAN), na qual o ZigBee se enquadra, são:

- facilidade de instalação;
- transferência confiável de dados;
- operação de curto alcance;
- extremamente baixo custo;
- duração razoável da bateria; e
- protocolo simples e flexível.

Dois tipos de dispositivos podem fazer parte de uma rede LR-WPAN: os FFDs (*Full-Function Devices*) e os RFDs (*Reduced-Function Devices*). Dispositivos FFD podem operar de três modos: coordenador PAN, coordenador e dispositivo. Já os RFDs se destinam apenas a aplicações mais simples.

Na arquitetura ZigBee, um dispositivo FFD pode se comunicar com um dispositivo RFD ou com outro dispositivo FFD. Já um RFD só pode se comunicar com um FFD.

Dois ou mais dispositivos se comunicando por um mesmo canal físico constituem uma WPAN. Para isso, toda rede WPAN precisa definir pelo menos um dispositivo FDD que funcione como coordenador PAN. Esse coordenador será o elemento principal da rede, iniciando, terminando e roteando todas as informações da rede.

Uma WPAN pode operar em duas topologias: estrela (*star topology*), e ponto a ponto (*peer-to-peer topology*).

10 APLICAÇÕES DA INTERNET DAS COISAS

A telemetria é uma tecnologia antiga, que permite a remota medição e comunicação de informações. Apesar de o termo geralmente se referir a mecanismos de transferência de dados sem fio, também abrange dados transferidos por outras mídias com fio. Para alguns pesquisadores, a telemetria é sinônimo de IoT, e pode ser considerada como um dos primeiros aplicativos para tal. É de perto relacionada e interligada com outras tecnologias IoT e aplicações como M2M e *supervisory control and data acquisition*, que significa supervisão, controle e aquisição de dados.

Em 1874, os engenheiros franceses construíram no Mont Blanc um sistema de clima e neve, usando sensores que transmitiam em tempo real informações para Paris. Telecomando e telemática (informática das telecomunicações) estavam mais relacionados à telemetria em tempos anteriores. No entanto, hoje, a telemática geralmente se refere ao rastreamento de veículos, especialmente ao rastreamento de carros de passageiros e serviços de sistema de posicionamento.

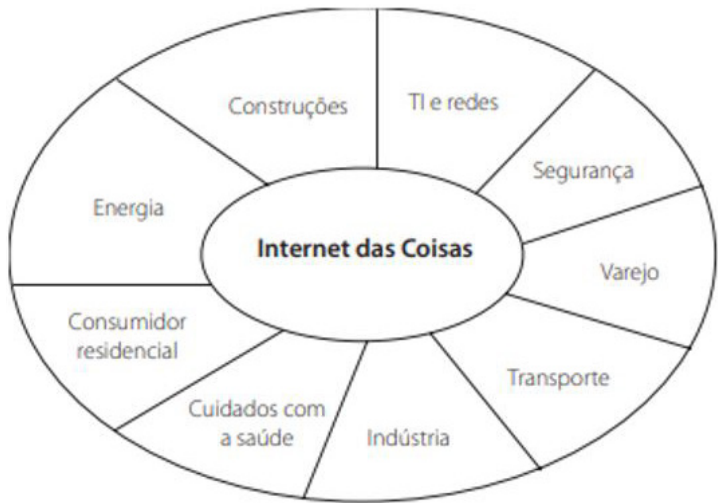
Avanços nas tecnologias de rede e na normatização de protocolos de comunicação baseados em Extensible Markup Language, representações de dados e arquiteturas de *middleware* tornam possível coletar dados de sensores e dispositivos praticamente em qualquer lugar, a qualquer momento. *Chips* de silício cada vez menores estão ganhando novas capacidades, enquanto os custos estão caindo. Aumentos cada vez maiores em capacidade de armazenamento e computação disponível via *cloud computing* possibilitam o processamento de números e dados em escala muito grande e com custo decrescente, como acontece no big data. Podemos listar algumas possibilidades de dispositivos e aplicações relacionadas a esse contexto:

- redes de sensores em malha para monitorar de forma confiável as erupções vulcânicas;
- óculos inteligentes para deficientes visuais, que possam interpretar o ambiente ao seu redor;
- uma rede de sensores para controlar o fluxo de veículos e evitar congestionamentos e, por conseguinte, diminuir a emissão de gases tóxicos;
- sensores IoT para coletar dados de várias linhas de produção na indústria e controlar todo um ciclo de produção.

A criação do conceito de IoT e o seu destaque mundial são relevantes para questões sociais, econômicas e ambientais, possibilitando encarar desafios como mudanças climáticas, proteção do meio ambiente, economia de energia e globalização. Por esses e outros motivos, a IoT é cada vez mais utilizada em um grande número de setores: indústria, medicina, pesquisa, segurança, energia e logística são alguns exemplos. Plataformas M2M e dispositivos móveis incorporados estão enviando dados para servidores cada vez mais robustos e autônomos.

O objetivo da IoT é alcançar conectividade M2M difundida e grande interação, fornecendo funcionalidades seguras, rápidas e personalizadas. Tais serviços podem ser de monitoramento, detecção, rastreamento, localização, alertas, agendamento, controle, automação, mineração de dados, tendências de mercado etc. Segundo a Beecham Research, empresa britânica líder em pesquisa, análise e consultoria no mercado de tecnologia, o mercado M2M é dividido em nove setores de serviços principais.

FIGURA 34 – INTERNET DAS COISAS E SETORES QUE UTILIZAM M2M



FONTE: Adaptada de Vermesane Friess (2014)

As aplicações para IoT podem ser classificadas com base no domínio do aplicativo e nos grupos de usuários de destino (BUYYA; DASTJERDI, 2016). Essas aplicações geralmente se enquadram em três categorias: monitoramento e atuação; processo de negócios e análise de dados; e coleta de informações e consumo colaborativo.

10.1 MONITORAMENTO E ATUAÇÃO

O monitoramento de dispositivos via M2M por meio de APIs pode ser útil em vários domínios. Em **indústrias**, as APIs podem relatar o uso de energia, o desempenho de um equipamento e o status de um sensor e podem executar ações, ao serem enviados comandos predefinidos. Aplicativos em tempo real podem utilizar esses recursos para relatar o status atual do sistema, enquanto os gerentes e os desenvolvedores têm a opção de acessar livremente essas APIs, sem a necessidade de acessar fisicamente os dispositivos. A medição inteligente e, de forma mais abrangente, as redes inteligentes podem ajudar na identificação de defeitos de desempenho, por meio da aplicação de detecção de anomalia nos dados coletados, aumentando, assim, a produtividade.

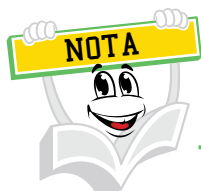
Da mesma forma, incorporando a IoT em **edifícios** ou mesmo no processo de construção destes, pode-se avançar em direção a soluções verdes, economizar energia e, consequentemente, minimizar os custos de operação. Outra área que tem sido objeto de foco dos pesquisadores são as **residências inteligentes** (*smart homes*), que visam principalmente a possibilitar economia de energia e monitoramento. Estruturas domésticas de monitoramento e controle suportam diferentes protocolos de comunicação (Wi-Fi, Bluetooth etc.) para criar uma rede interconectada de objetos, que possa controlar os parâmetros desejados e alterar configurações baseadas nas opções do usuário.

10.2 PROCESSO DE NEGÓCIOS E ANÁLISE DE DADOS

Buyya e Dastjerdi (2016) avaliaram a adoção da IoT na sociedade, por meio da utilização da análise de big data para as categorias listadas a seguir.

- **Nível da sociedade:** a IoT influencia e melhora principalmente os serviços governamentais, reduzindo os custos e aumentando a transparência na prestação de contas do governo.
- **Nível da indústria:** manufatura, serviços de emergência, varejo e educação foram estudados como exemplos.
- **Nível organizacional:** a IoT pode trazer o mesmo tipo de benefícios que os mencionados a nível de sociedade.
- **Nível individual:** melhorias na vida diária, na eficiência individual e na produtividade são marcadas como benefícios da IoT.

A capacidade de capturar e armazenar grandes quantidades de dados individuais trouxe oportunidades para a assistência médica. Os dados dos pacientes podem ser capturados com mais frequência, usando tecnologias vestíveis, como relógios inteligentes, e podem ser publicados na internet. Mais tarde, a mineração de dados e os algoritmos de aprendizado de máquina são usados para extrair conhecimento e padrões dos dados brutos e arquivar esses registros para futura referência.



O Healthsense eNeighbor, desenvolvido pela Humana, empresa líder em assistência médica, é um exemplo de sistema de controle remoto que usa sensores implantados nas casas para medir atividades diárias e parâmetros de saúde dos ocupantes. Os dados coletados são, então, analisados para prever riscos plausíveis e produzir alertas para evitar incidentes. Desafios de privacidade e segurança são duas barreiras principais que abstem pessoas e indústrias de adotarem a IoT no domínio da saúde.

10.3 COLETA DE INFORMAÇÕES E CONSUMO COLABORATIVO

A **Internet Social das Coisas** (SIoT) é onde a IoT encontra as redes sociais e, mais precisamente, promete vincular objetos ao nosso redor com nossas mídias sociais e nossa interação diária com outras pessoas.

O conceito SIoT, se relacionado às mídias sociais, como o Facebook e o Twitter, tem o potencial de afetar o estilo de vida de muitas pessoas.

Por exemplo, uma rede social é útil para a avaliação da confiança das multidões envolvidas em um processo de eleição.

Outra vantagem é usar as pessoas e os seus relacionamentos, as suas comunidades e as suas interações para a descoberta eficaz de serviços de IoT.



RESUMO DO TÓPICO 2

Neste tópico, você aprendeu que:

- A evolução do padrão Ethernet criou várias vertentes do padrão Ethernet, todas elas compatíveis entre si. Uma das vantagens do padrão é a possibilidade de usar diferentes tipos de cabos e dispositivos e, mesmo assim, compatíveis.
- Existe a necessidade de modernização; esta é a realidade atual. Com o surgimento da Indústria 4.0, expressão utilizada para a junção das tecnologias operacionais e digitais, tornou-se necessária a modernização das empresas e da indústria em geral para competitividade e sobrevivência no mercado nacional e internacional. O uso em conjunto da automação industrial, de sistemas ciberfísicos e dos conceitos da tecnologia da informação, como Internet das Coisas e Cloud Computing, permite novos métodos e aplicabilidades para a indústria convencional.



1 O padrão Ethernet, criado há mais de 40 anos, é o mais utilizado para a interconexão de redes. Entre os motivos para que ele ainda permaneça como líder no mercado, destacam-se:

- I- Ausência padrões concorrentes.
- II- Interoperabilidade entre os padrões Ethernet.
- III- Facilidade de expansão de redes Ethernet.

São CORRETAS as assertivas:

- a) () Apenas I.
- b) () Apenas II.
- c) () Apenas III.
- d) () Apenas II e III.
- e) () Apenas I e III.

2 Para compreender o funcionamento do padrão Ethernet, é necessário conhecer algumas terminologias para explicar seu funcionamento. Algumas delas são:

- I- Os nós são os dispositivos que se comunicam pela Ethernet.
- II- O meio é o caminho usado pelos dispositivos para se comunicar.
- III- O segmento é uma mensagem curta compartilhada pela rede.
- IV- O quadro é o meio compartilhado.

São CORRETAS as assertivas:

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

3 No padrão Ethernet, em virtude de compartilhar um mesmo meio, é necessário que se tenha controle de quem pode enviar um quadro pelo meio. No padrão Ethernet, quem realiza esse controle é o CSMA (Carrier Sense Multiple Access). Com relação ao CSMA, analise seguintes assertivas:

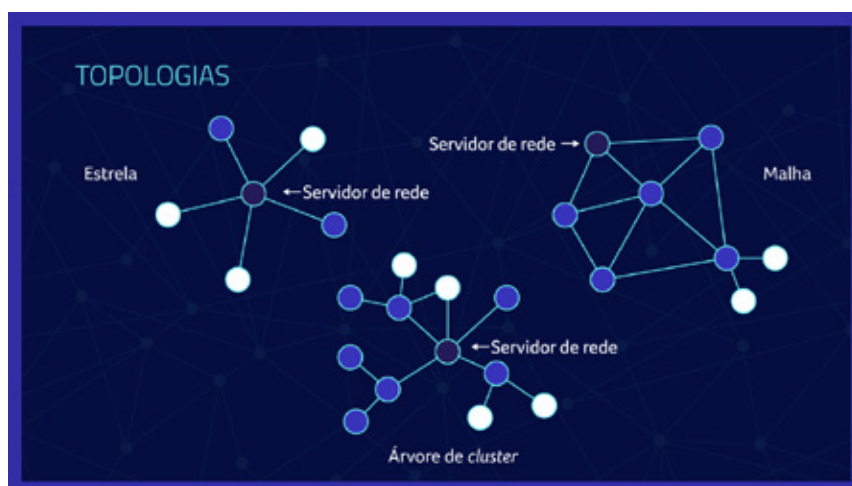
- I- Nas conexões 100Base-TX, é necessário o uso do CSMA.
- II- A finalidade desse protocolo é manipular os pacotes descartados, perdidos ou corrompidos.
- III- É possível que o processo falhe e dois dispositivos transmitam ao mesmo tempo.

São CORRETAS as assertivas:

- a) () Apenas I.
- b) () Apenas II.
- c) () Apenas I.
- d) () Apenas I e II.
- e) () Apenas II e III.

4 WPANs (Wireless PAN) são usadas para transmitir informações em curtas distâncias entre um grupo particular de dispositivos, chamado de nó (ou nodes). Diferentemente de uma WLAN (Wireless LAN), uma conexão feita por meio de uma WPAN envolve pouca ou nenhuma infraestrutura ou conectividade direta (tecnologia AD-HOC) para a Internet. Isso permite soluções pequenas, econômicas e com baixo consumo de energia a serem implementadas em uma ampla gama de dispositivos.

Em topologias diversas para rede WPAN em IoT, conforme a figura a seguir, qual a função dada ao dispositivo sinalizado como servidor de rede?



- a) () Piconet.
- b) () Access Point (AP) — ponto de acesso.
- c) () Coordenador PAN.
- d) () Scatternet.
- e) () PAN switch.

5 O padrão IEEE 802.15.1 (Bluetooth e BLE) visa a obter aceitação global, de forma que qualquer dispositivo Bluetooth, em qualquer lugar do mundo, possa conectar-se a outros dispositivos Bluetooth nas proximidades. Esse padrão dá suporte por canais de comunicação síncronos para comunicações de voz de nível telefônico e canais de comunicação assíncronos para comunicação de dados. Com base nessa informação, em qual das redes a seguir pode-se utilizar tal padrão para a comunicação entre dispositivos IoT?

- a) () LAN (Local Area Network) — área de rede local.
- b) () PAN (Personal Area Network) — área de rede privada.
- c) () WAN (Wide Area Network) — área de rede distante.
- d) () MAN (Metropolitan Area Network) — área de rede metropolitana.
- e) () LTE (Long-Term Evolution).

6 Electronic Product Code (EPC), código eletrônico de produto, é considerado um padrão bem estabelecido para sistema de numeração e identificação. Esse sistema objetiva ter melhor identificação quando comparado aos códigos de barras. Todos os sistemas são definidos em bits de cabeçalho EPC. O número restante consiste em bits do gerenciamento EPC, representando a empresa (fabricante) envolvida na produção do dispositivo/item. Objeto EPC são bits de classe que definem o código para o próprio produto, e os bits de número de série EPC servem para a identificação do produto individual. Esse sistema de numeração de 96 bits é capaz de fornecer capacidade suficiente para 268 milhões de empresas, permitindo que cada fabricante crie até 16 milhões de classes de objetos com 68 bilhões de números de série em cada classe (ADHIARNA; RHO,2009).

De acordo com o trecho citado, pode-se interpretar que se trata de um sistema de identificação para dispositivos, equipamentos, sensores etc. Qual das tecnologias sem fio listadas a seguir poderia ser utilizada caso você quisesse implementar tal sistema em uma rede privada de sensores inteligentes para IoT?

- a) () RFID.
- b) () LTE Advanced.
- c) () 4G/5G.
- d) () LPWAN.
- e) () ZigBee.

CONEXÃO DE EQUIPAMENTOS E NOÇÕES DE SEGURANÇA

1 INTRODUÇÃO

O módulo Bluetooth ligado ao Arduino tem sido bastante utilizado em projetos que têm a necessidade da troca de dados ou informações a distância, sem precisar utilizar cabos ou fios para realizar essa conexão. Conectar o Bluetooth na plataforma microcontrolada Arduino permite controlar dispositivos a distância através de celulares, tablets ou notebooks. Atualmente, utilizamos diversos aparelhos, portáteis ou não, que têm o padrão de comunicação Bluetooth embarcado, o que torna interessante você aprender a conectar o Bluetooth e o Arduino a esses aparelhos e controlar os seus projetos remotamente.

Hoje, uma parte da área de segurança de sistemas está relacionada a crimes e ataques cibernéticos. Assim, torna-se necessário o conhecimento sobre a estrutura da tecnologia empregada, para que se conheçam os possíveis pontos de invasão e as situações de vulnerabilidade. Ainda, deve-se compreender como a arquitetura de segurança para Internet of Things (IoT, também conhecida como Internet das Coisas) atua para proteger as informações.

Neste tópico, você vai estudar as características da comunicação Bluetooth, além de ver alguns componentes e dispositivos que propiciam a comunicação do Arduino com outros dispositivos por meio do Bluetooth. Por fim, vai ver alguns projetos que utilizam o Bluetooth e o Arduino.

Você também vai estudar neste tópico, os princípios de segurança de redes sem fio para IoT e vai compreender os principais desafios da IoT em relação à vulnerabilidades.

2 COMUNICAÇÃO VIA BLUETOOTH

O Bluetooth, segundo Harte (2009), é um padrão de comunicação sem fio (wireless) desenvolvido para fornecer conexão entre dispositivos como telefones celulares, tablets, notebooks, impressoras, câmeras digitais, consoles de videogames etc. O padrão, atualmente utilizado mundialmente, foi criado no final dos anos 1990, pelo grupo Bluetooth SIG (Bluetooth Special Interest Group) formado pelas empresas Ericson, Intel, IBM, Toshiba e Nokia. O Bluetooth é uma

especificação para personal area network (PAN), também conhecido como IEEE 802.15.1 (HEYDON, 2012).

O Bluetooth foi desenvolvido para ser uma solução wireless de especificação aberta, capaz de transmitir voz e dados por pequenas distâncias (de 1 a 100 metros). Assim, ele elimina a necessidade de cabos e fios para conectar os dispositivos fixos e/ou móveis, transmitindo as informações através de redes ad hoc e fornecendo a sincronização automática entre os equipamentos pareados (HARTE, 2009).

A conectividade dos equipamentos, que são embarcados com a tecnologia Bluetooth, é possível por meio de um chip que funciona como um rádio transceptor operando na frequência de 2.4 GHz, que opera na faixa ISM (industrial, scientific, medical) em sua camada física de rádio (HUANG, 2007). A classificação dos dispositivos Bluetooth é feita em classes, de acordo com o alcance e a potência máxima permitida, conforme você pode visualizar no Quadro 4.

QUADRO 4 – CARACTERÍSTICAS DAS CLASSES DO PADRÃO BLUETOOTH

	Potência máxima permitida	Alcance
Classe 1	100 mW (20 dBm)	até 100 metros
Classe 2	2.5 mW (4 dBm)	até 10 metros
Classe 3	1 mW (0 dBm)	aprox. 1 metro

FONTE: Adaptado de HC (2010)

Há também outras classes, mas são muito raras, por isso não veremos elas aqui.

Todas as especificações e características do padrão Bluetooth são regulamentadas pelo grupo Bluetooth SIG, que, em 2018, contava com mais de 30.000 empresas associadas por todo o mundo. Uma especificação importante regulada pelo grupo é o controle de versão/modelos do Bluetooth. Até 2019, há 11 versões disponíveis para o padrão Bluetooth (IEEE, 2002).

