Tópico 13

Tecnologia de Redes

Autor: Wu Shin-Ting

DCA - FEEC - Unicamp

Outubro de 2019

Vimos no Capítulo 7 uma variedade de transdutores que poderiam estar integrados nos diferentes sistemas para amostrar os fenômenos físicos que nos cercam. No Capítulo 8, mostramos os circuitos conversores que permitem a conversão entre os sinais analógicos do mundo físico e os sinais digitais processáveis pelos microprocessadores. No Capítulo 10 mostramos que os microcontroladores, com a sua capacidade de realizar de forma eficiente tarefas bem específicas em condições de operação adversas, são circuitos eletrônicos extremamente apropriados para processarem de forma dedicada os dados de entrada e saída. Vimos ainda no Capítulo 9 conceitos relacionados com os barramentos internos nos microcontroladores e os barramentos externos que interligam os microcontroladores com os periféricos (transdutores) através dos módulos de comunicação paralela e serial integrados. Com isso, transdutores passivos se evoluíram para transdutores *smart*, ganhando uma certa autonomia nas suas ações.

No entanto, a evolução destas células de trabalho dedicadas à tecnologia de **computação ubíqua**[1] e a **internet das coisas**, em inglês *Internet of Things*[2] (IoT), se deve principalmente à evolução da tecnologia de comunicação permitindo que as coisas se cooperem diretamente para cumprir uma missão mais complexa. Por exemplo, hoje em dia, muitos sistemas mecânicos dos automóveis modernos são substituídos pelos sistemas eletrônicos microcontrolados, que vão desde o simples controle do movimento de palhetas limpadores de pára-brisa até o complexo controle de freios antitravamento, em inglês *anti-lock braking system* (ABS), de recirculação de gases de escapamento, em inglês *exhaust gas recirculation* (EGR), de *airbags*, e de cruzeiro, em inglês *cruise control* (Figura 13.1). As unidades de controle eletrônico embutidas num automóvel são interconectadas por múltiplas redes locais, em inglês *Local Area Networks* (LANs), procurando contemplar as características elétricas, funcionais e temporais dos sinais dos diversos dispositivos interconectados. Como já discutido no Capítulo 9, é mais eficiente agrupar as unidades de controle pelas suas características elétricas, funcionais e temporais e associá-las a uma rede com um específico protocolo de comunicação. Figura 13.2 mostra as redes intraveiculares que se podem encontrar num automóvel moderno [2]: CAN (*Controller Area Network*), Ethernet, Flexray, LIN (*Local Interconnect Network*) e MOST (*Media Oriented System Transport*).

---

[1] O termo **computação ubíqua**, em inglês, *ubiquitous computing* ou ubicomp, foi cunhado por Mark Weiser em 1991, profetizando que no século 21 os serviços de computação interconectados seriam móveis, pervasivos e onipresentes no cotidiano das pessoas.

[2] O termo **Internet das Coisas**, em inglês *Internet of Things*, foi cunhado por Kevin Ashton em 1999 como uma forma de atrair atenção dos executivos de Companhia *Procter & Gamble* para a tecnologia RFID (Identificação por Radiofrequência). Ele trabalhava na otimização da cadeia de surpimentos.