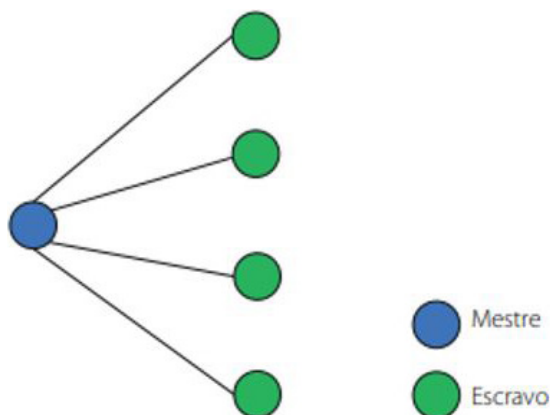
FIGURA 3 – VERSÕES DO PADRÃO BLUETOOTH

Versão	Descrição
Bluetooth 1.0 e 1.0B	As primeiras versões oficiais apresentaram muitos problemas, como velocidade baixa, pouca segurança, interoperabilidade entre equipamentos de fabricantes diferentes e impossibilidade de manter o anonimato nas transmissões.
Bluetooth 1.1	Lançada em 2002, esta versão apresentou a correção de muitos problemas apresentados na versão 1.0B. Incluiu suporte a canais não encriptados e indicador de sinal recebido (RSSI).
Bluetooth 1.2	Nesta versão foram implementadas algumas melhorias, entre elas busca e conexão mais rápida entre os dispositivos, pulso de frequência adaptável, resistência na frequência de rádio para evitar interferências, transmissões de dados mais rápidas (até 1 Mbps) e aumento da qualidade das conexões de voz e áudio.
Bluetooth 2.0 + EDR	Introduziu maior velocidade de transmissão dos dados (até 3 Mbps), devido à inclusão da característica <i>enhanced data rate</i> (EDR).
Bluetooth 2.1 + EDR	Adotada em 2007, trouxe melhorias no pareamento dos dispositivos Bluetooth, no desempenho (inclusão do e BER, <i>bit error rate</i>) e na segurança da transmissão dos dados e no consumo de bateria.
Bluetooth 3.0 + HS	Adotada em 2009, teve como característica importante a velocidade de transferência de dados em <i>high speed</i> (HS) com taxas de até 24 Mbps, além de a transmissão de dados ser realizada por meio do protocolo 802.11 da IEEE.
Bluetooth 4.0	Adotada em 2010, apresentou três protocolos: o Bluetooth clássico, o Bluetooth de alta velocidade e o Bluetooth de baixo consumo.
Bluetooth 4.1	Anunciada em 2013, trouxe uma atualização de <i>software</i> que adicionou novos recursos para melhorar a usabilidade do usuário.
Bluetooth 4.2	Lançado em 2014, introduziu características de Internet das Coisas (IOT, <i>Internet of Things</i>), como baixo consumo de energia, conexão segura, extensão do pacote de dados e inclusão da versão 6 do <i>Internet Protocol Support Profile</i> (IPSP).
Bluetooth 5.0	Adotada em 2016, esta versão trouxe a inclusão de novas características focadas na tecnologia emergente da IOT.
Bluetooth 5.1	Adotada em 2019, trouxe melhorias em diversas áreas, como Ângulo de chegada (AoA) e Ângulo de partida (AoD), que são usados para a localização e o rastreamento de dispositivos; suporte a HCI para chaves de <i>debug</i> em conexões seguras; hierarquia baseada em malha; entre outras.

FONTE: Adaptado de IEEE... (2002)

De acordo com Heydon (2012), a comunicação entre equipamentos Bluetooth é bidirecional, podendo ser ponto a ponto ou ponto a multiponto. No primeiro tipo, a conexão é estabelecida entre dois dispositivos, enquanto, no segundo, pode haver até 8 dispositivos. A comunicação é realizada por meio do compartilhamento do canal físico, denominado piconet. Nesse canal, um dispositivo tem o papel de mestre e os outros de escravos, conforme você pode visualizar no esquema a seguir. Ainda segundo Heydon (2012), uma vez que os dispositivos foram previamente pareados, eles podem se comunicar sempre que um estiver ao alcance do outro, pois o sincronismo da reconexão é realizado automaticamente.

FIGURA 35 – PICONET COM UM DISPOSITIVO MESTRE E QUATRO ESCRAVOS

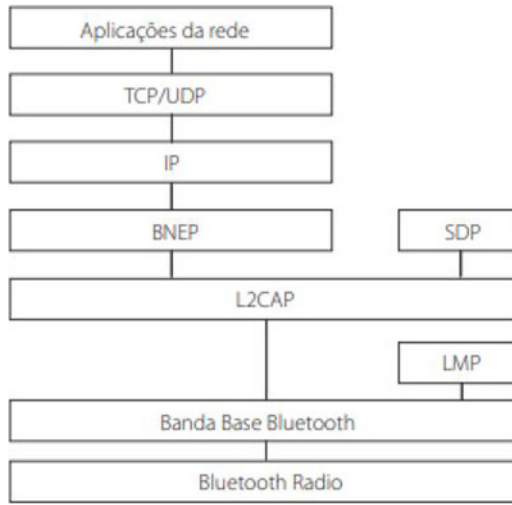


FONTE: Os autores

A comunicação Bluetooth funciona com uma arquitetura de camadas, que é dividida em enlace lógico e comunicação lógica. Ela também tem vários protocolos, que permitem a transmissão e o controle do pacote de dados (HUANG, 2007). Entre os protocolos, os mais importantes são os seguintes.

- **L2CAP:** é responsável pelo fornecimento de serviços orientados e não orientados à conexão para as camadas superiores, além de permitir aos protocolos de maior nível transmitir e receber pacotes de dados L2CAP acima dos 64 KB Bluetooth.
- **BNP:** pacote baseado no EthernetII/DIX Bluetooth, que define um formato de pacotes comum aos dispositivos.

FIGURA 36 – ESTRUTURA DE CAMADAS DA COMUNICAÇÃO BLUETOOTH



FONTE: Os autores

3 COMPONENTES ELETRÔNICOS PARA A TROCA DE DADOS DO ARDUINO VIA BLUETOOTH

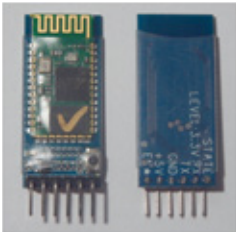
O padrão Bluetooth é uma das comunicações sem fio mais utilizadas para a transmissão e a recepção de dados com o Arduino (McROBERTS, 2011). Isso se deve à simplicidade de configuração e programação e à facilidade de encontrar módulos para comprar no mercado. Os módulos mais populares, atualmente, são os da série HC, particularmente o HC-05 e o HC-06. A diferença mais importante entre esses dois modelos é que o HC-05 pode exercer o papel de mestre ou escravo em uma conexão, enquanto o HC-06, apenas o papel de escravo. Por esse motivo, vamos estudar em mais detalhes o módulo HC-05.

3.1 MÓDULO BLUETOOTH HC-05

O Bluetooth HC-05 utiliza o protocolo serial Bluetooth (Bluetooth SPP, Serial Port Protocol), que é composto de uma interface serial e de um adaptador Bluetooth em um único módulo (HC, 2010). O HC-05 fornece uma interface simples para a conexão com o microcontrolador e uma fácil configuração do dispositivo, além de ser uma solução barata para realizar a troca de informações/dados sem fio com o microcontrolador no seu projeto.

Todo componente eletrônico tem especificações técnicas e elétricas próprias, então, é importante conhecer essas características do dispositivo para utilizá-lo de forma correta e obter funcionamento adequado do mesmo (HC..., 2010). O Quadro 3 mostra algumas dessas características técnicas e elétricas do módulo Bluetooth HC-05.

FIGURA 37 – MÓDULO HC - 05



FONTE: Os autores

TABELA 4 – CARACTERÍSTICAS TÉCNICAS E ELÉTRICAS DO BLUETOOTH HC-05

Características	Descrição
Protocolo	Bluetooth 2.0 + EDR
Frequência	2,4 GHz Banda ISM
Modulação	GFSK
Emissão de energia	< / = 4 dBm, classe 2
Sensibilidade	< / = 84 dBm com 0,1% BER
Velocidade assíncrono	2,1 Mbps (máx.)/160 Kbps
Velocidade síncrono	1 Mbps/1 Mbps
Segurança	Autenticação e encriptação
Tipo de comunicação	Serial Bluetooth
Modo de operação	Mestre ou escravo
Tensão	3,3V (podendo variar entre 2,7V e 4.2V)
Corrente	Durante o pareamento 35 mA; quando conectado, 8 mA
Alcance	10 metros
Taxa de transmissão (bps)	4.800, 9.600, 19.200, 38.400, 57.600, 115.200, 230.400, 460.800, 921.600, 1.382.400
Dimensões	26,9 × 13 × 2,2 mm
Peso	9,6 g

FONTE: Adaptado de HC (2010)

Entre as especificações do Tabela 4, é importante você estar atento às seguintes, pois exercem grande influência no desenvolvimento do seu projeto:

- o protocolo de comunicação Bluetooth 2.0;
- a frequência de 2,4 GHz ISM;
- o tipo de comunicação serial;
- o fato de que pode operar como mestre ou escravo;

- a faixa de tensão;
- o consumo de corrente;
- o alcance de 10 metros;
- a taxa de transmissão.

Segundo do manual HC Serial Bluetooth Products (HC, 2010), o módulo HC-05 tem seis conectores, que você pode visualizar mais adiante. Cada um desses conectores tem uma função específica. Veja a seguir.

- **STATE**: está ligado ao LED interno do módulo e fornece um feedback para verificar se o Bluetooth está funcionando corretamente.
- **RXD**: receptor de dados Serial.
- **TXD**: transmissor de dados Serial.
- **GND**: terra.
- **VCC**: tem alimentação positiva 3,3V, mas esse módulo suporta 5V.
- **KEY/ENABLE**: este pino é usado para trocar o estado de funcionamento entre o modo de transferência de dados ou comandos AT.



Se você quiser saber mais sobre o módulo Bluetooth HC-05, acesse dois links interessantes com outras informações relevantes sobre o dispositivo.

Instruções para o usuário HC-05: <https://goo.gl/XUQ2MR>

Datasheet HC-05: <https://goo.gl/1vwojT>

3.2 CONEXÃO DO MÓDULO BLUETOOTH HC-05 AO ARDUINO

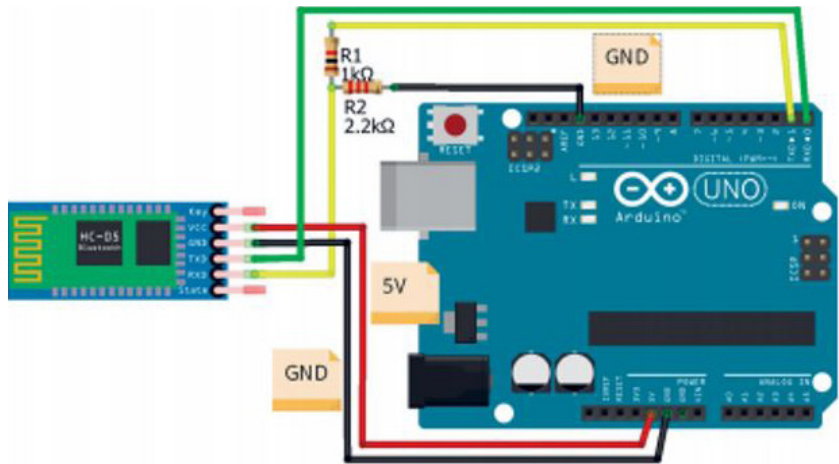
Segundo Monk (2014), os componentes mínimos necessários para montar um circuito de comunicação com o Arduino via Bluetooth são:

- uma placa Arduino UNO;
- um módulo HC-05;
- um resistor de 1k Ω ;
- um resistor de 2k Ω .

A Figura 39 mostra a montagem do circuito mais simples que você pode montar entre o Bluetooth e o Arduino. Duas observações são importantes nesse circuito: a primeira é o divisor de tensão (dois resistores) ligado no conector RX do HC-05 — isso é necessário para evitar qualquer dano no seu módulo Bluetooth, pois a tensão de saída do pino do Arduino é 5V e a tensão de operação do HC-

05 é de 3,3V (podendo trabalhar na faixa entre 2,7V e 4.2V). A segunda é que o conector RX do HC-05 está ligado ao pino TX do Arduino e o conector TX do HC-05 está ligado ao pino RX do Arduino, assim, o dado transmitido pelo pino TX do Arduino será recebido na entrada de dados RX do HC-05 e o dado enviado pelo conector TX do HC-05 será recebido pelo pino de entrada de dados RX do Arduino (MONK, 2014).

FIGURA 42 – CIRCUITO BLUETOOTH E ARDUINO



FONTE: Os autores



Se você pesquisar na internet, poderá encontrar muitas montagens do circuito ligando o pino do Arduino diretamente ao conector RX do módulo HC-05, sem passar pelo divisor de tensão. Essa ligação direta irá funcionar, no entanto não é indicada para montagens permanentes, pois pode diminuir a vida útil do seu módulo.

3.3 PROGRAMAÇÃO DO MÓDULO BLUETOOTH HC-05 LIGADO AO ARDUINO

O código do sketch para o funcionamento do circuito Bluetooth como escravo, ligado à plataforma microcontrolada Arduino, não é tão complexo. De acordo com Monk (2014), basicamente, você precisa configurar a taxa de transmissão da comunicação serial, aguardar o recebimento de um dado, processar esse dado e enviar uma resposta ao dispositivo mestre. Aqui, veremos somente a comunicação serial necessária para utilizar o módulo Bluetooth.

FIGURA 40 – CÓDIGO PARA O FUNCIONAMENTO DO MÓDULO BLUETOOTH E O ARDUINO

```

1  /*****
2  Programa: Envio e recepção de dados no Arduino via Bluetooth
3  *****/
4
5  #define LED_PINO 13 //Cria uma Macro para o pino 13
6
7  /* Função: void setup()
8   * Descrição: Contém as configurações do hardware
9   *             utilizado no programa.
10  */
11 void setup(){
12     // Pino do pino 13 como saída digital
13     pinMode (LED_PINO, OUTPUT);
14     //Inicializa a comunicação Serial (taxa de transmissão 9600bps)
15     Serial.begin (9600);
16     //Espera um terminal de comunicação serial conectar a módulo
17     while (!Serial);
18     //Mensagem inicial enviada do Arduino para o dispositivo conectado
19     Serial.println ("Conectado OK!");
20 }//Fim da função void setup()
21
22 /* Função: void loop()
23  * Descrição: Contém a lógica principal do código.
24  */
25 void loop(){
26     //Verifica se existe dados disponível no buffer da serial
27     if (Serial.available() > 0) { ...
28         //Lê o valor recebido no Arduino pela comunicação serial
29         int valor_recebido = Serial.read();
30         //Testa se o valor recebido é L ou l (Ligar)
31         if (valor_recebido == 'L' || valor_recebido == 'l') {
32             //Liga o LED interno da placa do Arduino
33             digitalWrite (LED_PINO, HIGH);
34             //Envia a mensagem do estado do LED ao dispositivo conectado
35             Serial.println ("Estado do LED Ligado!");
36         }//Fim do if (valor_recebido == 'L' || valor_recebido == 'l')
37
38         //Testa se o valor recebido é D ou d (Desligar)
39         if (valor_recebido == 'D' || valor_recebido == 'd') {
40             //Desliga o LED interno da placa do Arduino
41             digitalWrite (LED_PINO, LOW);
42             //Envia a mensagem do estado do LED ao dispositivo conectado
43             Serial.println ("Estado do LED Desligado!");
44         }//Fim do if (valor_recebido == 'D' || valor_recebido == 'd')
45     }//Fim do if (Serial.available())
46 }//Fim da função void loop()

```

FONTE: Os autores

No código apresentado, o Arduino aguarda receber a letra L, maiúscula ou minúscula, para ligar o LED interno da placa conectado ao pino 13 (padrão de todas as placas do Arduino), ou a letra D, maiúscula ou minúscula, para desligar o LED interno da placa. Qualquer outro valor enviado pelo dispositivo que estabeleceu a conexão será ignorado e descartado.

De acordo com Margolis (2012) e Banzi e Shiloh (2015), o comando **Serial.begin (9600)** seta a taxa de transmissão em bit por segundo da comunicação serial. Os valores de taxas disponíveis são 300, 600, 1.200, 2.400, 4.800, 9.600, 14.400, 19.200, 28.800, 38.400, 57.600 ou 115.200.

O comando **Serial** indica se a porta serial está pronta para comunicar. Retorna: True (Comunicação disponível) ou False (Comunicação indisponível).

O comando **while(!Serial)** trava o código enquanto uma conexão serial não estiver disponível. Quando uma comunicação serial é aberta — por exemplo, o monitor serial da IDE do Arduino —, o código segue a execução normalmente (MARGOLIS, 2012; BANZI; SHILOH, 2015).

O comando **available()** retorna o número de bytes (caracteres) disponível para ser lido pela porta serial. Sintaxe: **Serial.available()**.

O comando **Serial.read()** lê um dado serial (MARGOLIS, 2012; BANZI; SHILOH, 2015). Retorno da sintaxe **Serial.read()**: o primeiro byte no buffer da serial (formato int).

O comando **Serial.print()** tem a seguinte sintaxe:

- **Serial.print(valor);**
- **Serial.print(valor, formato).**

Esse comando imprime um dado na serial, onde **valor** é valor a ser impresso, qualquer dado — string, caractere, variável etc. Já **formato** especifica a base numérica ou o número de casas decimais. Base numérica: DEC (Decimal), BIN (Binário), OCT (Octal) e HEX (Hexadecimal); 0, 1, 2...: zeros, casas decimais, uma casa decimal, duas casas decimais (MARGOLIS, 2012; BANZI; SHILOH, 2015).

O comando **Serial.println()** tem a seguinte sintaxe:

- **Serial.println(valor);**
- **Serial.println(valor, formato).**

Esse comando imprime um dado na serial e quebra uma linha, onde **valor** e **formato** têm as mesmas especificações do comando anterior **print** (MARGOLIS, 2012; BANZI; SHILOH, 2015).

3.4 CONEXÃO ENTRE O ARDUINO E O CELULAR

Para conectar o circuito Bluetooth ligado no Arduino ao seu celular/tablet com sistema operacional Android (O sistema iOS possui algumas restrições de conexão e troca de dados via Bluetooth, por será abordado apenas o sistema Android nesse material), primeiramente você deverá parear o módulo Bluetooth ao seu telefone (MONK, 2014). Para isso, siga os passos a seguir.

1. Ligue a placa Arduino no seu computador para energizá-la e ligar o módulo Bluetooth.
2. Habilite a conexão Bluetooth do seu aparelho celular.
3. Aguarde o celular procurar por dispositivos Bluetooth disponíveis nas proximidades. Caso o celular atualize a lista, faça a busca manualmente.
4. Procure o dispositivo com o nome HC-05 ou linvor (vai depender do modelo que você tem) e escolha “conectar” para fazer o pareamento.
5. No campo senha digite 1234 (alguns podem vir de fábrica com o código 0000, mas é muito raro de acontecer).
6. Pronto, seu celular já está pareado com o circuito Bluetooth.



O sistema iOS tem algumas restrições de conexão e troca de dados via Bluetooth, por isso é abordado apenas o sistema Android neste material.

É necessário fazer esse pareamento entre o celular/tablet e o módulo Bluetooth apenas uma vez, mas caso você remova o pareamento manualmente, terá que refazer os passos novamente (MONK, 2014). Agora, para enviar e receber dados do seu Celular para o Arduino e vice-versa, você precisará seguir os passos a seguir.

1. Faça o download do aplicativo S2 Bluetooth Terminal Free na loja de aplicativos da Google.
2. Clique no botão “conectar” e selecione o dispositivo Bluetooth que foi pareado anteriormente (HC-05 ou linvor).
3. Pronto, você já está pronto para receber e enviar mensagens para o seu Arduino.
4. Teste enviar o valor L e depois D.

4 APLICAÇÕES DA COMUNICAÇÃO BLUETOOTH COM ARDUINO

A comunicação Bluetooth utilizando a plataforma microcontrolada Arduino pode ser aplicada em diversos projetos que necessitam de uma comunicação sem fio em distâncias pequenas. Na internet, você encontra diversos projetos que utilizam a comunicação Bluetooth e o Arduino para fazer medições de sensores, acionamento de atuadores, controle de dispositivos remotamente, entre outros. Vamos analisar o projeto de Domótica que pode desenvolvido utilizando essa tecnologia de comunicação wireless.

4.1 AUTOMAÇÃO RESIDENCIAL (DOMÓTICA)

De acordo com Monk (2014), a automação residencial, conhecida também como domótica, pode ser utilizada para controlar remotamente diversos equipamentos na sua casa, como as tomadas para ligar e desligar aparelhos, o sistema de climatização do ambiente e, até mesmo, a fechadura da sua porta da frente ou do seu quarto.

As placas do Arduino podem fazer esse tipo de automação de uma residência, esteja conectado ou não a um computador. Às vezes, a presença de um computador é necessária no caso de você querer implementar uma interface

gráfica mais elaborada para gerenciar os equipamentos automatizados, mas, se quiser apenas controlar remotamente o acionamento dos dispositivos, um aplicativo no celular ou tablet é mais do que suficiente (MONK, 2014).

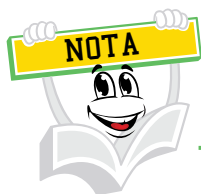
Suponha que você queira acionar uma lâmpada na sua casa. Você precisará, além da placa Arduino, alguns componentes eletrônicos como, por exemplo, o módulo Bluetooth (para a conexão com o celular ou tablet) e um módulo relé 5V (para o acionamento da lâmpada ligada na energia elétrica da sua casa).

5 OS DESAFIOS DA ÁREA DE SEGURANÇA EM REDES SEM FIO PARA A IoT

A IoT é uma evolução da internet que possibilita à infraestrutura de rede conectar um grande número de dispositivos e permitir que eles colem dados e se comuniquem para realizar processos e tomadas de decisões inteligentes. Vale lembrar que esses dispositivos são qualquer objeto incorporado ao hardware e software necessários para suportar o processamento e os recursos da rede. A IoT fornece às empresas aplicativos (software) para serem usados para controlar esses dispositivos e criar modelos de negócios eficientes e com boa relação custo-benefício.

A tecnologia pode ser vista como uma facilitadora na nossa sociedade superconectada e pode ser utilizada para otimizar alguns serviços do nosso dia a dia, como já ocorre nas áreas de transportes e mobilidade, alimentação e educação. No entanto, essas facilidades reportam muitos desafios na área de segurança da informação, que precisam ser enfrentados para melhorar o uso dos diversos recursos tecnológicos disponíveis (ALHALAFI; VEERARAGHAVAN, 2019). De fato, sem uma clara abordagem dos desafios colocados pelas questões de segurança e privacidade relacionados à IoT e das possíveis soluções para os problemas, o sucesso da tecnologia e a privacidade dos usuários enfrentam riscos significativos.

A segurança da IoT (IoT security) é a área de atuação relacionada à proteção dos dispositivos e das redes conectadas à IoT. Essa área envolve a crescente prevalência de objetos e aparelhos com identificadores exclusivos e a capacidade de transferir dados automaticamente por meio de uma rede. Grande parte do aumento na comunicação em redes IoT se deve ao uso crescente de dispositivos de computação e sistemas de sensores embarcados usados na comunicação M2M (machine to machine), como redes inteligentes de energia, automação residencial e predial, veículos, entre outros.



O conceito de M2M representa duas máquinas se comunicando e se refere às tecnologias que permitem que sistemas com fio e sem fio se comuniquem com outros dispositivos que possuem a mesma habilidade, sem intervenção ou interação humana (PERSIA; REA, 2016).

A IoT conta, na prática, com uma gama extensa de redes interconectadas por dispositivos que possuem recursos limitados. Como esses dispositivos têm essa característica, eles não podem usar conjuntos de segurança complexos usados em redes típicas. Isso representa um grande desafio, pois se faz necessário projetar uma estrutura de segurança exclusiva ou usar as soluções existentes. Devem ser feitos esforços para garantir que soluções de segurança simples sejam implementadas, de modo que os recursos dos dispositivos não sejam esgotados em segurança em detrimento do desempenho.

Dentre os desafios de segurança e privacidade associados à IoT está a dificuldade de se estabelecer uma comunicação segura. Isso ocorre porque a tecnologia compreende diferentes componentes e dispositivos, tornando difícil garantir que todos os componentes se comuniquem com segurança. Existem também algumas preocupações de sigilo e confidencialidade de dados associados à IoT. Por exemplo, a tecnologia envolve a interconexão de várias redes, e, em alguns casos, o usuário pode não estar no controle da rede, o que pode acarretar a exposição dos dados a ameaças de sigilo e confidencialidade. Além disso, como a IoT envolve muitos dispositivos e redes, torna-se difícil identificar, avaliar e monitorar componentes importantes, para garantir a conformidade com as políticas de segurança.

Por fim, é um desafio garantir um nível adequado de troca segura de informações e confiança entre diferentes infraestruturas verticais de tecnologia da informação (TI). O principal problema é que, como a ideia de dispositivos de rede e outros objetos é relativamente nova, a segurança nem sempre foi considerada na construção dos objetos. Objetos para IoT geralmente são vendidos com sistemas operacionais e software desatualizados. Além disso, os usuários pecam ao não alterarem as senhas padrão dos dispositivos inteligentes, ou, se alteram, não seguem as recomendações para a criação de senhas mais seguras. Para melhorar a segurança, um dispositivo IoT que precise estar diretamente acessível pela internet deve ser segmentado em sua própria rede e ter acesso restrito. O segmento de rede deve ser monitorado para identificar tráfego perigoso em potencial, e ações devem ser tomadas se houver algum problema.

A seguir, são descritos os principais desafios da IoT em relação à segurança e à privacidade.

5.1 CONFIDENCIALIDADE E ACESSO

Existem várias tecnologias principais que oferecem suporte a redes IoT. Dentre elas, destacam-se a identificação por radiofrequência (RFID, do inglês radio frequency identification), a comunicação por campo próximo (NFC, do inglês near field communication) e as redes de sensores sem fio (WSN, do inglês wireless sensor network).

A tecnologia RFID suporta redes IoT, garantindo que os dispositivos sejam equipados com marcadores e etiquetas inteligentes, que os tornam gerenciáveis. Além disso, a tecnologia RFID permite que esses objetos da IoT tenham chips inteligentes, que dão a eles a capacidade de detectar informações em seu ambiente, calcular e se comunicar com outros objetos ou seres humanos. O componente RFID é, no entanto, propenso a ataques de negação de serviços, interceptação, desvio de acesso e retransmissão, que podem comprometer a segurança e a privacidade dos usuários dentro do ambiente da IoT.

As WSNs geralmente são usadas para oferecer suporte a aplicativos de sensoriamento remoto e coleta de informações em redes IoT. Elas são preferidas em tais aplicações, porque são econômicas, eficientes, consomem pouca energia e possuem recursos inteligentes de processamento. Já a NFC é a tecnologia que suporta a comunicação a pequena distância, com baixo consumo de energia e taxa de dados, como a comunicação de cartões inteligentes (cartões do tipo contactless) e controle de acesso. É uma tecnologia propensa a ataques do tipo phishing, rastreamento de usuário, retransmissão e falsificação de dados (BURHAN et al., 2018).



A RFID é uma tecnologia que usa campos eletromagnéticos para identificar objetos. Uma etiqueta RFID é composta por um pequeno rádio transponder, formado por um transmissor e um receptor. Por muitos anos, essa tecnologia foi considerada uma das 10 maiores contribuições tecnológicas do século XXI.

5.2 CIBERSEGURANÇA (CYBERSECURITY)

Com relação à IoT, os problemas de cibersegurança giram em torno de confidencialidade, autenticação e acesso. Nesse caso, a confidencialidade se refere à necessidade de garantir que os dados sejam mantidos em sigilo, apenas com os usuários autorizados a acessar os dados. Na IoT, a criptografia surge como a tecnologia mais importante para garantir a confidencialidade. Por sua vez, a autenticação se refere à verificação dos dados, para garantir que não houve violação

e que as informações foram entregues pelo suposto remetente ou autor. Já o acesso se refere a garantir que apenas usuários autorizados possam recuperar ou acessar a infraestrutura, as comunicações e as informações, garantindo que os usuários autorizados não sejam impedidos de adquirir os dados (ALBISHI *et al.*, 2017).

5.3 SEGURANÇA E PRIVACIDADE

Em IoT, cada dispositivo poderá ser uma potencial porta de entrada à infraestrutura ou aos dados pessoais (TRYFONAS; LI, 2016). As preocupações com segurança e privacidade de dados são muito importantes, mas os riscos potenciais associados à IoT atingem novos níveis com a interoperabilidade, quando a tomada de decisões autônomas começa a incorporar complexidade, originando brechas de segurança e vulnerabilidade em potencial. Riscos surgirão, porque a complexidade pode criar mais vulnerabilidades do que as relacionadas aos serviços.

Na IoT, as informações abrangem dados pessoais, como data de nascimento, localização, endereço e formas de pagamento. Esse é um dos desafios das tecnologias de big data, e as profissões relacionadas à segurança precisam garantir que os riscos potenciais à privacidade associados ao conjunto de dados serão considerados. A IoT deve ser implementada de maneira legal, ética, social e politicamente aceitável, e desafios legais, sistemáticos, técnicos e de negócios devem ser considerados.

5.4 IDENTIFICAÇÃO, LOCALIZAÇÃO E RASTREAMENTO

Os recursos e tecnologias em evolução da IoT, juntamente com a interação com os sistemas emergentes, levaram a desafios específicos de privacidade e segurança. Um dos desafios da IoT está relacionado ao risco de se associar um identificador a um endereço, abrangendo dados individuais e relacionados de um usuário. Nesse caso, o principal risco está relacionado à associação da identidade a um contexto específico, que viola a privacidade do indivíduo, fornecendo identificação e informações para entidades fora da esfera pessoal do usuário, aumentando o número de possíveis ciberataques.

Outro desafio de privacidade e segurança vinculado à IoT está relacionado à localização e ao rastreamento. Nesse caso, a ameaça está relacionada à determinação e ao registro da localização do indivíduo em espaço e tempo. Embora a localização e o rastreamento já sejam possíveis por vários meios, como o tráfego da internet e o GPS dos aparelhos celulares, muitos usuários podem considerá-los uma violação da privacidade, se os dados são usados de forma inadequada ou se não há nenhum controle sobre o compartilhamento destes. Assim, a IoT enfrenta o desafio de garantir a conscientização sobre o rastreamento e o controle dos dados de localização (TRYFONAS; LI, 2016).

5.5 CRIAÇÃO DE PERFIL (PROFILING) E AUTENTICAÇÃO

A IoT também apresenta desafios significativos com relação à privacidade e à segurança na criação de perfis, bem como na apresentação de dados que violem a privacidade. Em relação ao perfil, a IoT enfrenta um risco na compilação de dados sobre os usuários, a fim de determinar seus interesses por meio da correlação com outras fontes de dados. Os métodos de criação de perfil podem ser usados no comércio eletrônico para a personalização do consumidor, bem como para segmentação e otimização internas, com base nos interesses e acessos dos clientes. No entanto, a criação de perfil pode levar a violações da privacidade, se os dados forem usados para anúncios não solicitados, discriminação de preços e engenharia social. A coleta e venda de perfis de usuários no mercado de dados sem o consentimento do indivíduo também é considerada uma violação de privacidade.

Outro desafio encarado pela IoT é o fato de informações particulares poderem ser transportadas inadvertidamente pela mídia pública, de forma a serem divulgadas para pessoas indesejadas. Várias aplicações usadas em redes da IoT, como assistência médica, transporte e varejo, dependem de interações significativas do usuário (TRYFONAS; LI, 2016).

5.6 ATAQUES A BANCOS DE DADOS E INVENTÁRIOS

Os dispositivos inteligentes interagem com inúmeros serviços e pessoas e acumulam dados sobre essas interações em seu histórico. Considerando que o ciclo de vida da maioria dos bens de consumo é baseado no cliente que possui o produto, a venda ou o compartilhamento de tais dispositivos pode resultar no acesso a dados confidenciais sobre o proprietário anterior, violando a privacidade do indivíduo.

A IoT é desafiada em situações de ameaça de ataques a bancos de dados ou inventários. Como as capacidades de interconexão da IoT com o desenvolvimento da tecnologia M2M evoluíram muito nos últimos anos, os dispositivos inteligentes podem ser consultados pela internet tanto por usuários legítimos quanto por falsos usuários do sistema. Quando um sistema IoT é consultado pelos falsos usuários, eles podem explorar os dispositivos, para coletar informações não autorizadas. Assim, a IoT pode permitir a divulgação de dados abrangentes sobre a vida e a rotina dos usuários, ameaçando sua segurança e privacidade (ALHALAFI; VEERARAGHAVAN, 2019).

LEITURA COMPLEMENTAR

Talvez o termo “domótica”, ou casas inteligentes, não seja mais uma realidade tão distante. Saiba como transformar sua casa em uma casa inteligente.

Casas inteligentes: afinal de contas, a revolução digital fora implacável ao transformar o cotidiano das pessoas com os smartphones.



A vida nos tempos atuais é uma constante oportunidade para a admiração. Afinal de contas, a **revolução digital** fora implacável ao transformar o cotidiano das pessoas com os *smartphones*. E se disséssemos que o futuro reserva uma integração ainda maior entre os indivíduos e suas residências?

Pois bem, isso acontecerá devido à popularização da **casa inteligente**!

Apesar de soar como algo que tenha saído da ficção científica, trata-se de uma tendência que veio para ficar. Como é natural a qualquer novidade no mercado, ainda existem dúvidas pairando sobre a cabeça dos consumidores. Para respondê-las, desenvolvemos este artigo, esclarecendo todas as curiosidades e soluções do **futuro imobiliário**. Sem mais demoras, acompanhe!

O conceito da casa inteligente

Para a grande maioria das pessoas, as casas são seus templos particulares, recantos repletos de conforto e calma. Um porto seguro isento das preocupações do caótico mundo moderno. Portanto, o conceito por trás das **casas inteligentes** é tornar os lares ainda mais compreensivos e acolhedores para aqueles que ali descansam.

No entanto, afinal de contas: como é possível tornar uma **casa compreensiva**? Aqui entram as **inúmeras inovações tecnológicas**, que utilizam de uma variedade de sensores e estatísticas para aperfeiçoar a experiência com o seu lar. Essa descrição pode até parecer abstrata, mas é a realidade: um futuro em que as casas sabem quando seus proprietários chegam, bem como a temperatura, a iluminação e a melodia com que gostariam de ser recebidos.

Por essa razão, a **automação residencial** foca em três pilares essenciais, aumentando o **controle, a segurança e o conforto** dos residentes. A seguir, você entenderá um pouco mais sobre cada um desses fundamentos. Veja!

Controle

Uma característica básica da **casa inteligente** é a existência de um **painel de controle**, em que seja possível gerenciar a maioria dos aspectos dessa residência. Essa centralização tem a intenção de substituir todos os controles remotos específicos, unificando os comandos em apenas um aplicativo, disponível no **smartphone do proprietário**, por exemplo.



Atualmente, o mercado já conta com uma ampla gama de produtos, que podem ser controlados remotamente por **conexão bluetooth**. Você já imaginou controlar TV, home theater, persianas, geladeira, lava-louças, portões, lâmpadas, climatização e muito mais, apenas com um *app*?

Pois bem, isso já é possível! Basta que o proprietário invista em produtos com boa conectividade entre si. Uma excelente opção centralizadora está presente em um **aplicativo nativo dos** dispositivos Apple, o Casa. Para garantir seu funcionamento, será necessário adquirir produtos que tenham o selo “Works with Apple HomeKit”, apontando compatibilidade.

Essa é uma solução completa para **controlar a sua casa**, permitindo criar diferentes configurações para cada um dos cômodos. Além disso, você ainda poderá criar cenários, que são conjuntos de especificações para determinados momento do dia.

Como exemplo, o cenário “Bom Dia” que pode abrir as persianas, preparar o café e ligar a TV no canal de notícias. Já um cenário como “Estou em Casa” pode iluminar o corredor, climatizar a sala e trancar as portas. Tudo depende da personalização elaborada pelo morador.

Segurança

O segundo ponto basilar das **casas inteligentes** é representado pela segurança aprimorada. Todos conhecemos as soluções tradicionais para incrementar a proteção das residências: grades, **cercas elétricas**, câmeras e afins. A segurança também passou por evoluções com a automação residencial.



Um primeiro exemplo: as câmeras. Até recentemente, esses dispositivos realizavam apenas captações de baixa resolução, com difícil acesso a essas filmagens. Hoje em dia, pode-se **adquirir câmeras discretas**, funcionais e com muita **tecnologia embarcada**, **monitorando setores da casa** com ângulos de 180 até 360 graus, em *Full HD* e em tempo real. Tudo por meio de um aplicativo, de onde quer que esteja.

Além dessas câmeras, também existem as fechaduras eletrônicas, acessadas com senhas numéricas PIN, impressão digital, **reconhecimento facial** ou cartão magnético. Perceba que as **soluções que descartam as chaves**, sejam físicas ou virtuais, também eliminam o problema do esquecimento, bastando que você utilize o seu dedo, **mão ou rosto para acessar a casa**.

Conforto

Por último, o argumento mais sólido aos consumidores interessados na automação: o aumento da comodidade. A popularização das **casas autônomas** será responsável por residências cada vez mais integradas ao cotidiano de seus residentes, sendo ambientes projetados para atender todas as necessidades do morador, mesmo as mais sutis.

O maior causador de conforto nessas **casas é seu potencial de controle remoto e situacional**. Lembra-se da funcionalidade de cenários, no *app Casa da Apple*? Pois então, considere o quão futurista, bacana e conveniente é poder contar com as seguintes configurações:

- **Cinema**: ligando a TV no *app* da Netflix, configurando o *home theater* ao modo Cinema, fechando as persianas, reduzindo a temperatura ambiente e diminuindo a iluminação para 10%;
- **Jantar Romântico**: ligando o sistema de áudio conectado a um *app* como Spotify, reproduzindo uma playlist pré-selecionada e diminuindo a iluminação para 20%;
- **Festa**: ligando o sistema de áudio conectado a um *app* de música, reproduzindo uma playlist pré-selecionada, intensificando a refrigeração de bebidas na geladeira e abrindo as persianas.

Esse é o principal motivo para as **casas inteligentes** serem um sucesso certo no **futuro imobiliário**, pois elas são completamente personalizáveis de acordo com as vontades do proprietário, impossibilitando a insatisfação.

As melhores formas para investir na automação da casa

O fato mais interessante sobre as **casas inteligentes** é de que elas já são uma possibilidade concreta e comprável. Na realidade, o futuro apenas contribuirá com um cenário em que a maioria da população tenha acesso a essas soluções, que estão começando a emergir no mercado nacional.



Apesar dessa fase inicial, vale dizer que o Brasil já conta com muitas opções no **segmento de automação residencial** que, em sua grande maioria, são importados. No entanto, não há motivo para ser receoso com os custos que, embora mais elevados que as soluções tradicionais, destacam-se por oferecer uma experiência diferente de qualquer outro produto no mercado.

Além disso, as gigantes da eletrônica como a holandesa Philips e a norte-coreana Samsung já mergulharam de cabeça nesse segmento, **inovando em**

iluminação, sonorização, refrigeração e muito mais. Agora, confira as melhores soluções para transformar a sua **residência em uma casa inteligente**.

Câmeras internas e externas

Nossa primeira sugestão prioriza a proteção do imóvel, que é uma preocupação válida, haja vista a situação vulnerável da segurança pública em boa parte do país. Dessa maneira, você poderá “potencializar” a **inteligência da sua casa** ao instalar algumas câmeras por dentro e por fora, podendo visualizar qualquer um dos cômodos monitorados, remotamente, 24 horas por dia.

Entre as câmeras internas pode-se considerar os monitores dos quartos de bebê, ou melhor dizendo, as já famosas **babás eletrônicas**. Inclusive, é possível automatizar esse cômodo em específico, tornando o despertar e o adormecer em momentos mais sutis, reduzindo a insatisfação da criança ao acordar ou sua resistência ao dormir.

Climatização adaptável

Uma **casa não é verdadeiramente inteligente** se ela não consegue interpretar a sensação térmica do momento, não é mesmo? Sendo assim, você poderá investir em um termostato inteligente, capaz de regular e monitorar a temperatura corrente, identificando e aplicando as melhores configurações para a manutenção de um ambiente agradável.



Caso você mesmo decida criar suas condições e cenários, sem problemas, já que esses termostatos também permitem que você **controle os dispositivos de climatização remotamente**, por meio de um **aplicativo mobile**. Naturalmente, as soluções mais sofisticadas apresentarão um custo elevado, mas sempre oferecendo um grau de customização incomparável a qualquer outra alternativa.

Iluminação adaptável

Falaremos de uma solução que é relativamente conhecida ao consumidor nacional. Isso acontece pois já faz bastante tempo que a Philips tenta familiarizar o mercado com suas lâmpadas dinâmicas da linha Hue. Seja dessa marca ou não, todas as **lâmpadas inteligentes** compartilham uma característica importante: a adaptabilidade.