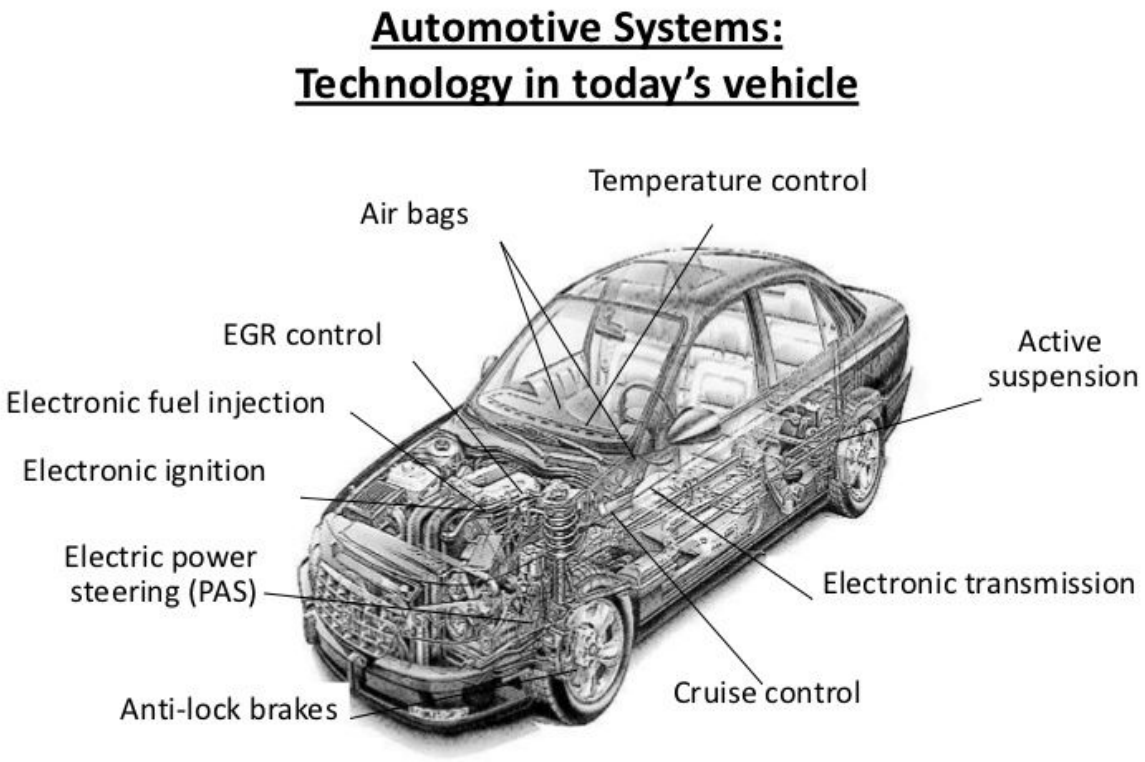


Figura 13.1: Unidades de controle eletrônico embutidas nos automóveis modernos (Fonte: [1]).

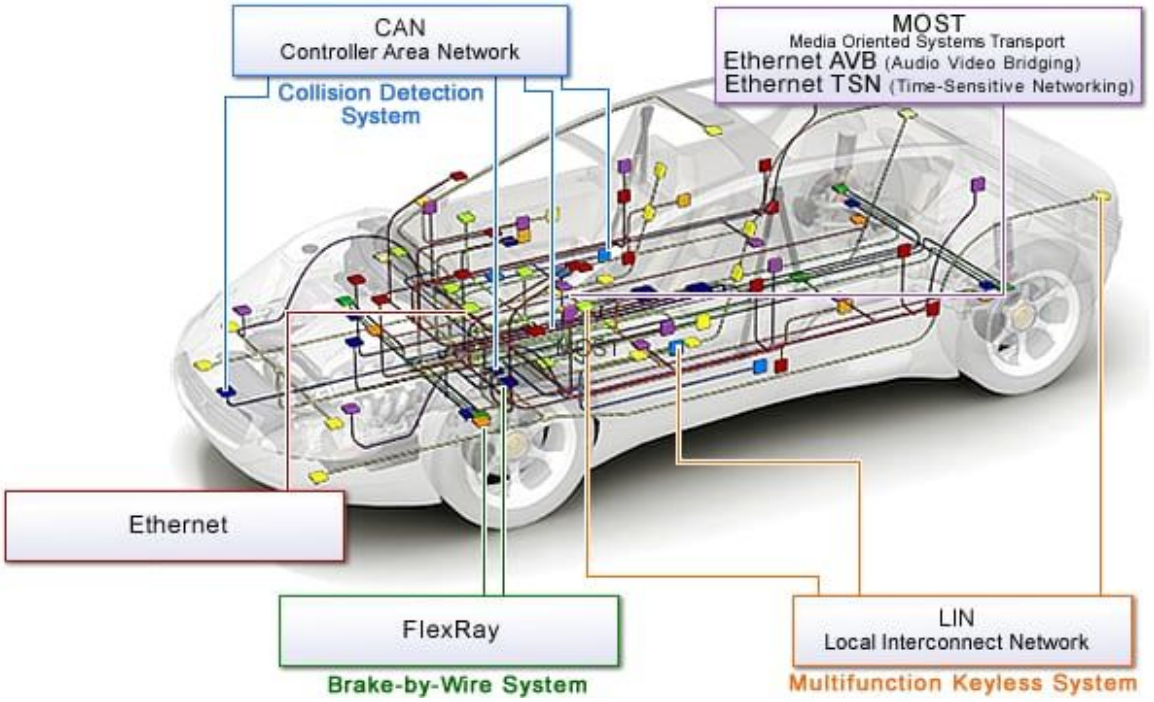


Figura 13.2: Redes intraveiculares (Fonte: [2]).