Elas são soluções que permitem alterar a temperatura da sua iluminação. Além disso, podem ser controladas remotamente, com bastante precisão no ajuste da intensidade, não sendo apenas lâmpadas que acendem e apagam. Essas soluções também apresentam bons índices de economia de energia, já que frequentemente são produzidas com tecnologias de baixo consumo, como o LED.

Porteiro digital

Novamente, uma solução que prioriza a **segurança residencial**. O **porteiro eletrônico** nada mais é do que uma campainha inteligente, que permite visualizar quem solicita o acesso à sua casa ou apartamento. Esse dispositivo consegue liberar a entrada apenas com um comando, também por meio de um aplicativo ou de uma central fixada à parede do imóvel.

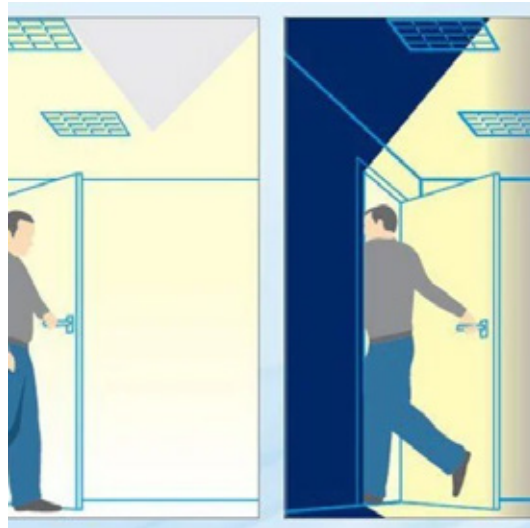
Robô-faxina



Provavelmente você já viu um desses em um dos milhares de vídeos virais que circulam pela internet. Esses robôs são nada mais, nada menos do que **aspiradores de pó inteligentes**, encarregados da limpeza do chão, sem que nenhum esforço seja realizado.

As versões mais novas desse dispositivo já conseguem descartar toda a sujeira coletada no local apropriado, além de se deslocarem sozinhas para sua base de carregamento. Uma vez energizadas, continuam nesse ciclo perpétuo de manter a casa limpa, sem interferências dos moradores.

Sensores de presença



Esses dispositivos são fundamentais na **redução do consumo de energia elétrica em sua casa**. Essa é a solução mais familiar ao consumidor, já que estão presentes na ampla maioria dos prédios condominiais. Trata-se de sensores que captam a movimentação em um ambiente a fim de acender uma luz.

No entanto, os modelos mais sofisticados também realizam a função contrária, monitorando o ambiente para identificar a ausência de pessoas e, assim, **desligar as lâmpadas do cômodo**. Dessa maneira, evita-se o incômodo ocasionado pelos desligamentos temporizados.

Smart Lock

A nossa última sugestão com ênfase na **segurança residencial**: as fechaduras inteligentes. Como apontamos antes, trata-se de dispositivos robustos e capazes de restringir o acesso de qualquer pessoa não autorizada ou devidamente orientada a adentrar no ambiente. Essas fechaduras, inclusive, são utilizadas estrategicamente, na porta principal e nos cômodos mais críticos, ou em todos os ambientes.

No entanto, caso se decida implementar *smart locks* em todos os cômodos da casa, recomenda-se utilizar as opções de **reconhecimento facial** ou **impressão digital**, já que digitar uma senha ou passar um cartão a todo momento que for adentrar em um cômodo pode ser um tanto contra produtivo.



Smart TV

As populares, famosas e queridas *Smart TVs*! Como é bastante natural durante a temporada de eventos esportivos, como a Copa do Mundo ou as Olimpíadas, esses televisores ganharam ainda mais espaço nas salas dos consumidores brasileiros.

As **TVs inteligentes** costumam contar com um sistema operacional dedicado, viabilizando a utilização de aplicativos que ampliam suas funcionalidades. Além disso, essas televisões contam com excelente **conectividade Wi-Fi e Bluetooth**, sendo facilmente controladas por meio do aplicativo desenvolvido pelos seus fabricantes.

Acesse o artigo na íntegra através do link abaixo.

FONTE: <www.chavesnamao.com.br/dicas-e-reformas/casa-inteligente/>. Acesso em: 29 jun. 2020.



RESUMO DO TÓPICO 3

Neste tópico, você aprendeu que:

- A tecnologia Bluetooth é utilizada em projetos para facilitar a transmissão de dados e de voz e para eliminar cabos e fios na conexão entre os dispositivos. Atualmente, diversos produtos são fabricados com esse tipo de comunicação, por exemplo: fones de ouvido, caixas de som, câmeras digitais, Chromecast.
- O número de ameaças à segurança direcionadas a dispositivos de IoT aumentou nos últimos anos. Dada a penetração cada vez mais ampla da IoT em todo o espectro de atividades diárias e infraestruturas críticas, a ocorrência de incidentes de segurança cibernética deve ter uma taxa crescente nos próximos anos.



- 1 Projetos microcontrolados, que transferem informações por meio da comunicação sem fio Bluetooth, estão sendo utilizados para diversas soluções práticas, por exemplo: na aquisição remota de dados de sensores em uma planta industrial e no controle remoto de dispositivos atuadores. Dada a importância do protocolo Bluetooth em várias aplicações, marque a alternativa com a definição CORRETA desse protocolo.
 - a) () É um padrão de comunicação wireless desenvolvido para fornecer conexão entre diversos dispositivos e que transmite as informações por meio de redes ad hoc e fornece a sincronização automática entre os equipamentos pareados.
 - b) () É um conjunto de especificações para a comunicação sem fio entre dispositivos eletrônicos, com ênfase na baixa potência de operação, na baixa taxa de transmissão de dados e no baixo custo de implementação. Tal conjunto de especificações define camadas do modelo OSI subsequentes àquelas estabelecidas pelo padrão IEEE 802.15.
 - c) () É um padrão de comunicação sem fio que abrange uma rede de longa distância de baixo consumo (LPWAN), que tem taxas de transmissão abaixo de 50kbps para garantir o baixo consumo de energia.
 - d) () É uma tecnologia utilizada por produtos certificados que pertencem à classe de dispositivos de rede local sem fios (WLAN) baseados no padrão IEEE 802.11, que possibilita a conexão de dispositivos à internet.
 - e) () É uma tecnologia livre e aberta para a comunicação sem fio ponto a ponto por meio de luz do espectro visível ou infravermelho através do ar.

- 2 O módulo HC-05 tem seis conectores: STATE, RXD, TXD, GND, VCC, KEY. Cada um desses conectores tem uma função específica. Marque a alternativa CORRETA sobre a especificação dos pinos.
 - a) () O pino STATE, podendo também estar identificado como ENABLE, é usado para trocar o estado de funcionamento entre o modo de transferência de dados ou comandos AT.
 - b) () O pino RXD (transmissor de dados serial) e o pino TXD (receptor de dados serial).
 - c) () O pino KEY está ligado ao LED interno do módulo e fornece um feedback para verificar se o Bluetooth está funcionando corretamente.
 - d) () O pino GND (terra) e o pino VCC (alimentação positiva 3,3V, mas esse módulo suporta 5V).
 - e) () O pino ENABLE fornece a alimentação do Bluetooth quando estiver habilitado e corta a alimentação quando estiver desabilitado.

- 3 Um modelo de arquitetura IoT, proposto para segurança, pode ser dividido em três camadas básicas. No entanto, pode mudar de acordo com

o uso, como em algumas soluções para a indústria, que podem exigir mais camadas, mas todas seguindo as definições propostas para segurança IoT.



Qual das definições a seguir melhor define a camada de percepção?

- a) () É a camada composta por sensores inteligentes e atuadores que interagem com outros dispositivos do mundo físico para enviar e receber dados entre si ou para um dispositivo central IoT.
- b) () É a camada responsável por comportar todos os dados de segurança da rede IoT e serve como banco de dados para todas as aplicações, inclusive autorização de usuários e dispositivos.
- c) () Camada mais externa da arquitetura IoT que tem a função de permitir o acesso vindo da internet, propor as chaves de segurança e dar as devidas autorizações de acesso à rede privada.
- d) () É a camada que faz a comunicação entre os usuários e as aplicações (softwares) que estão instaladas nos equipamentos e têm a função de criar os scripts de acesso aos sites.
- e) () É a camada responsável por lidar com todo processamento de dados da rede IoT, controle de acesso dos dispositivos e liberação de acesso à internet por meio de permissões específicas do protocolo IoT.

4 Como a geração e a análise de dados são tão essenciais para a IoT, é necessário considerar a proteção de dados durante todo o seu ciclo de vida e comunicação. O gerenciamento de informações nesse nível é complexo porque os dados fluem por muitos limites administrativos com diferentes políticas e intenções. Os indivíduos certamente terão objetivos de privacidade diferentes das entidades corporativas, que, por sua vez, terão objetivos diferentes do governo ou de outras organizações. Muitas vezes, os dados são processados ou armazenados em dispositivos finais da rede IoT com recursos altamente limitados e vulneráveis a ataques sofisticados.

O texto acima retrata uma preocupação com segurança em nível de dispositivos que pode ser ilustrada na figura a seguir:



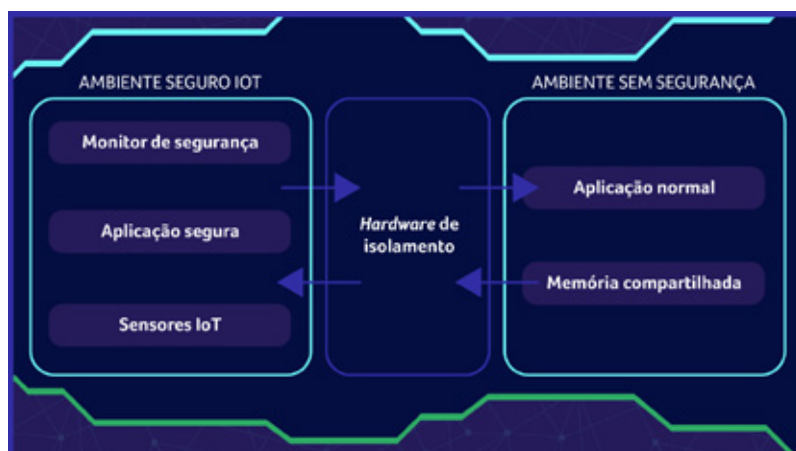
Qual camada do modelo de segurança para IoT o texto e a área designada como tecnologias sem fio para IoT representam?

- a) () Camada de detecção.
- b) () Camada de rede.
- c) () Camada de enlace.
- d) () Camada de interface.
- e) () Camada *wireless*.

5 A camada de interface, também conhecida como camada de aplicação, caracteriza-se por definir todos os aplicativos que usam a tecnologia IoT ou nos quais a IoT foi implantada. Capacidade de lidar com dados em massa é uma das possíveis vulnerabilidades de segurança que podem ser aproveitadas por invasores. Qual das seguintes afirmações poderia justificar o motivo da afirmativa apresentada?

- a) () Todas as camadas de segurança em IoT, e não só a camada de aplicação, têm a capacidade de executar atividades de processamento de alto volume de dados sem comprometer a segurança.
- b) () As aplicações para IoT são de responsabilidade das APIs que ajudam a camada a processar tal volume de informação. Com a ajuda dela, a camada não corre o risco de alto volume de processamento de dados.
- c) () As aplicações para IoT só são de responsabilidade da camada de detecção, que, além de determinar quais aplicações são permitidas, tem a função de encaminhar tudo para a camada de rede.
- d) () Nem sempre os dispositivos em uma rede IoT estarão operacionais/ativos. Isso representa que, enquanto estiverem inativos, não haverá troca de informações. Sem troca de informações, não corremos o risco de alto processamento de dados.
- e) () A enorme quantidade de fluxo de informações entre usuários requer capacidade para lidar com alto processamento de dados. Como resultado, se o sistema não for robusto, isso causará distúrbios na rede e perda de dados.

- 6 Em uma situação hipotética, uma estrutura de sensor foi sugerida com base em um hardware, conforme a figura a seguir, que protegerá os sensores em um dispositivo IoT de uma aplicação não autorizada (ameaça virtual). Isso é feito usando o recurso chamado de isolamento de hardware.



Implementando uma memória compartilhada no ambiente não seguro, o ambiente IoT pode acessá-lo; com isso, somos capazes de compartilhar o sensor quando necessário, por meio de um aplicativo seguro. Para realizar a segurança do acesso proposto, em qual nível entre as camadas de segurança para redes IoT essa estrutura de hardware deverá ser instalada?

- a) () Camada de detecção.
- b) () Camada de interface.
- c) () Camada de rede.
- d) () Camada de roteamento.
- e) () Camada de comutação.

APLICANDO A INTERNET DAS COISAS - IoT

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, você deverá ser capaz de:

- reconhecer as principais características dos sensores;
- diferenciar sensores de posição, velocidade, aceleração, força, pressão e torque;
- definir a aplicação de cada sensor baseando-se em suas características;
- reconhecer o uso do sistema RFID na gestão da armazenagem;
- relacionar o uso do sistema na automação das operações de estocagem;
- identificar a origem do RFID no Brasil e as suas vantagens competitivas;
- construir o conceito de big data e IoT;
- identificar elementos que contemplam uma solução de IoT;
- definir possibilidades de uso de IoT para automação.

PLANO DE ESTUDOS

Esta unidade está dividida em três tópicos. No decorrer da unidade você encontrará autoatividades com o objetivo de reforçar o conteúdo apresentado.

TÓPICO 1 – SENSORES

TÓPICO 2 – SISTEMAS DE RÁDIO POR FREQUÊNCIA (RFID)

TÓPICO 3 – BIG DATA E INTERNET DAS COISAS (IoT)



Preparado para ampliar seus conhecimentos? Respire e vamos em frente! Procure um ambiente que facilite a concentração, assim absorverá melhor as informações.

1 INTRODUÇÃO

Quando você acorda, antes mesmo de abrir seus olhos, você sabe onde estão suas extremidades, você não tem que olhar para seu braço ou sua perna para saber que estão dobrados. Da mesma forma, em um robô, quando os elos e articulações se movem, sensores, tais como potenciômetros, codificadores e resolvers enviam sinais para o controlador, permitindo-lhe determinar os valores articulares.

Neste tópico, estudaremos as características gerais dos sensores de posição, velocidade, força, pressão e torque.

2 CARACTERÍSTICAS DOS SENSORES

Diferentes tipos de sensores podem ser usados para uma mesma finalidade. A escolha de um sensor envolve características como:

- **Custo:** muito importante quando muitos sensores são utilizados para uma mesma máquina. Deve-se sempre buscar um equilíbrio do custo com a confiabilidade, precisão e importância dos dados fornecidos.
- **Tamanho:** na maioria das vezes, deve ser condizente com o tamanho do que será controlado. Um sensor não pode, por exemplo, prejudicar os movimentos de um braço mecânico por causa de seu tamanho elevado. Da mesma maneira, usar um potenciômetro para controlar o posicionamento de um guindaste limita o uso do sensor.
- **Peso:** em aplicações que envolvem movimento, o peso do sensor é um fator muito importante. Um sensor de visão (câmera) colocada sob um drone não deve impedi-lo de voar, por exemplo.
- **Tipo de saída (digital ou analógica):** a saída de um sensor de posição pode ser analógica, no caso do potenciômetro, ou digital, no caso de um codificador. Se um microcontrolador for utilizado para o controle do sistema, o codificador pode ser utilizado diretamente nele, ao passo que o sinal analógico do potenciômetro necessita ser convertido para digital para ser utilizado em conjunto com o microcontrolador.
- **Interfaceamento:** a saída de um sensor pode necessitar de um circuito auxiliar para se conectar a um controlador, por exemplo. Estes podem ser resistores, chaves, fontes de alimentação, fios, entre outros.

- **Resolução:** é tamanho do passo mínimo dentro do intervalo de medição. Em um dispositivo digital com n bits, a resolução será:

$$\text{Resolução} = \frac{\text{Alcance Total}}{2^n}$$

No caso de um codificador de 4 bits, teremos:

$$\text{Resolução} = \frac{360^\circ}{2^4} = 22,5^\circ$$

Em um dispositivo analógico como, por exemplo, um potenciômetro, a resolução é a própria resistência medida no fio (tende ao infinito).

- **Sensibilidade:** é a relação da saída com a entrada do sensor. Um sensor de deformação colocado em uma ponte pode indicar 1 V de tensão de saída para uma deformação de 10 cm em sua estrutura (baixa sensibilidade), enquanto um sensor de deformação colocado em uma balança, quando tem sua plataforma deslocada apenas 1 cm, pode indicar 5 V de tensão de saída (alta sensibilidade).
- **Linearidade:** um sensor com saída linear apresenta a mesma variação que ocorreu na entrada em sua saída. Entretanto, quase todos os dispositivos não são totalmente lineares, ou supostamente lineares em uma faixa de operação. Um sensor, em que sua saída varia de acordo com uma equação de segunda ordem, pode ter a saída linearizada tomando-se a raiz quadrada desse sinal, seja por um circuito eletrônico, seja por programação em um controlador.
- **Gama:** diferença entre a menor e a maior saídas que o sensor pode produzir, ou entre a menor e maior entradas com que pode operar corretamente.
- **Tempo de resposta:** é o tempo que leva para um sensor apresentar em sua saída uma porcentagem da variação total, geralmente 95% do valor nominal, quando ocorre uma excitação na entrada. Esses 95% correspondem a 4 constantes de tempo τ , que é o tempo que leva para o sensor chegar a 63,2% do valor nominal do sinal. O tempo de resposta de um termômetro é bem lento, enquanto o tempo de resposta de um potenciômetro é instantâneo.
- **Resposta de frequência:** um sensor de posição com tempo de resposta de 1 segundo, colocado em um transportador de containers que se move de maneira extremamente lenta, cumpre bem seu papel. A resposta em frequência desse sensor tem frequência de corte em 1 Hz, enquanto o transportador se move muito abaixo dessa frequência. Esse mesmo sensor, colocado em um braço robótico que solda componentes eletrônicos em uma frequência muito alta (10 soldas por segundo, ou 10 Hz), não tem tempo suficiente para fazer a leitura das posições do braço robótico, indicando ao controle sempre uma leitura errônea, pois sua resposta em frequência, com frequência e cone de 1 Hz, não suporta a frequência muito superior do braço robótico (10 Hz).

- **Confiabilidade:** é a relação de quantas vezes um sistema opera corretamente divididas por quantas vezes ele é usado. Um sensor que nunca falha tem 100% de confiabilidade. Sensores confiáveis, que durem ao longo do tempo, devem ser preferidos, ponderando-se seu custo.
- **Precisão:** é o quão próximo o valor da saída está do valor esperado. Um termômetro, no nível do mar, colocado em água fervente pura deve indicar 100 °C.
- **Repetibilidade:** é o quão variadas são as saídas para uma mesma entrada. Se para uma mesma entrada aplicada várias vezes o sensor apresenta valores muito próximos, apresenta boa repetibilidade.

FIGURA 1 – PRECISÃO VERSUS REPETIBILIDADE



FONTE: Adaptado de Niku (2013)



Um sensor impreciso pode ser corrigido ou compensado para funcionar próximo do ideal, desde que o mesmo seja repetível. Isso porque a repetibilidade faz com que o sensor apresente respostas sempre muito próximas para uma mesma entrada. Se estas respostas não condizem com o que deveria ser medido (imprecisão), basta aproximar essas respostas do valor que deveria ser apresentado, corrigindo assim a imprecisão. Sensores com baixa repetibilidade não são facilmente compensáveis.

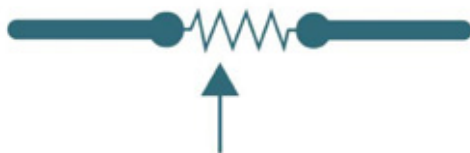
3 TIPOS DE SENSORES

3.1 SENSORES DE POSIÇÃO

Sensores de posição são utilizados para medir deslocamentos, tanto lineares quanto angulares, bem como movimentos. São exemplos de sensores de posição:

- **Potenciômetros:** transformam uma informação de posição em uma tensão. A medida que a posição do potenciômetro varia, a resistência medida varia conforme o cursor desliza sobre o resistor, e uma tensão proporcional é gerada (Figura 2). Podem ser lineares ou rotativos, podendo medir movimentos lineares ou angulares (Figura 3).

FIGURA 2 – ESQUEMÁTICO DO CIRCUITO DE UM POTENCIÔMETRO



FONTE: Os autores

FIGURA 3 – EXEMPLO DE POTENCIÔMETROS (A) ROTATIVOS E (B) LINEARES



(a)



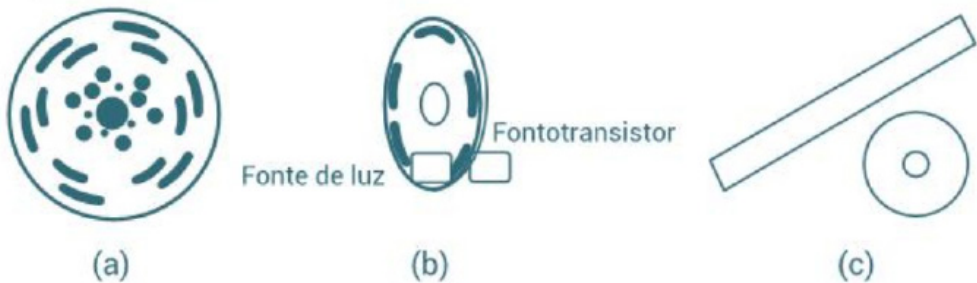
(b)

FONTE: Os autores

- **Codificadores:** pode ser um disco ou uma fita, os quais são divididos em pequenas sessões que podem ser opacas ou transparentes, ou reflexiva e não reflexiva (Figura 4). Uma fonte de luz é aplicada em um lado do codificador, ao passo que no outro lado existe um sensor de luz (fototransistor). A medida que o codificador se move, a luz é revelada (sinal em alta) ou obstruída (sinal em baixa) para o fototransistor, caracterizando uma saída digital. A medida que o disco gira, os sinais podem ser contados e o deslocamento pode ser medido (Figura 4 (b)).

- **Codificador incremental:** neste tipo de codificador, as áreas de seções opacas e transparentes são todas iguais e repetidas, de mesmo tamanho, representando cada uma um ângulo de rotação igual. Se o disco é dividido em apenas duas porções, cada porção é de 180° , logo, a resolução será de 180° , com uma precisão bastante baixa. Tipicamente, podem ter de 512 a 1024 seções, fornecendo deslocamentos angulares com resolução de $0,7^\circ$ a $0,35^\circ$. Este tipo de codificador é como um integrador, ou seja, apenas fornece as variações na posição angular (deslocamento). Quando um movimento é feito, o controlador conta o número de sinais que o codificador envia, informando quanto foi a variação no deslocamento, mas é incapaz de informar a posição real. Por esse motivo, um codificador incremental deve sempre ser reiniciado no início das operações para se saber a posição inicial e, a partir dele, estimar as outras posições partindo de seu deslocamento. Adicionalmente, se apenas um conjunto de fendas é usado, será impossível determinar se o disco está girando no sentido horário ou anti-horário, pois o fototransistor apenas recebe a informação da intensidade da luz e conta o número dessas variações. Para remediar essa situação, os codificadores incrementais tem dois conjuntos de fendas (dois canais: A - diâmetro externo e B - diâmetro interno), $1/2$ passo fora de fase cada um (Figura 4(a)). Assim, se o controlador recebe do codificador um sinal de A e depois B, o disco está girando em sentido anti-horário. Se recebe um sinal de B, depois de A, o disco está girando em sentido horário. O crucial no controle desse sensor é configurar o sistema para contar as variações do sinal, e não apenas reconhecer se o sinal é alto ou baixo.

FIGURA 4 – CODIFICADORES



Codificadores (a) Um simples codificador incremental rotativo em forma de disco montado sobre um eixo motor. Esse codificador mede rotações angulares. (b) Esquema de um arranjo codificador rotativo. (c) Um codificador linear absoluto do tipo refletivo que pode medir movimentos lineares e um codificador incremental rotativo em forma de disco com 1024 fendas.

FONTE: Adaptado de Niku (2013)

- **Codificadores absolutos:** diferente dos incrementais, esses codificadores indicam a posição exata do disco a qualquer momento, não necessitando ser reiniciados. Apresentam múltiplas linhas de seções, cada uma diferente das outras, com sua própria fonte e detector de luz. Um codificador com 3 linhas

pode ter $2^3 = 8$ combinações distintas, cada seção cobrindo um ângulo de 45° , como mostrado na Figura 5.

FIGURA 5 – CÓDIGO BINÁRIO E CÓDIGO DE GRAY



FONTE: Adaptado de Niku (2013)

Dentro dessa sessão de 45° , o controlador não pode determinar onde o codificador está, portanto, a resolução é de apenas 45° . Para aumentar a resolução, deveria haver mais seções, ou bits. Um codificador com 10 linhas, com 1.024 divisões em uma linha, tem 10 bits de informação ($2^{10} = 1.024$), ou seja, $0,35^\circ$ de resolução. Codificadores comerciais com 16 bits estão disponíveis. Nesses codificadores, é preferível os que utilizam o código de Gray ao invés do código binário. No código binário, vários bits variam simultaneamente de uma leitura para outra. Por alguma imperfeição, se todas essas variações não ocorrem exatamente no mesmo tempo, a leitura é errônea, pois vários valores são lidos antes de se chegar ao valor esperado. No código de Gray, uma vez que existe apenas uma variação de bit por vez, o sistema irá sempre encontrá-la. A Tabela 1 lista o código de Gray para os números 0 a 11.

TABELA 1 – CÓDIGOS BINÁRIO E DE GRAY

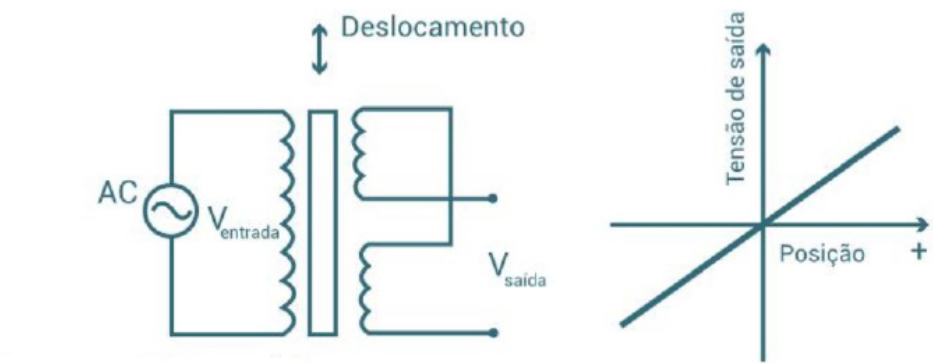
#	Código de Gray	Código Binário
0	0000	0000
1	0001	0001
2	0011	0001
3	0010	0011
4	0110	0100
5	0111	0101
6	0101	0110
7	0100	0111
8	1100	1000
9	1101	1001

10	1111	1010
11	1110	1011

FONTE: Adaptado de Niku (2013)

- **Transformadores Diferenciais Variáveis Lineares (TDVL):** é um transformador cujo núcleo se move com a distância medida e que gera uma tensão variável analógica como resultado desse deslocamento. Em um transformador, duas bobinas com diferentes números de espiras apresentam um núcleo de ferro. A energia elétrica em uma bobina cria um fluxo, por meio do magnetismo do núcleo de ferro, que induz uma tensão proporcional na segunda bobina. Na presença de um núcleo de ferro, as linhas de fluxo estão reunidas para dentro, aumentando a intensidade do campo e a tensão induzida na segunda bobina. Se nenhum núcleo de ferro está presente, as linhas de fluxo podem dispersar-se, reduzindo a intensidade do campo magnético.

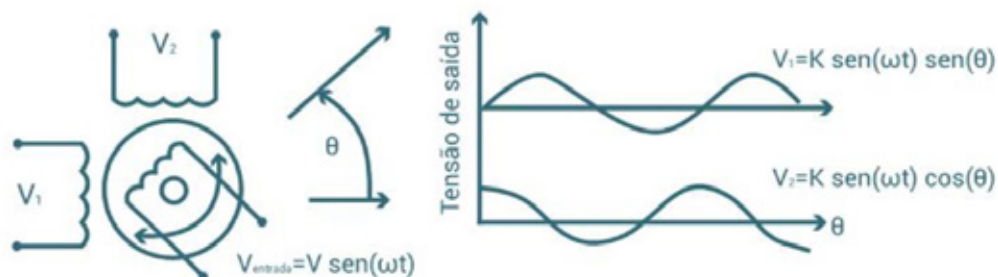
FIGURA 6 – TRANSFORMADOR DIFERENCIAL VARIÁVEL LINEAR



FONTE: Adaptado de Niku (2013)

- **Resolvedores:** apresentam o princípio de funcionamento de um TDVL, mas são usados para medir um movimento angular. Têm duas bobinas secundárias, montadas e afastadas 90° uma da outra. Entre elas, um rotor com um núcleo e uma bobina primária, conforme a Figura 7. À medida que o rotor gira, a tensão aumenta na bobina secundária que está mais paralela à bobina primária do rotor. Ao ficarem totalmente paralelas, a tensão induzida nesta bobina secundária será máxima, na outra, mínima. Para todos os ângulos entre o máximo e o mínimo, as duas bobinas secundárias desenvolvem uma tensão proporcional ao seno e ao cosseno do ângulo entre o primário e as duas bobinas secundárias, eliminando a necessidade do cálculo desses valores mais tarde. Resolvedores são confiáveis, robustos e precisos.

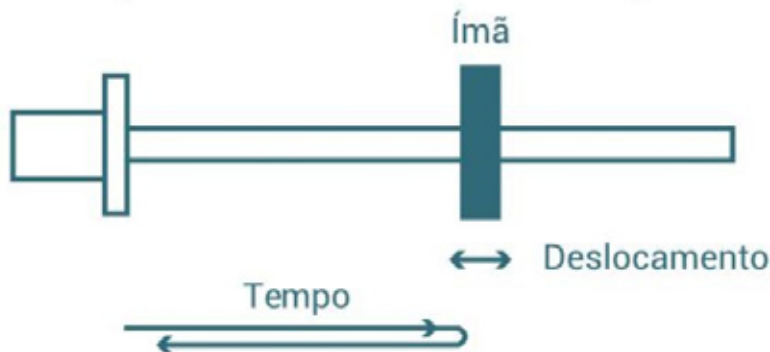
FIGURA 7 – ESQUEMA DE UM RESOLVEDOR



FONTE: Adaptado de Niku (2013)

- **Transdutores de Deslocamento Magnetostrictivos (Lineares) (TDML ou TDM):** um pulso gerado em um condutor atinge um ímã e salta para trás. O tempo de ida e volta do ímã é convertido em uma distância se a velocidade do movimento é conhecida. Um esquema simples do sensor é mostrado na Figura 8.

FIGURA 8 – DESENHO ESQUEMÁTICO DE UM SENSOR DE DESLOCAMENTO MAGNETOSTRITIVO



FONTE: Adaptado de Niku (2013)

- **Sensores de Efeito Hall:** a tensão de saída do sensor varia toda vez que um ímã permanente ou uma bobina que produz um fluxo magnético estão próximos do sensor. A saída analógica desse sensor deve ser convertida para aplicações digitais.

3.2 SENSORES DE VELOCIDADE

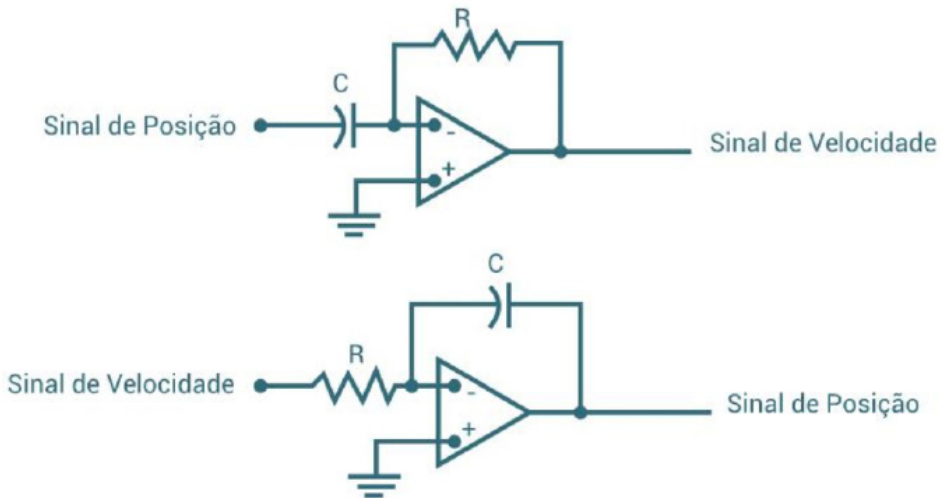
- **Codificadores:** se um codificador é utilizado para medição de deslocamento, não há necessidade de um sensor de velocidade. A variação do deslocamento pode ser calculada. Um valor típica para $d\tau$ é 10 ms. Pode ser utilizado um valor menor para movimentos rápidos, ou maiores para movimentos lentos. O $d\tau$ ideal é o que proporciona maior precisão e eficácia do controlador.
- **Tacômetro:** convertem a energia mecânica em energia elétrica. Um bom exemplo é o alternador de um carro. A tensão de saída é proporcional à velocidade

angular de entrada. São geralmente imprecisos em velocidades muito baixas.

- **Diferenciação de Sinal de Posição:** um potenciômetro de fio enrolado produz um sinal entrecortado, com degraus, impróprio para a diferenciação. Um potenciômetro com filme de polímero condutor usado na medição de posição produz um sinal limpo e contínuo, evitando a criação de grandes impulsos no sinal de velocidade. A diferenciação do sinal de posição é a velocidade. Um simples circuito R-C com um amplificador operacional (Figura 9) pode ser utilizado para a diferenciação, em que o sinal de velocidade é:

$$V_o = -RC \frac{dv_i}{dt}$$

FIGURA 9 – ESQUEMA DE DIFERENCIAÇÃO E INTEGRAÇÃO DE CIRCUITOS R-C COM UM AMPLIFICADOR



FONTE: Adaptador de Niku (2013)

Da mesma forma, os sinais de velocidade (ou aceleração) podem ser integrados para fornecer a posição (ou velocidade) como:

$$V_o = -\frac{1}{RC} \int V_i dt$$

3.3 SENSORES DE ACELERAÇÃO

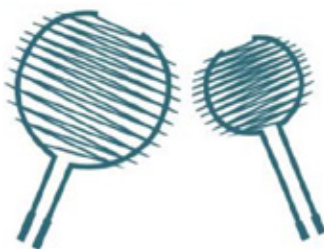
Acelerômetros são sensores muito comuns para medir acelerações. Entretanto, em geral, não são usados em robôs industriais. A partir de um codificador, pode-se medir a velocidade e, conseqüentemente, a aceleração, tomando-se a diferença da velocidade atual com a velocidade anterior, no tempo Δt . A partir de um potenciômetro de polímero condutor, basta diferenciar o sinal

de posição duas vezes: a primeira diferenciação resulta na velocidade, a segunda, na aceleração.

3.4 SENSORES DE FORÇA E PRESSÃO

- **Piezoelétricidade:** material piezoelétrico comprime se exposto a uma tensão e produz tensão se é comprimido. Desse modo, pode medir pressões ou forças. A tensão analógica deve ser condicionada e amplificada para uso.
- **Resistor Sensor de Força (RSF):** é um dispositivo de polímero espesso que apresenta uma resistência decrescente com o crescimento da força aplicada perpendicularmente à sua superfície. Em um modelo particular, a resistência varia de cerca de 500 k Ω para 1 k Ω . A Figura 10 mostra um típico resistor de detecção de força.

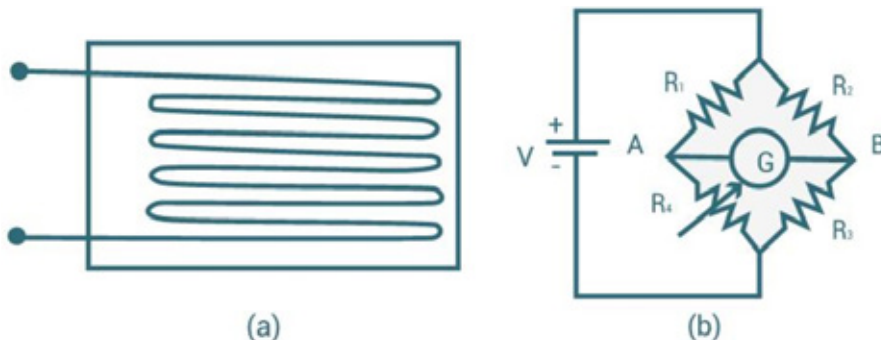
FIGURA 10 – UM TÍPICO RESISTOR DE SENSORIAMENTO DE FORÇA (RSF). A RESISTÊNCIA DESSE SENSOR DIMINUI À MEDIDA QUE A FORÇA AGINDO SOBRE ELE AUMENTA



FONTE: Adaptador de Niku (2013)

- **Strain Gauge:** quando uma pressão, que é uma função das forças, é aplicada em um Strain Gauge, sua resistência variável produz uma tensão proporcional a essa pressão. A Figura 11 (a) é um desenho esquemático simples de um strain gauge, que são usados dentro de uma ponte de Wheatstone (Figura 11 (b)).

FIGURA 11 – (A) UM STRAIN GAUGE E (B) UMA PONTE DE WHEATSTONE



FONTE: Adaptador de Niku (2013)

Supondo que R é o strain gauge, quando sob tensão, seu valor vai variar, causando desequilíbrio na ponte de Wheatstone e um fluxo de corrente de A para B, em que a tensão proporcional é medida entre esses dois pontos. Ajustando a resistência de um dos outros resistores até que o fluxo de corrente torna-se zero, a variação na resistência do strain gauge pode ser determinada por:

$$\frac{R_1}{R_4} = \frac{R_2}{R_3}$$

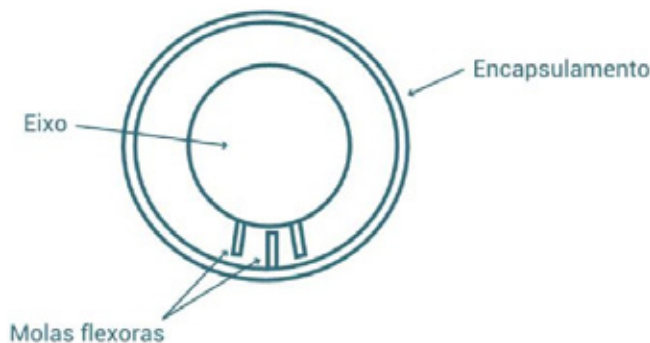
- **Espuma antiestática:** é condutora, e sua resistência varia com a força aplicada. É um simples e barato sensor de força e contato. Para usá-la, basta pegar um pedaço da espuma e inserir um par de fios em dois lados do mesmo e medir a tensão ou resistência por meio dela.

3.5 SENSORES DE TORQUE

Um sensor de torque é formado por dois sensores de força colocados em um mesmo eixo, um de frente pro outro. Se um torque é aplicado nesse eixo, duas forças opostas, de sinais contrários, são medidas, o que pode ser convertido para um torque.

A Figura 12 mostra uma representação esquemática de um sistema, o qual apresenta molas instrumentada, com pelo menos seis strain gauges. Essas molas de flexão, presas a um eixo, formam um par de capacitores usados como parte de um circuito oscilador a diodo-túnel. À medida que o eixo gira ligeiramente sob a carga, a capacitância de cada par varia, provocando uma variação na frequência de oscilação do circuito. Ao medir a frequência das oscilações, o torque pode ser determinado.