Hoje em dia, um sistema ciber-físico, em inglês *Cyber-Physical Systems* (CPS)[3], procura integrar a dinâmica processos físicos com a computação e a rede. A rede não se limita à *Internet* dos humanos. Ela inclui também a *Internet* das coisas e a *Internet* entre as coisas e os humanos, como mostra o modelo de referência de um projeto da Universidade de Berkeley na Figura 13.1. Para que eles se comunicam de forma adequada novos protocolos de comunicação foram desenvolvidos.

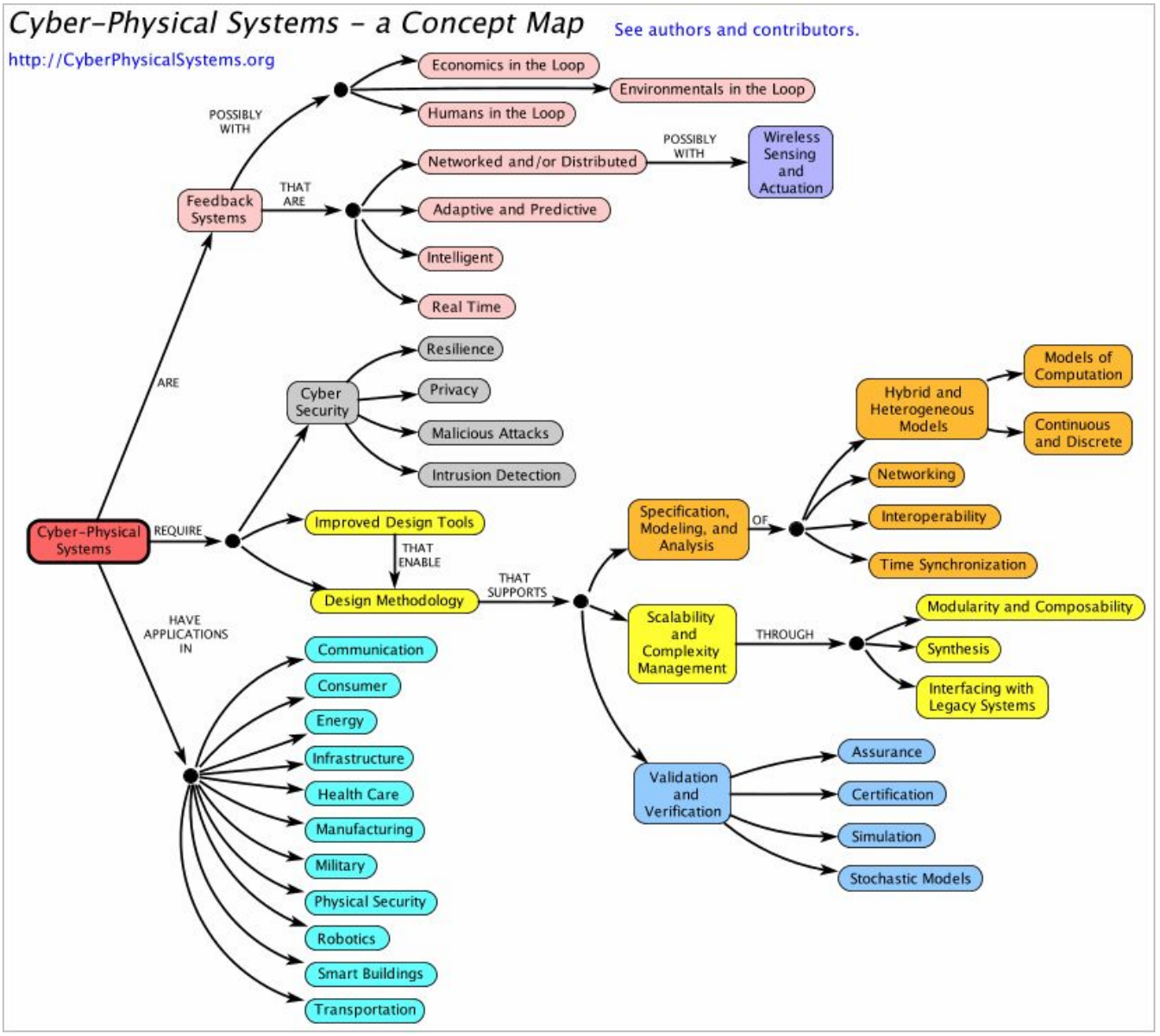


Figura 13.3: Um modelo de sistema ciber-físico (Fonte: [27]).