FIGURA 12 – O TORQUE PODE SER MEDIDO POR MEIO DA MEDIÇÃO DAS VARIAÇÕES NA FREQUÊNCIA DE OSCILAÇÃO DE UM OSCILADOR DIODO-TÚNEL QUANDO A CAPACITÂNCIA DAS MOLAS DE FLEXÃO VARIA DEVIDO AO TORQUE APLICADO



FONTE: Adaptador de Niku (2013)

4 APLICAÇÕES DE CADA TIPO DE SENSOR:

Sensores de posição são utilizados para medir deslocamentos, tanto lineares quanto angulares, bem como movimentos. São exemplos de sensores de posição:

- **Sensor de posição:** em robótica, podem medir e indicar a posição e o ângulo de cada junta do robô. Em uma mesa XYZ, podem medir e indicar a posição da garra. Em uma impressora, pode indicar ao controle a posição exata onde deve ser despejada a tinta. Um sensor de efeito Hall pode ser utilizado na detecção de minas subterrâneas, já que sua tensão de saída irá variar quando próximo ao magnetismo da mina.
- **Sensor de velocidade:** em robótica, pode ser utilizado para medir e controlar a velocidade com que o robô se move. Em um carro, informa a velocidade em que o veículo está.
- **Sensor de aceleração:** em robótica, para o controle de alta precisão de atuadores lineares e para o controle por realimentação de articulação de robôs. Pode ser utilizado para detectar a força de batidas, no caso de uma bateria eletrônica musical.
- **Sensores de força e pressão:** em robótica, sensor de força e pressão são utilizados na garra do robô para que esta não esmague um material muito delicado, nem que o deixe cair por não ter atrito suficiente entre a garra e o material. Um sensor piezoelétrico também pode ser usado em uma bateria eletrônica para detectar a intensidade das batidas da baqueta na pele dos tambores. Balanças comerciais utilizam sensores de força e pressão para medir peso.
- **Sensores de torque:** em robótica, usados na ponta dos dedos de robôs antropomórficos. Na indústria, podem medir o torque em processos de parafusamento automáticos, impedindo que a rosca se danifique. Na produção automatizada de garrafas PET, o sensor de torque permite que a tampa seja colocada com o torque ideal, fazendo com que a mesma não se desenrosque e permita a fuga de gás, nem fique muito apertada de tal modo que o usuário não possa abrir a garrafa.



RESUMO DO TÓPICO 1

Neste tópico, você aprendeu que:

- Sensores servem para informar um circuito eletrônico a respeito de um evento. Imediatamente a partir da leitura, ele atua ou comanda uma determinada ação.



- 1 Um sensor utilizado em robótica apresenta várias vezes a mesma saída para uma mesma entrada. Esse sensor também apresenta uma grande variação na saída para uma pequena oscilação na entrada, sendo que a resposta da saída é semelhante à entrada. Estamos nos referindo às características de:
 - a) ☐ Repetibilidade, sensibilidade e linearidade.
 - b) ☐ Precisão, interfaceamento e resolução.
 - c) ☐ Repetibilidade, confiabilidade e linearidade.
 - d) ☐ Repetibilidade, gama e resolução.
 - e) ☐ Precisão, sensibilidade e resolução.

- 2 Um sensor de posição de uma articulação rotativa robótica deve ser escolhido para uma aplicação onde se deseja a informação do seno do ângulo dessa articulação. Além disso, esse sensor deve ser confiável, robusto e preciso. O sensor de posição ideal para essa aplicação é um:
 - a) ☐ Potenciômetro.
 - b) ☐ Resolvedor.
 - c) ☐ Transformadores Diferenciais Variáveis Lineares (TDLV).
 - d) ☐ Codificador.
 - e) ☐ Sensor de efeito Hall.

- 3 Um potenciômetro com filme de polímero está sendo usado para medição de posição da articulação de um robô. Para medir apenas a velocidade angular dessa articulação, de maneira a se obter boa resolução a baixas velocidades e baixo custo, é necessário:
 - a) ☐ Substituir o potenciômetro por um codificador.
 - b) ☐ Substituir o potenciômetro por um tacômetro.
 - c) ☐ Utilizar esse mesmo sensor e diferenciar seu sinal com um amplificador operacional e um circuito R-C.
 - d) ☐ Utilizar esse mesmo sensor e integrar seu sinal com um amplificador operacional e um circuito R-C.
 - e) ☐ Substituir o potenciômetro por um tacômetro e integrar seu sinal com um amplificador operacional e um circuito R-C.

- 4 Alguns Robôs são utilizados na indústria de computadores para inserir pequenas placas pré-soldadas com CIs em outras placas maiores. Para isso, a força deve ser medida para que a placa maior não se quebre. Quando o robô faz esse movimento, as placas com os CIs ainda encontram-se em uma temperatura maior que as placas maiores devido ao processo de soldagem.

Para medir essa força, de maneira barata e sem necessidade de complicados condicionadores de sinais, pode ser utilizado:

- a) () Um sensor de aceleração com a informação da massa da placa.
- b) () Um sensor de força e pressão piezoelétrico.
- c) () Um resistor sensor de força.
- d) () Um sensor de força e pressão de espuma antiestática.
- e) () Sensor de força e pressão Strain Gauge.

5 Um robô, utilizado na indústria alimentícia, deve tampar um recipiente de vidro com uma tampa de metal. Se apertar demais, o vidro quebra. Se deixar folgado, o líquido que protege o alimento vaza pelo espaço entre a tampa e o vidro. Para o robô apertar essa tampa corretamente no recipiente de vidro, deve-se utilizar um:

- a) () Sensor de posição.
- b) () Sensor de velocidade.
- c) () Sensor de aceleração.
- d) () Sensor de força e pressão.
- e) () Sensor de torque.

SISTEMAS DE RÁDIO POR FREQUÊNCIA (RFID)

1 INTRODUÇÃO

Atualmente, produtividade e redução de custos são palavras de ordem para as organizações que querem ter competitividade e sustentabilidade financeira. Para tanto, a logística tem auxiliado as empresas na organização e no controle do fluxo de produtos e serviços, melhorando a sua qualidade e aumentando a vantagem competitiva.

Nesse contexto, as soluções de tecnologia da informação são de grande importância para que se possa atingir níveis de confiabilidade propícios para a tomada de decisões. Uma tecnologia que tem se mostrado muito útil para inúmeras empresas é a identificação por radiofrequência, que usa ondas de rádio para identificar automaticamente pessoas ou objetos. Existem vários métodos de identificação, mas o mais comum é armazenar um número serial que identifica uma pessoa, um objeto, dentre outras informações, em um microchip que está ligado a uma antena.

Neste tópico, estudaremos como essa tecnologia funciona, como ela surgiu e foi implementada no mundo e no Brasil e quais são as vantagens que ela traz para os processos de armazenamento e estocagem no âmbito da logística.

2 SISTEMA RFID NA GESTÃO DA ARMAZENAGEM

A gestão da armazenagem é um fator crítico para o sucesso de um processo logístico. Ao armazenar produtos, é fundamental que haja o efetivo controle da informação sobre o que está disponível no estoque, o que está faltando, como são administrados os itens perecíveis, que tipo de transporte será utilizado e de que forma a demanda do cliente será atendida. A informação da armazenagem tem relação direta com a tomada de decisão e, por conseguinte, com a possibilidade de redução de custos operacionais, tornando todo o processo logístico mais eficaz e ágil.

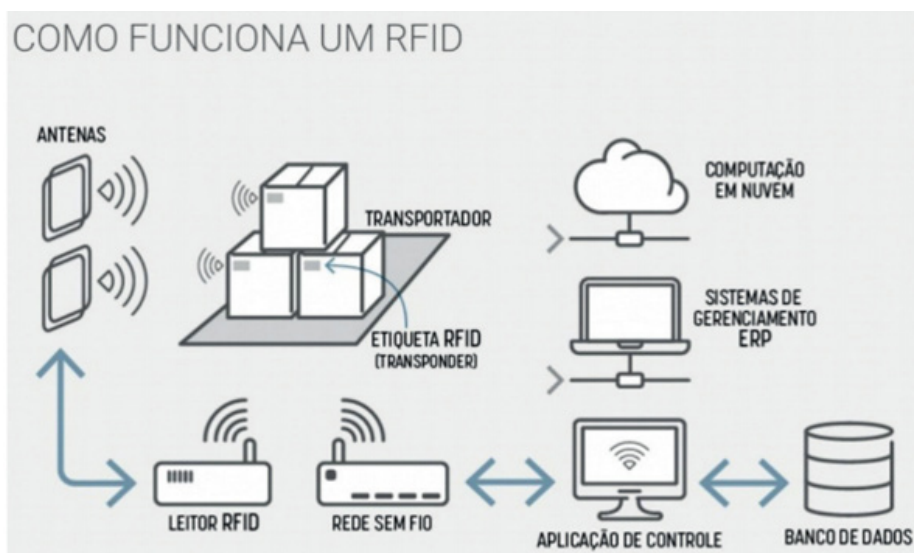


Dentro do processo logístico, a armazenagem é considerada uma das atividades de apoio, aquelas que dão suporte ao desempenho das atividades primárias, possibilitando que a empresa alcance o sucesso, mantenha seus clientes e conquiste novos, por meio do pleno atendimento do mercado e da satisfação total do acionista em receber seu lucro, conforme leciona Pozo (2004).

Os fluxos de informação do estoque precisam de acuracidade, especialmente quanto às entradas e saídas. Uma das tecnologias mais recentes no sistema de armazenagem e que pode fornecer os dados precisos dos produtos é a identificação por radiofrequência (RFID, do inglês radio frequency identification). Esse sistema é uma poderosa e versátil tecnologia para identificar, rastrear e gerenciar produtos em estoques nas organizações.

Mas como isso acontece? As chamadas etiquetas inteligentes (em inglês, tags), ou chips, são colocados nos produtos e emitem uma onda de rádio, que, ao ser capturada, revela as informações de rastreabilidade daqueles itens. Sempre que a leitura enviar sinais relacionados a um objeto, o circuito de RFID fornece as informações referentes a ele. Na Figura 13, você pode visualizar as ondas de radiofrequência sendo emitidas pelas etiquetas e captadas pelas antenas de RFID. Essas informações são enviadas para os bancos de dados disponíveis e podem ser acessadas pelos sistemas disponíveis.

FIGURA 13 – FUNCIONAMENTO DO SISTEMA RFID



FONTE: <<https://bit.ly/3gjyGsh>>. Acesso em: 30 jun. 2020.

A antena, que é localizada na etiqueta, recebe os sinais eletromagnéticos emitidos por um leitor e transmite as informações armazenadas. Diferentemente dos códigos de barras convencionais, que exigem um contato direto entre o código impresso e o leitor (scanner), o sistema RFID envia sinais eletromagnéticos e possibilita a identificação à distância.

Existem dois tipos de etiquetas: as ativas e as passivas. A etiqueta ativa possui uma bateria, cuja energia permite que a etiqueta se comunique com o receptor; já a etiqueta passiva obtém energia por meio do campo eletromagnético criado pela antena, conforme leciona Santini (2008). Uma tag RFID tem um tamanho bem reduzido e, mesmo com a antena necessária para o seu funcionamento, pode ser embutida em cartões com a espessura de um cartão magnético, ou mesmo em etiquetas de roupas.

Os cartões com tags RFID têm sido utilizados para o controle de acesso em prédios e empresas; nesses casos, o próprio crachá do funcionário contém informações, como quem ele é e qual o nível de acesso que ele possui dentro daquele edifício. Outro exemplo de uso dessa tecnologia são as etiquetas implantadas em paletes que contêm produtos industrializados — estas contêm informações como validade, origem, destino e quantidades consolidadas. Ao passar pelos leitores que captam a radiofrequência, todas as informações daquele unitizador são transmitidas para o sistema de armazenamento do estoque. Nesse caso, não há interação humana no processo, o que facilita o fluxo contínuo de entradas e saídas dos produtos e proporciona ganhos de tempo e diminuição de erros na informação.



As funcionalidades da tecnologia RFID na gestão de armazenamento são diversas e representam uma grande oportunidade de inovação e melhoria de processos. Saiba mais sobre essa tecnologia e as suas diferentes aplicações acessando os links indicados a seguir.

Supermercado do futuro — O vídeo disponível no link a seguir demonstra como pode se dar a aplicação da tecnologia RFID em supermercados.

<https://goo.gl/HX1bvM>

Custos da tecnologia RFID — Neste artigo, você pode conferir informações sobre o custo da tecnologia RFID e os ganhos relacionados à sua implantação.

<https://goo.gl/5ra5Zm>

Empresas que utilizam RFID em seus processos — Nesta matéria da RFID Brasil, você pode conferir cinco empresas que já utilizam a tecnologia RFID em seus negócios.

<https://goo.gl/ANuosZ>

3 VANTAGENS DO SISTEMA RFID PARA A GESTÃO DE ARMAZENAMENTO

A flexibilidade dos sistemas RFID é um ponto que proporciona competitividade no processo logístico. Quando comparada com outros sistemas de gestão de armazenamento, a tecnologia RFID ganha em confiabilidade (códigos de barras tendem a apagar com o tempo) e facilidade de leitura (tags podem estar dentro da água, na lama ou circundados por metal). Além disso, como a captura de dados é feita de forma automática, existe a redução de falhas humanas no processo, conforme lecionam Dresch, Efrom e Grumovski (2008).

Os benefícios primários da tecnologia RFID são:

- eliminação de erros de escrita e leitura de dados;
- coleta de dados de forma mais rápida e automática;
- redução do processamento de dados; e
- maior segurança na operação.

Mas a principal vantagem do uso de sistemas RFID é realizar a leitura sem o contato e sem a necessidade de visualização direta no leitor. É possível, por exemplo, colocar a tag dentro de um produto e realizar a leitura sem ter que desempacota-lo, já que as tags RFID podem ser lidas simplesmente ao passar por um leitor. Isso representa inovação, agilidade e ganhos operacionais. Outro fator que facilita a aceitação dessa tecnologia é o fato de que múltiplas tags podem ser lidas ao mesmo tempo.



Imagine um fornecedor que está mandando um palete com 40 caixas de matéria-prima para uma indústria. Se a tecnologia RFID for usada, as caixas já estarão cada uma com a sua tag; ao ser entregue na fábrica, o palete passa por um leitor que automaticamente lê as 40 tags, registrando a entrada daquele material na base de dados. Na linha de produção, as tags podem identificar um determinado produto desde o início de sua produção. A etiqueta pode conter dados como a cor com a qual o produto deve ser pintado, os funcionários encarregados da produção, o modelo que está sendo produzido, dentre outros.

Mas um dos maiores ganhos que a radiofrequência traz para a gestão de armazenamento é a diminuição de estoques. Com o uso das informações disponíveis em tempo real, há menos necessidade de estoques de produtos, pois há um controle mais eficaz. Também é possível o ganho com a agilidade no reabastecimento, suprindo os itens faltantes mais rapidamente e identificando aqueles próximos da validade.

4 SISTEMA RFID NA AUTOMAÇÃO DE OPERAÇÕES DE ESTOCAGEM

Para que você possa entender bem a influência da tecnologia de radiofrequência nos sistemas logísticos, é importante compreender o grande desafio que as operações de estocagem têm de atender o consumidor final sem incorrer em custos desnecessários de inventário. Torna-se cada vez mais necessário garantir a presença dos itens indispensáveis à produção, com uma equivalente redução dos investimentos financeiros.

Portanto, é inegável que os sistemas de controle devem garantir a confiabilidade da informação existente, contábil ou não, em relação à existência física dos itens controlados. Quando a informação no sistema não confere com o saldo real, o inventário não é confiável ou não tem acuracidade.



Imagine que um dos seus maiores clientes deseja comprar um grande lote de sapatos produzidos por sua indústria, e você acaba de fechar um grande negócio com ele. Você está satisfeito porque suas metas financeiras serão atingidas. No entanto, quando você acerta os detalhes com a produção, sente a inoportuna sensação de incapacidade ao ouvir o relato de seu gerente dizendo que não há matéria-prima suficiente para realizar a demanda. Até contatar os fornecedores e receber a matéria-prima, haverá imenso prejuízo no prazo de entrega prometido ao seu cliente. Perceba a perda financeira, institucional e até mesmo de credibilidade no mercado diante dessa situação. Conclusão: uma gestão de estoque ineficiente pode levar à perda de vendas importantes por falta de produtos ou matérias-primas, ou causar uma situação financeira difícil, devido ao excesso de itens estocados sem demanda para consumi-los.

Esse pequeno exemplo explica o quanto um estoque necessita de precisão no inventário dos seus itens. As diferenças de quantidade e a falta de previsão adequada são originadas por vários motivos, como erros dos sistemas e, até mesmo, equívocos nas entregas pelos fornecedores, demonstrando a falta de controle operacional.

Tal situação demanda o investimento em automação no estoque, que aumenta a eficiência, reduz perdas significativas e aumenta a produtividade. A automação prevê equipamentos que eliminam o esforço físico e ainda oferecem maior segurança, além de agregar valor ao negócio e indicar soluções inteligentes de performance diferenciada, com confiabilidade e rastreabilidade. É bom lembrar que existem dois tipos de automação: mecânica e computadorizada.

- O **equipamento mecânico** é aquele cujos processos são realizados com motores de forma mecânica, sendo impulsionado por meio de alavancas manuais.

- O **equipamento computadorizado** é aquele que funciona por meio de chip e desenvolve todos os processos por meio de programas (software) pré-programados.

É nesse contexto que a utilização da tecnologia RFID se apresenta como uma solução de automação, com o uso de chips e software nas operações de estocagem. Condea, Thiesse e Fleisch (2012) lecionam que as políticas de estoque baseadas no uso de RFID têm potencial para elevar a eficiência em custos e o nível de serviço.

Mas vale lembrar que diferentes sensibilidades aos fatores de custo e taxas baixas de leitura devem ser consideradas quando se escolhe uma política de controle de estoques com RFID. Para automatizar a atividade de estocagem, há a necessidade de uma avaliação técnica adequada, evitando o investimento sem critérios. Alguns indícios que justificam a análise da viabilidade da automação na estocagem são (SENAI, 2014):

- falta de espaço;
- alto custo de mão de obra;
- estocagem de cargas perigosas;
- complexidade do sistema de separação de pedidos;
- itens de alta movimentação (giro/popularidade);
- padronização de volumes e embalagens;
- elevada exigência no controle do estoque (acuracidade de saldo);
- estocagem em áreas com altas e/ou baixas temperaturas.



Acesse o artigo da Imam Consultoria sobre a automação na estocagem de transelevadores e entenda mais sobre a hora certa de automatizar, considerando diversos fatores.

<https://goo.gl/PfMkn1>

5 ORIGEM DO RFID NO BRASIL E VANTAGENS COMPETITIVAS

A tecnologia RFID surgiu com o advento da Segunda Guerra Mundial. Nos anos de 1930, o Exército e a Marinha enfrentaram o desafio de identificar adequadamente alvos no ar, no mar e no solo. Nesse contexto, países como Estados Unidos, Japão, Alemanha e Inglaterra passaram a utilizar sistemas de radares que permitiam identificar a aproximação de aviões. Na década de 1960

foram lançadas as primeiras atividades comerciais relacionadas ao RFID. Mas foi somente na década de 1970 que pesquisadores e instituições acadêmicas passaram a se interessar muito mais pelo conhecimento daquela nova tecnologia, e foram realizados avanços em laboratórios.

A década de 1980 marcou a expansão do sistema RFID no Brasil, especialmente no transporte, no controle de acessos e em pedágios. Essa época também foi marcada pelo avanço do uso dessa tecnologia no varejo de grandes marcas, como Procter & Gamble, Gillette e Wal-Mart. No setor comercial, a sua primeira utilização se deu em sistemas antifurto, que utilizavam ondas de rádio para determinar se um item havia sido roubado ou pago normalmente. Foi nesse contexto que surgiram as tags (etiquetas eletrônicas), que fazem parte do sistema de RFID até hoje (RFID..., [2018?]). O Quadro 1 sintetiza os eventos relacionados à tecnologia RFID.

QUADRO 1 – HISTÓRICO DO SISTEMA RFID POR DÉCADAS

Década	Eventos
1940–1950	Utilização de radar, principalmente no desenvolvimento da Segunda Guerra Mundial.
1950–1960	Explorações tecnológicas do sistema RFID e experimentos em laboratório.
1960–1970	Começo das aplicações de campo (<i>field trials</i>).
1970–1980	Explosão do desenvolvimento do RFID; os testes com o sistema RFID aceleraram.
1980–1990	As aplicações comerciais do sistema RFID viraram tendência.
1990–2000	Emergência dos padrões; sistema RFID largamente implantado.

FONTE: Adaptado de Rfid (2018)

Cabe destacar, ainda, que a RFID é uma tecnologia de identificação que utiliza a radiofrequência, e não a luz, como no caso do sistema de códigos de barras, para capturar dados. Logo, a solução pode ser usada em outros segmentos. Por exemplo, muitos prédios e escritórios usam essa tecnologia para controlar a entrada e a saída de pessoas, como visto anteriormente, bem como hospitais, laboratórios e clínicas. Com a possibilidade de rastreabilidade oferecida pelo chip ou pela etiqueta inteligente, também é possível buscar a localização de médicos e materiais cirúrgicos, fazer o controle de estoque de medicamentos, verificar a compatibilidade de sangue e, até mesmo, marcar a linha de chegada em corridas ao ar livre.



Como você viu ao longo do tópico, a RFID é uma solução relevante para os processos de armazenagem e estocagem de produtos. No entanto, é preciso considerar que a implantação desse recurso apresenta custos elevados de investimento. Portanto, é preciso realizar um estudo de viabilidade técnica e de retorno financeiro.

Veja que a RFID não é necessariamente melhor do que os códigos de barras. A grande diferença entre essas duas tecnologias é que os códigos de barras são uma tecnologia de linha de visão. Isto é, um leitor precisa "ver" o código de barras para o ler, o que significa que as pessoas normalmente têm de orientar o código de barras em direção a um leitor para que ele seja lido. A identificação por radiofrequência, por outro lado, não requer linha de visão. As tags podem ser lidas desde que estejam dentro do alcance de um leitor.

O custo da tecnologia RFID em relação aos sistemas de código de barras é um dos principais obstáculos para o aumento de sua aplicação comercial. Atualmente, uma etiqueta inteligente custa nos EUA cerca de 25 centavos de dólar, na compra de um milhão de chips. No Brasil, segundo a Associação Brasileira de Automação, esse custo sobe e já foi cotado em 80 centavos a unidade.

6 VANTAGENS COMPETITIVAS DA TECNOLOGIA RFID

Diante da captura da identificação de produtos em alta velocidade, sem precisar do contato visual do produto, a RFID permite inventariar grandes quantidades com precisão e integridade da informação, além de fornecer a localização exata dos produtos. Essas soluções se apresentam como elementos fundamentais para as demandas atuais da logística, como redução de custos e controle de fluxo de produtos e serviços, melhorando a qualidade e aumentando o nível de competitividade das organizações.

Com a implantação do sistema automatizado, é possível eliminar perdas em função de manuseio inadequado e furtos, atingir controle total de estoques, ter uma economia operacional e, principalmente, oferecer uma expedição otimizada para o atendimento aos clientes. A redução de tempo de manuseio de produtos é outro fator que gera ganhos e redução de custos. O processo de leitura pelas tags se repete em todas as etapas que exigem conferência, como receber mercadorias dos fornecedores, levá-las para a área de vendas, os caixas e o estoque, embalar os produtos já vendidos e separá-los para transporte.



RESUMO DO TÓPICO 2

Neste tópico, você aprendeu que:

- Aos poucos, a tecnologia RFID vem substituindo a leitura de código de barras e facilitando as operações de estoque. Portanto, é importante entender quais são os itens que compõem esse sistema e de que forma a informação é transmitida por radiofrequência.



- 1 A tecnologia de RFID é uma ferramenta que vem sendo cada vez mais utilizada na gestão de armazenamento. Pode-se afirmar que o conceito de RFID corresponde:
 - a) ☐ à tecnologia capaz de emitir uma onda de rádio que é capturada, revelando as informações de rastreabilidade de itens.
 - b) ☐ à tecnologia específica para fazer leitura em etiquetas de código de barras.
 - c) ☐ à tecnologia capaz de realizar a previsão orçamentária da empresa, a gestão de competências ou a escolha do tipo de orçamento.
 - d) ☐ ao sistema de avaliação de competências e habilidades na gestão de pessoas.
 - e) ☐ à tecnologia de análise de dados para orçamento base zero.

- 2 Há diversos benefícios na implantação do RFID. Dentre as alternativas a seguir, destaque a que indica os benefícios primários do uso de RFID na gestão do armazenamento.
 - a) ☐ Eliminação de erros dos lançamentos de balanço patrimonial da empresa.
 - b) ☐ Economia de recursos de salários e impostos, bem como despesas operacionais no armazém.
 - c) ☐ Eliminação de erros de escrita e de leitura de dados, bem como coleção de dados de forma mais rápida e automática.
 - d) ☐ Ganhos de educação corporativa com desenvolvimento de competências gerenciais.
 - e) ☐ Aumento de remuneração para os gestores operacionais do armazém.

- 3 A tecnologia RFID é muito utilizada na gestão de estoque. Os estoques que têm suas diretrizes baseadas em uso de RFID caracterizam-se por:
 - a) ☐ necessidade de baixo investimento.
 - b) ☐ menos agilidade para o processo.
 - c) ☐ mais pessoas manuseando os produtos.
 - d) ☐ potencial para elevar a eficiência em custos e nível de serviço.
 - e) ☐ foco total no controle de custos.

- 4 As etiquetas inteligentes RFID podem ser implantadas em paletes que contêm produtos industrializados, cujas informações contemplam:

- a) () resultados operacionais do armazém.
- b) () códigos de barras impressos para leitura manual.
- c) () validade, origem, destino e quantidades consolidadas.
- d) () indicadores de qualidade de prazo de entrega do varejo.
- e) () controle da receita da empresa.

5 Quanto à automação do processo de estocagem, é necessário avaliar a viabilidade financeira dos investimentos devido a alguns critérios, tais como:

- a) () salário dos motoristas da frota.
- b) () alto custo de mão de obra.
- c) () layout dos escritórios da planta.
- d) () níveis de varejo do processo logístico.
- e) () sistema de ouvidoria externa do armazém.

BIG DATA E INTERNET DAS COISAS (IoT)

1 INTRODUÇÃO

Com o avanço da tecnologia e a utilização cada vez maior da internet em todo mundo, torna-se necessário aprimorar os serviços prestados pela tecnologia da informação (TI). Diante desse contexto, os conceitos conhecidos como Big Data e Internet das Coisas (IoT), ocupam um papel de destaque nas discussões relacionadas aos avanços em diversas áreas. Tanto o tratamento de grandes volumes de dados (Big Data) como a conectividade de dispositivos auxiliando no cotidiano das pessoas (IoT), são temas recentes e que têm muito a evoluir em termos de discussões das suas aplicações.

Neste tópico, aprenderemos sobre as características das tecnologias chamadas de Big Data e IoT.

2 CONCEITO DE BIG DATA

Atualmente, o tema Big Data desperta o interesse em todas as pessoas que têm algum envolvimento com atividades relacionadas à gestão da informação. Porém, quem não tem afinidade com a TI pode ter dificuldades para entender do que se trata. A princípio, podemos definir o conceito de Big Data como conjuntos de dados extremamente amplos e que, por esse motivo, necessitam de ferramentas preparadas para lidar com grandes volumes de dados, de forma que toda e qualquer informação nesses meios possa ser encontrada, analisada e aproveitada em tempo hábil.

Com o aumento significativo da quantidade de dados gerados pela internet e com o surgimento das mídias sociais, é necessário gerenciar e armazenar as informações de maneira organizada. Esses dados podem ser classificados em estruturados, não estruturados e semiestruturados, com base no seu gerenciamento e armazenamento.

3 DADOS ESTRUTURADOS

Dados estruturados são aqueles que possuem formato e comprimento definido, por exemplo, números, datas e grupos de palavras. Em geral, uma base de dados usada em sistemas informatizados convencionais é organizada de forma que se tenham dados armazenados em estruturas tubulares, nas quais as linhas armazenam uma ocorrência de um evento, caracterizado por um conjunto de colunas que representam características que descrevem um exemplar (instância) daquele evento.

Na maioria dos casos, os dados estruturados são resultados de processos de geração de dados inerente a sistemas transacionais ou resultantes de observações e processos de medição. Esses dados, geralmente, são armazenados em um conjunto de tabelas relacionadas entre si.

4 DADOS NÃO ESTRUTURADOS

Dados não estruturados são aqueles que não seguem um formato específico, por exemplo, imagens de satélite, dados científicos, fotografias e vídeos, texto próprio de empresas e dados de mídias sociais. Esse tipo de dado requer dispositivos de armazenamento e processamento, que suportem seu formato e garantam melhor eficiência em suas análises.

5 DADOS SEMIESTRUTURADOS

Pode-se definir dados semiestruturados como um meio termo entre a estruturação e total falta de estruturação. Como exemplo de dados semiestruturados, temos os conteúdos disponibilizados na Web acompanhados de tags e arquivos XML.

6 ANÁLISE DE DADOS

A coleta e o armazenamento de dados têm como finalidade a extração de informações que possam gerar vantagens competitivas para as organizações, bem como auxiliar nas tomadas de decisões. Os diversos dispositivos conectados à internet produzem dados das mais variadas formas. Porém, dados, mesmo que em um grande volume, não passam de dados. É necessário gerar informação e conhecimento para explorar os benefícios desses dados brutos, ou seja, os dados necessitam ser analisados.

Os sistemas gerenciais têm como característica o fato de apresentarem as informações, mas a inteligência nos negócios converge para a análise detalhada dos dados, a procura de padrões, modelos ou repetições. Se não

forem encontrados padrões, fica complicado afirmar quais eventos geram determinadas consequências. Isso gera uma confusão de dados desordenados e sem explicações. Diante desse contexto, existem três tipos de análises que podem ser aplicadas aos dados, conforme você verá a seguir.

- **Análise exploratória:** permite a compreensão de como os dados estão distribuídos e qual o formato em que se encontram. A informação adquirida nas análises exploratórias serve de apoio na tomada de decisão sobre o tipo de tarefa de mineração dos dados e na escolha do algoritmo.
- **Análise preditiva:** prevê resultados futuros com base em dados do passado. Pode ser entendida como um processo que permite descobrir o relacionamento existente entre os exemplares de um conjunto de dados, descritos por uma série de características e rótulos atribuídos a esses dados.
- **Análise de agrupamento:** consiste no agrupamento de objetos de acordo com suas características. Também é conhecida como clustering e permite, com base em um conjunto de características, a descoberta de relações existentes entre exemplares de conjuntos de dados.
- **Regras de associação:** procurar encontrar padrões ou relacionamentos que aparecem com frequência em bases de dados.

7 5V'S DO BIG DATA

O principal objetivo do desenvolvimento de soluções de Big Data é oferecer uma abordagem consistente no tratamento do constante crescimento e da complexidade dos dados. Para isso, você precisa considerar o conceito dos 5 V's do Big Data: o volume, a velocidade, a variedade, a veracidade e o valor.

- **Volume:** trata-se do volume diário de troca de e-mails, transações bancárias, interações em redes sociais, registro de chamadas e tráfego de dados em linhas telefônicas. Essas situações servem de ponto de partida para a compreensão do volume de dados presentes no mundo atual. É importante também compreender que o conceito de volume é relativo à variável tempo, ou seja, o que é grande hoje, pode não ser nada amanhã.
- **Velocidade:** as empresas necessitam de dados atuais sobre seus negócios, por isso a importância da velocidade é tamanha e, em algum momento, deverá existir uma ferramenta capaz de analisar os dados em tempo real. Atualmente, os dados são analisados somente após serem armazenados, mas o tempo gasto para o armazenamento em si já desclassifica esse tipo de análise como uma análise 100% em tempo real. A velocidade com a qual você obtém essa informação é uma vantagem competitiva das empresas. A velocidade pode limitar a operação de muitos negócios, quando utilizamos o cartão de crédito, por exemplo, se não obtivermos uma aprovação da compra em alguns segundos, pensamos em utilizar outro método de pagamento. É a operadora perdendo uma oportunidade de negócios pela falha na velocidade de transmissão e análise dos dados do comprador.

- **Variedade:** diferentemente do passado, hoje em dia os dados não são estruturados e armazenados em tabelas relacionais, pois uma grande variedade de dados como mensagens, fotos, vídeos e sons torna mais complexa a análise desses dados. Os dados não estruturados podem ser administrados juntamente aos dados tradicionais.
- **Veracidade:** para colher bons frutos do processo do Big Data é necessário obter dados verídicos, de acordo com a realidade. O conceito de velocidade, já descrito, é bem alinhado ao conceito de veracidade pela necessidade constante de análise em tempo real, isso porque dados passados não podem ser considerados dados verídicos para o momento da análise.
- **Valor:** quanto maior for a riqueza de dados, mais importante será saber realizar as perguntas certas no início de todo o processo de análise. É necessário estar focado para a orientação do negócio, o valor que a coleta e a análise dos dados trarão para o negócio. Não é viável realizar todo o processo de Big Data se não se tem questionamentos que ajudem o negócio de modo realístico.

8 TECNOLOGIAS PARA O BIG DATA

As tecnologias que sustentam o Big Data podem ser categorizadas sob duas perspectivas, as ferramentas de análise (analytics) e as tecnologias de infraestrutura, que servem para processar e armazenar os grandes volumes de dados. O Big Data não se resume a um grande volume de dados não estruturados, ele também inclui as tecnologias que possibilitam o processamento e a análise dos dados. A tecnologia associada ao Big Data possibilita a criação de modelos estatísticos que servem para otimizar e prever os dados. A seguir, você verá uma relação de algumas tecnologias referentes ao Big Data.

Hadoop: plataforma de software em Java de computação distribuída voltada para clusters e processamento de grandes volumes de dados, com suporte a tolerância a falhas.

- Map Reduce: é um framework desenvolvido pela Google para suportar computações paralelas em grandes coleções de dados em clusters de computadores.
- Linguagens de Script: linguagens de programação adequadas ao Big Data, como Python.
- Visual Analytics: método de análises em grandes volumes de dados com saída em formato visual ou gráfico.
- Processamento de Linguagem Natural (PLN): conceito de inteligência artificial que permite a análise de textos.
- In-memory analytics: processamento de Big Data realizado na memória do computador com o objetivo de aumentar a velocidade das análises.

No que se refere à infraestrutura, as arquiteturas de hardware atuais auxiliam no processamento de dados com serviços especializados para Big Data. O advento da tecnologia In-memory analytics colabora muito com a velocidade de processamento, pois evita que os dados sejam armazenados em disco.

9 INTERNET DAS COISAS (IoT)

O termo IoT, do inglês Internet of Things e que é traduzido como Internet das Coisas, é utilizado para transmitir a ideia de que a internet pode estar presente em todas as coisas. A ideia por trás do conceito é que todos equipamentos podem estar conectados a internet e, assim, facilitar a vida das pessoas no seu dia a dia.

O conceito de IoT é baseado na ideia de fusão do mundo real com o mundo digital, fazendo os indivíduos estarem em constante comunicação e interação com outras pessoas e objetos. A IoT possui funções de reconhecimento inteligente, localização, rastreamento e gerenciamento dos diversos dispositivos, trocando informações a todo o momento.

A IoT deve permitir uma conexão autônoma e segura para troca de dados entre os dispositivos e aplicações do mundo real, utilizando a internet para comunicação, troca de informações, tomada de decisões e invocação de ações. A tendência é que sejam oferecidos serviços surpreendentes, baseados no conceito de IoT. Assim, esse tema se torna muito relevante em instituições acadêmicas, na indústria e para as organizações governamentais, pois a IoT tem um potencial significativo de proporcionar melhorias em questões sociais, profissionais e econômicas.

10 ARQUITETURA DA IOT

Ainda não foi definida uma arquitetura universal para IoT, devido ao fato de que as aplicações desenvolvidas funcionam em uma arquitetura de rede, quase que exclusivamente orientada à aplicação. As aplicações de IoT precisarão se integrar com outros sistemas e aí é que surgem os desafios relacionados à falta de interoperabilidade, ou seja, as aplicações possuem arquiteturas distintas. Para se atingir o nível de integração que a IoT irá demandar, será necessário uma base comum para construção de sub arquiteturas, ou seja, um conjunto comum de blocos de construção, para o desenvolvimento da arquitetura do sistema, que garantirá interoperabilidade em vários níveis.

Diante desse cenário, diversas empresas que compõem a Standards Development Organizations (SDO), que atua no desenvolvimento de padrões, se uniram para formar uma arquitetura genérica para IoT, a oneM2M, cujo principal objetivo é desenvolver especificações para garantir a funcionalidade global dos sistemas.

A arquitetura básica M2M possui três tipos de camadas:

- camada de aplicação;
- camada de serviços comuns;
- camada de serviços de rede.

A camada de aplicação engloba os elementos de ponta como sensores, geolocalizadores, smartphones, e formam a chamada entidade de aplicação. Essa entidade, implementa uma ou mais lógicas de serviços, que são reconhecidos por uma identificação exclusiva, o que permite que uma solicitação de uma lógica de serviço faça uso do aplicativo desenvolvido para se comunicar.

Na camada de serviços comuns, existe uma outra entidade chamada de entidade de serviços comuns. Essa entidade representa uma solicitação de um conjunto de funções comuns, utilizando uma arquitetura funcional. A camada de aplicação interage com a camada de serviços comuns por meio de bibliotecas de desenvolvimento (API).

As especificações desenvolvidas pela M2M serviram como um projeto estrutural comum para redes e sistemas para executar um amplo conjunto de aplicações e pretendiam desenvolver uma camada de serviço comum, que facilitasse a interoperabilidade entre redes de sensores, dispositivos e aplicativos baseados em nuvem.

11 ELEMENTOS DA IOT

A implementação de soluções para IoT é constituída por redes heterogêneas e amplamente distribuídas. Uma importante característica dessas redes é a identificação por radiofrequência, sensores, tecnologias inteligentes e nanotecnologias, que são importantes para que exista uma grande variedade de serviços. A rede utilizada em IoT abrange uma infraestrutura que inclui softwares, hardware e serviços, que serão utilizados para dar suporte às redes de comunicação. Os elementos físicos podem trocar dados sobre as suas propriedades devido à integração física.

A identificação de dispositivos pode ser realizada por meio de tecnologias de identificação, como radio-frequency identification (RFID). O RFID é um método que permite a identificação automática e a captura de dados utilizando campos eletromagnéticos que identificam e rastreiam etiquetas anexadas aos objetos. A tecnologia RFID utiliza um chipset que armazena os dados exclusivos e os recursos de segurança disponíveis. O chip possui uma antena que o permite receber energia e que sejam transmitidas informações. As etiquetas contêm informações eletrônicas e não necessitam estar visualmente alinhadas com um equipamento leitor, além de poderem ser divididas em etiquetas passivas, que recebem energia a partir das ondas de rádio de um leitor RFID próximo. As etiquetas ativas possuem fonte de energia local, como uma bateria, e podem operar a centenas de metros do leitor RFID.

Equipamentos como sensores e atuadores são extremamente importantes para a coleta e saída de dados, e têm a capacidade de permitir que os dispositivos conectados se comportem de forma autônoma. Atualmente, esses equipamentos são capazes de permitir a tomada de decisões inteligentes.

As redes de comunicação utilizadas para IoT são comuns e conhecidas: Wi-Fi, Bluetooth e near field communication (NFC). Porém, essas redes possuem alcance limitado e determinadas aplicações dependem de redes móveis como 3G e 4G. As redes móveis atuais (2G, 3G e 4G) são direcionadas a dispositivos como smartphones, tablets e laptops. O foco está sobre aplicações de texto, voz, imagem e vídeo. Esse aspecto não impede as redes atuais de serem utilizadas para IoT, mas uma otimização para dispositivos variados é necessária, principalmente para garantir o baixo consumo de energia e de recursos de processamento. Isso deve vir com a próxima onda de redes móveis, o 5G (quinta geração).

Com a eminente difusão da IoT, temos sensores, chips e dispositivos relacionados por todos os lados. Todos esses itens precisam estar conectados. Com a tecnologia de endereçamento de rede IPv6, que oferece um número extremamente elevado de endereços para os dispositivos, conectar esses dispositivos não será problema. A limitação vem das tecnologias de comunicação: as redes atuais não foram projetadas para permitir tantas conexões de dispositivos tão distintos. Por isso, a rede 5G terá um papel importante para IoT, pois, além de proporcionar uma velocidade bastante elevada para transmissão de dados, permitirá, por exemplo, que cada dispositivo baseado em IoT utilize apenas os recursos necessários, sempre na medida exata. Isso evitará gargalos na rede, assim como desperdício de energia (um grave problema em dispositivos que usam bateria).

12 RISCOS ASSOCIADOS À IOT

A IoT possibilita inúmeras oportunidades e conexões, muitas das quais não conseguimos imaginar nem entender seu impacto nos dias de hoje. É fácil perceber por que esse assunto tem sido tão comentado atualmente, ele certamente abre portas para muitas oportunidades, mas também muitos desafios.

Com a grande quantidade de dispositivos conectados surge um cenário que impõe alguns riscos. Parâmetros preventivos e corretivos já estão sendo estudados, e o foco principal são as ameaças relacionadas à segurança e privacidade. Os riscos não são apenas individuais, problemas de ordem coletiva também podem ocorrer. Um exemplo do cotidiano é a conectividade dos semáforos, que, quando interconectados, podem causar problemas de congestionamentos e caos nas cidades em caso de falhas.

A indústria tem um papel importante na definição de critérios que garantam a disponibilidade dos serviços, proteção das comunicações, normas de privacidade, confidencialidade e integridade dos dados. Todos esses aspectos tornam a tarefa mais complexa do que o trivial. Além das questões tecnológicas, ainda existem desafios relacionados às convenções globais e legislação dos países.

Outro aspecto que não pode ser esquecido no contexto de IoT é a transparência, ou seja, deixar claro para empresas e usuários os riscos associados à IoT. Além disso, orientações relacionadas às questões de segurança também devem ser realizadas.



RESUMO DO TÓPICO 3

Neste tópico, você aprendeu que:

- Para que seja possível a difusão das soluções baseadas em IoT, é necessário que existam padrões de desenvolvimento das soluções, ou seja, uma arquitetura que permita aos fabricantes desenvolverem as soluções com a garantia de que funcionem corretamente independentemente do hardware utilizado.



1 Qual dos conceitos a seguir é o mais adequado para definir Big Data?

- a) () Big data é um grande volume de dados disponíveis de forma estruturada ou não, oriundo de diversas fontes, sejam internas ou externas à organização, e acessíveis em alta velocidade que exigem formas inovadoras de processamento para uso em tomada de decisões.
- b) () Big data é um conjunto de dados fortemente estruturados, que servem para orientar equipamentos de automação em relação as suas tarefas básicas.
- c) () Big data é uma sequência finita de instruções bem definidas e não ambíguas, cada uma das quais devendo ser executada mecânica ou eletronicamente em um intervalo de tempo finito e com uma quantidade de esforço finita.
- d) () Big data é uma rede de objetos físicos, veículos, prédios e outros elementos que possuem tecnologia embarcada, sensores e conexão com rede capaz de coletar e transmitir dados.
- e) () Big data é a linguagem de pesquisa declarativa padrão para banco de dados relacional.

2 Qual das tecnologias a seguir representa um tipo de conexão utilizado em equipamentos que compõem soluções baseadas no conceito de IoT?

- a) () Intel Dual Core.
- b) () Bluetooth.
- c) () SQL.
- d) () Oracle.
- e) () ARPNET.

3 A arquitetura mais geral definida para IoT é composta por três elementos básicos. São eles:

- a) () Entrada, processamento e saída.
- b) () Rede lógica, rede física e protocolo de rede.
- c) () Percepção/atuação, rede e aplicação.
- d) () Integridade, veracidade e confiabilidade.
- e) () Gestão, operação e análise.

4 Pode-se afirmar que os dados gerados para análises baseadas em Big Data na Internet são classificados como:

- a) () Estruturados.
- b) () Estruturados ou arrançados.
- c) () Estruturados, não estruturados ou semiestruturados.
- d) () Dados brutos.
- e) () Dados brutos e dados binários.

5 Dentre as tecnologias de comunicação utilizadas em IoT, as mais conhecidas são:

- a) () Banco de dados, processador e memória.
- b) () Notebook, smartphone e tablets.
- c) () HDMI, VGA e DVI.
- d) () Rede coaxial, intranet e extranet.
- e) () Wi-Fi, zigbee, bluetooth e 3G/4G.

REFERÊNCIAS

3GPP. **Specifications**. 2020. Disponível em: <https://www.3gpp.org/specifications>. Acesso em: 25 abr. 2020.

ADHIARNA, N.; RHO, J. J. Standardization and global adoption of Radio Frequency Identification (RFID): Strategic issues for developing countries. *In: INTERNATIONAL CONFERENCE ON COMPUTER SCIENCES AND CONVERGENCE INFORMATION TECHNOLOGY*, 4., 2009. **Anais eletrônicos...** Disponível em: <https://www.researchgate.net/publication/232653086>. Acesso em: 25 abr. 2020.

ALBISHI, S. *et al.* Challenges and solutions for applications and technologies in the internet of things. **Procedia Computer Science**, Amsterdam, v. 124, p. 608-614, 2017.

ALHALAFI, N.; VEERARAGHAVAN, P. Privacy and security challenges and solutions in IOT: a review. *In: INTERNATIONAL CONFERENCE ON SMART POWER & INTERNET ENERGY SYSTEMS*, 2019, Melbourne. **Anais eletrônicos** [...] Melbourne: IOP Conference Series: Earth and Environmental Science, 2019. Disponível em: <https://iopscience.iop.org/article/10.1088/1755-1315/322/1/012013/pdf>. Acesso em: 7 maio 2020.

ALI, I.; SABIR, S.; ULLAH, Z. Internet of things security, device authentication and access control: a review. **International Journal of Computer Science and Information Security**, [s. l.], v. 14, n. 8, p. 456-466, ago. 2016.

ARAÚJO, T. **Raspberry Pi B+**: Introdução a Porta GPIO. Fazedores, 24 out. 2014. Disponível em: <https://blog.fazedores.com/raspberry-pi-b-introducao-porta-gpio/>. Acesso em: 3 jan. 2020.

ARDUINO. **Arduino uno wifi rev2**. 2019a. Disponível em: <https://store.arduino.cc/usa/arduino-uno-wifi-rev2>. Acesso em: 24 mar. 2019.

ARDUINO. **Arduino mkr wifi 1010**. 2019b. Disponível em: <https://store.arduino.cc/usa/mkr-wifi-1010>. Acesso em: 24 mar. 2019.

ARDUINO. **Arduino yún**. 2019c. Disponível em: <https://store.arduino.cc/usa/arduino-yun>. Acesso em: 24 mar. 2019.

ARDUINO. **What is Arduino?** 2019d. Disponível em: <https://www.arduino.cc>. Acesso em: 24 mar. 2019.

BANZI, M.; SHILOH, M. **Primeiros Passos com o Arduino**. 2. ed. São Paulo: Novatec, 2015. 240p.

BURHAN, M. *et al.* IoT elements, layered architectures and issues: a comprehensive survey. **Sensors**, Basileia, v. 18, n. 9, ago. 2018. Disponível em: <https://www.researchgate.net/publication/327272757IoTElementsLayeredArchitecturesandSecurityIssuesAComprehensiveSurvey>. Acesso em: 7 maio 2020.

BUYA, R.; DASTJERDI, A. V. (ed.). **Internet of Things: principles and paradigms**. New York: Elsevier, 2016.

CARISSIMI, A. S.; ROCHOL, J.; GRANVILLE, L. Z. **Redes de computadores**. Porto Alegre: Bookman, 2009. (Série Livros Didáticos Informática UFRGS, v. 20).

CHEN, J. *et al.* **China' Internet of Things**: research report prepared on behalf of the U.S.- China Economic and Security Review Commission. Washington, 2018. Disponível em: <https://www.uscc.gov/research/chinas-internet-things>. Acesso em: 25 abr. 2020.

CHOI, J. *et al.* A general consensus algorithm for wireless sensor networks. *In*: WIRELESS ADVANCED (WIAD), 2012, London. **Anais [...]** [s. l.]: IEEE. 2012. p. 16-21.

COMER, D. E. **Redes de computadores e internet**. 6. ed. Porto Alegre: Bookman, 2016.

COMO funciona a radiofrequência. **Jornal do Comércio**, Porto Alegre, RS, 7 dez. 2017. Disponível em: https://www.jornaldocomercio.com/_conteudo/2017/12/cadernos/jc_logistica/599976-como-funciona-a-radiofrequencia.html. Acesso em: 8 mar. 2019.

CONDEA, C.; THIESSE, F.; FLEISCH, E. RFID-enabled shelf replenishment with backroom monitoring in retail stores. **Decision Support Systems**, v. 52, n. 4, p. 839-849, 2012.

DEAN, A.; AGYEMAN, M. O. A study of the advanced in IoT security. *In*: INTERNATIONAL SYMPOSIUM ON COMPUTER SCIENCE AND INTELLIGENT CONTROL, 2., 2018, Stockholm. **Anais eletrônicos [...]** New York: Association for Computing Machinery, 2018. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3284557.3284560>. Acesso em: 6 mai. 2020.

DRESCH, A.; EFROM, D. R.; GRUMOVSKI, D. Controle de patrimônio por sistema wireless (RFID). **Revista E-Tech**, v. 1, n. 1, p. 47-57, 2008.

EBERMAM, E. *et al.* **Programação para leigos com Raspberry Pi**. João Pessoa: Edifes, 2017.

EL HAKIM, A. **Internet of Things (IoT) system architecture and technologies**. Egito, 2018. Disponível em: <https://www.researchgate.net/publication/323525875>. Acesso em: 25 abr. 2020.

ESP32. **What is ESP32?** 2018. Disponível em: <http://arduinoinfo.mywikis.net/wiki/Esp32>. Acesso em: 24 mar. 2019.

ESP8266. **What is ESP8266?** 2019. Disponível em: <https://en.wikipedia.org/wiki/ESP8266>. Acesso em: 24 mar. 2019.

ESPRESSIF SYSTEMS. **ESP32 WROOM 32 Datasheet**. 2015. Disponível em: <https://www.espressif.com/sites/default/files/documentation/esp32-wroom-32datasheeten.pdf>. Acesso em: 24 mar. 2019.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. Porto Alegre: AMGH; Bookman, 2008. 1134 p.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de computadores**. Porto Alegre: McGrawHill, 2013.

GARCIA, P. S. R.; KLEINSCHMIDT, J. H. Tecnologias emergentes de conectividade na IoT: estudo de redes LPWAN. In: SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES E PROCESSAMENTO DE SINAIS, 35., 2017, São Pedro. **Anais [...]**. São Paulo, 2017. Disponível em: <http://www.sbrt.org.br/sbrt2017/anais/1570361881.pdf>. Acesso em: 16 ago. 2019.

GENG, H. **Internet of things and data analytics handbook**. Palo Alto: Wiley, 2017.

GOULART, A. **Acesso remoto via RDP no Raspberry Pi**. 2014. Disponível em: <https://ange-litomg.com/blog/acesso-remoto-via-rdp-no-raspberry-pi>. Acesso em: 5 maio 2020.

HARTE, L. **Introduction to Bluetooth: Technology, Operation, Profiles, and Services** 2nd Edition. DiscoverNet, 2009. 102p.

HAWKINS, M. **Simple Guide to the Raspberry Pi GPIO Header**. Raspberry Pi, 9 jun. 2012. Disponível em: <https://www.raspberrypi-spy.co.uk/2012/06/simple-guide-to-the-rpi-gpio-header-and-pins/>. Acesso em: 3 jan. 2020.

HAYES, C. Managing power in the IoT with cellular LPWAN technology. In: ELETRONIC SPECIFIER. 2020. Disponível em: <https://www.electronicsspecifier.com/news/analysis/managing-power-in-the-iot-with-cellular-lpwan-technology>. Acesso em: 25 abr. 2020.

HAYLER, R. **Build your own weather station with our new guide! Raspberry Pi Foundation**, 2018. Disponível em: <https://www.raspberrypi.org/blog/build-your-own-weather-station/>. Acesso em: 3 jan. 2020.

HC Serial Bluetooth Products-User Instructional Manual. [S. l.], 29 jan. 2010. Disponível em: https://cdn.makezine.com/uploads/2014/03/hc_hc-05-user-instructions-bluetooth.pdf. Acesso em: 27 fev. 2019.

HENRIQUE, C. **Lançado o Raspbian 2016-02-06, baixe agora!** Ferramentas Linux, 15 fev. 2016. Disponível em: <https://portallinuxferramentas.blogspot.com/2016/02/lançado--o-raspbian-2016-02-06-baixe.html>. Acesso em: 3 jan. 2020.

HEYDON, R. **Bluetooth Low Energy: The Developer's Handbook 1st Edition**. Prentice Hall, 2012. 368p.

HUANG, A. **Bluetooth Essentials for Programmers 1st Edition**. Cambridge University Press, 2007. 212p.

IEEE 802.15.1. [S. l.], 14 jun. 2002. Disponível em: <http://www.ieee802.org/15/pub/TG1.html>. Acesso em: 26 fev. 2019.

IPV6. **Cabeçalho**. 2012. Disponível em: <https://ipv6.br/post/cabecalho/>. Acesso em: 4 mar. 2020.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet: uma abordagem top-down**. 3. ed. São Paulo: Pearson Addison Wesley, 2007. 634 p.

KUROSE, J. F.; ROSS, K. W.; ZUCCHI, W. L. **Redes de computadores e a internet: uma abordagem top-down**. São Paulo: Pearson Addison Wesley, 2013.

LI, S.; TRYFONAS, T.; LI, H. **The internet of things: a security point of view**. Internet Research, Bingley, v. 26, n. 2, p. 337-359, 2016.

LU, Y.; PAPAGIANNIDIS, S.; ALAMANOS, E. Internet of things: a systematic review of the business literature from the user and organizational perspectives. **Technological Forecasting and Social Change**, v. 136, p. 285-297, 2018. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0040162518301136?via%3Dihub>. Acesso em: 16 ago. 2019.

MADEIRA, D. **Projeto Raspberry Pi 3 no acionamento de lâmpadas**. 2018. Disponível em: <https://www.usinainfo.com.br/blog/utilizando-o-raspberry-pi-3-no-acionamento-de--lampadaspronto-post-de-automacao-residencial/>. Acesso em: 5 maio 2020.

MARGOLIS, M. **Make an Arduino-Controlled Robot** (Make: Projects). Sebastopol CA (EUA): Maker Media, Inc, 2012. 256p.

MARKETS AND MARKETS. **Machine-to-Machine (M2M) Connections Market by Technology (Wired, Wireless), Industry (Healthcare, Utilities, Retail, Consumer Electronics, Automotive & Transportation, Security & Surveillance), and Geography: global forecast to 2023**. 2020. Disponível em: <https://www.marketsandmarkets.com/Market-Reports/machine-to-machine-market-732.html>. Acesso em: 25 abr. 2020.

MCROBERTS, M. **Arduino básico**. São Paulo: Novatec, 2011. 453p.

MEKKI, K. *et al.* **A comparative study of LPWAN technologies for large-scale IoT deployment**. ICT Express, 2018. Disponível em: <https://doi.org/10.1016/j.ict.2017.12.005>. Acesso em: 25 abr. 2020.

MELO, P. Padrão IEEE 802.15.4: a base para as especificações Zigbee, WirelessHart e MiWi. *In: EMBARCADOS*. [S. l., 2020?]. Disponível em: <https://www.embarcados.com.br/padrao-ieee-802-15-4/>. Acesso em: 25 abr. 2020.

MENDONÇA, H. S. **Serial**. [2015]. Disponível em: <https://paginas.fe.up.pt/~hsm/docencia/edm/edm-201516/serial/>. Acesso em: 5 maio 2020.

MONK, S. **Projetos com Arduino e Android** - Use seu Smartphone ou Tablet para Controlar o Arduino - Série Tekne. Porto Alegre: Bookman, 2013. 212p.

MORAES, A. **Redes de computadores**. São Paulo: Érica, 2014.

MUNDO ELETRÔNICA. **Novo Raspberry Pi 3 (pi3)**: Quadcore 1.2ghz (10x+rapido) 1gb.c2020. Disponível em: <https://www.mundoeletronica.com.br/produtos/novo-raspberry-pi-3-pi3-quadcore-1-2ghz-10xrapido-1gb1/>. Acesso em: 15 maio 2020.

OLIVEIRA, S. **Internet das coisas**: com ESP8266, Arduino e Raspberry PI. São Paulo: No-vatec, 2017.

PERSIA, S.; REA, L. Next Generation M2M Cellular Networks: LTE-MTC and NB-IoT Capacity analysis for smart grids applications. *In: AEIT International Annual Conference (AEIT)*, 2016. **Anais...** [S. l.]: IEEE, 2016.

PIPPLEWARE. **RetroPie**. 2015. Disponível em: <http://pipplware.pplware.pt/wiki/retropie/>. Acesso em: 3 jan. 2020.

POZO, H. **Administração de recursos materiais e patrimoniais**: uma abordagem logística. 3. ed. São Paulo: Atlas, 2004.

RAHIM, M. R. B. A. *et al.* Service-oriented architecture for IoT home area networking in 5G. *In: AL-DULAIMI, A.; WANG, X.; I, CHIH-LIN. 5G Networks*: fundamental requirements, enabling technologies and operations management. Hoboken: Wiley: 2018. p. 577-602.

RAJ, P.; RAMAN, A. C. **The Internet of Things**: enabling technologies, platforms and use cases. Boca Raton: CRC Press, 2017.

RASPBERRY PI FOUNDATION. **GPIO**. [2019?]a. Disponível em: <https://www.raspberrypi.org/documentation/usage/gpio/README.md>. Acesso em: 5 maio 2020.

RASPBERRY PI FOUNDATION. **GPIO in Python**. [2019?]b. Disponível em: <https://www.rasp-berrypi.org/documentation/usage/gpio/python/README.md>. Acesso em: 5 maio 2020.

RASPBERRY PI ROBOTICS. **Raspberry Pi GPIO Access**. 2019. Disponível em: <https://www.raspberrypi.org/products/>. Acesso em: 3 jan. 2020.

RASPBERRY PI FOUNDATION. **Raspberry Pi 4**. 2019a. Disponível em: <https://www.raspberrypi.org/products/raspberry-pi-4-model-b/>. Acesso em: 3 jan. 2020.

RASPBERRY PI FOUNDATION. **Products**. 2019b. Disponível em: <https://www.raspberrypi.org/products/>. Acesso em: 3 jan. 2020.

RFID como tecnologia de identificação. **PUC-Rio**, Rio de Janeiro, RJ, [2018?]. Disponível em: https://www.maxwell.vrac.puc-rio.br/31906/31906_4.PDF Acesso em 7 fev. 2019.

RICHARDSON, M.; WALLACE, S. **Primeiros passos com o Raspberry PI**. São Paulo: Novatec, 2013.

ROMKEY, J. Toast of the IoT: the 1990 interop internet toaster. **IEEE Consumer Electronics Magazine**, v. 6, n. 1, p. 116-119, 2017.

SANTINI, A. G. RFID: conceitos, aplicabilidades e impactos. Rio de Janeiro: Ciência Moderna, 2008.

SANTOS, G. A. *et al.* Internet of Things (IoT): Um cenário guiado por patentes industriais. **Revista Gestão.Org**, v. 13, nesp., p. 271–281, 2015. Disponível em: <https://periodicos.ufpe.br/revistas/gestaoorg/article/download/22134/18499>. Acesso em: 25 abr. 2020.

SANTOS, M.; MANHÃES, A. M.; LIMA, A. R. Indústria 4.0: desafios e oportunidades para o Brasil. In: SIMPÓSIO DE ENGENHARIA DE PRODUÇÃO DE SERGIPE, 10., 2018, São Cristóvão, SE. **Anais...** São Cristóvão, SE, 2018. p. 317 - 329. Disponível em: <http://ri.ufs.br/jspui/handle/riufs/10423>. Acesso em: 24 mar. 2019.

SENAI. **Automação logística**. Vitória: SENAI-ES, 2014. Disponível em: https://teclog.files.wordpress.com/2015/02/2_g12_ap-automacao-logistica_aut_log.pdf. Acesso em: 8 mar. 2019.

SNAPDRAGON TECH BLOG. **Raspberry Pi as Budget BitTorrent Server**. 15 ago. 2012. Disponível em: <https://blog.snapdragon.cc/2012/06/29/raspberry-pi-as-bittorrent-server/>. Acesso em: 3 jan. 2020.

TANENBAUM, A. S. **Redes de computadores**. Rio de Janeiro: Campus, 1997.

TANENBAUM, A. S.; WETHERALL, D. J. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011. 600 p.

TECNOTRONICS. **Como acender um LED usando o Raspberry Pi**. 2017. Disponível em: <https://www.tecnotronics.com.br/acender-um-led-usando-o-raspberry-pi/>. Acesso em: 5 maio 2020.

TRIPATHY, B. K; ANURADHA, J. **Internet of things (IoT): technologies, applications, challenges and solutions**. Boca Raton: CRC Press, 2018.

UPTON, E.; HALFACREE, G. **Raspberry Pi: guia do usuário**. Rio de Janeiro: Alta Books, 2017.

UPTON, E.; HALFACREE, G. **Raspberry Pi user guide**. Chichester, England: John Wiley & Sons, 2014.

VERMESAN, O.; FRIESS, P. (ed.). **Internet of Things applications: from research and innovation to market deployment**. [S. l.]: River Publishess, 2014. Disponível em: <http://www.internet-of-things-research.eu/pdf/IERCClusterBook2014Ch.3SRIAWEB.pdf>. Acesso em: 25 abr. 2020.

VISSER, H. J. **Teoria e aplicações de antenas**. Rio de Janeiro: LTC, 2015.

ZHOU, H. **The Internet of Things in the cloud: a middleware perspective**. Boca Raton: CRC Press, 20