Como já vimos no Capítulo 9, um protocolo é um conjunto de regras e procedimentos estabelecido entre dois processos (eventualmente executados em diferentes máquinas) para emitir e receber os dados numa rede. Em frente à grande

[3] O termo sistema ciber-físico, em inglès Cyber-Physical System (CPS), foi cunhado por Helen Gill da *National Science Foundation* dos Estados Unidos. Ele surgiu em torno de 2006. Acredita-se que está relacionado com o termo *cyberspace* usado pelo escritor William Gibson na sua novela *Neuromancer*, embora haja muitos outros termos mais antigos com prefixo *cyber*.

diversidade de potenciais áreas de aplicação dos sistemas embarcados, há um volume muito grande e específico de protocolos de comunicação embarcada [19]. A rápida proliferação de redes e sub-redes de comunicação de computadores, com uma parafernália de nomes, levou à proposta de um modelo de rede de computador, o **modelo *Open System Interconnection*** (**OSI**), em 1971 e formalizado em 1983 pela Organização Internacional para a Normalização, em inglês *International Organization for Standardization* (ISO), com o objetivo de padronizar os protocolos de comunicação entre os diversos sistemas em uma rede local.

O objetivo deste capítulo não é esmiuçar nenhum protocolo de comunicação. Vamos dar apenas uma visão introdutória às interconexões globais entre diferentes microcontroladores e processadores para formar uma complexa rede móvel de serviços.

13.1 Características de uma Rede Embarcada

As principais medidas de desempenho de uma rede de comunicação são [20]:

- **largura de banda**, em inglês *bandwidth*: corresponde à quantidade máxima que uma informação pode ser transferida por um intervalo de tempo, é tipicamente dada em *bits*/segundo.
- **taxa de transferência**, em inglês *throughput*: corresponde à percentagem de transferência bem sucedida de dados em relação ao volume total de dados transferidos.
- **latência**, em inglês *latency*: é o tempo de atraso entre o envio pelo transmissor e a recepção pelo receptor, depois de desempacotados e decodificados os dados. Vale lembrar que este tempo depende do meio em que o sinal eletromagnético (portador de informação) se propaga e dos nós pelos quais o sinal passa.
- **desvios aleatórios**, em inglês *jitter*: são variações indesejadas do sinal de *clock* nos receptores em relação ao sinal de *clock* de referência.
- **taxa de bits de erro**, em inglês *error rate*: corresponde à taxa de *bits* recebidos errados em relação à quantidade total de *bits* recebidos.

De acordo com Upender e Koopman [3], para uma rede embarcada devemos observar adicionalmente os seguintes pontos:

- **eficiência**: como a largura de banda é muito mais limitada do que a de sistemas clássicos de rede, as mensagens transmitidas são tipicamente curtas e com uma quantidade de *bits* de *overhead*[4] muito pequena.

[4] *Bits* de *overhead* de uma mensagem são os *bits* de controle ou de estado que não representam os dados de informação propriamente ditos.

- **determinismo**: é desejável que seja determinável o tempo de resposta para o pior dos casos em tarefas críticas em tempo, como o processamento de interrupções ou de laços de controle de altíssimo desempenho.
- **robustez operacional**: é desejável que o protocolo de comunicação seja robusto tanto na detecção quanto na recuperação dos erros detectados e/ou de um *reset*.
- **configurabilidade**: é desejável que o sistema suporta diferentes meios de comunicação (fios, fibras or sem fios) e diferentes topologias mistas.
- **baixo custo por nó**: é desejável que a infra-estrutura *hard* e *software* seja de baixo custo e os protocolos de comunicação sejam de amplo e pronto uso.
- **conectividade**: alta capacidade de comunicação simultânea entre diversos nós.

Até agora vimos que, numa rede embarcada cabeada, distinguem-se essencialmente dois tipos de comunicação entre os microcontroladores e os processadores envolvidos [4,5,6] (Figura 13.4):

- **intra-sistema**, ou barramentos externos (Seção 9.1): estabelece a comunicação entre os dispositivos dentro de um sistema, como as comunicações via os protocolos I2C e SPI que vimos na Seção 9.9.
- **inter-sistema**, ou barramentos globais (Seção 9.1): estabelece a comunicação entre os dispositivos de diferentes sistemas, usualmente através de protocolos de comunicação UART/USART (Seção 9.8) e USB (Seção 9.10).

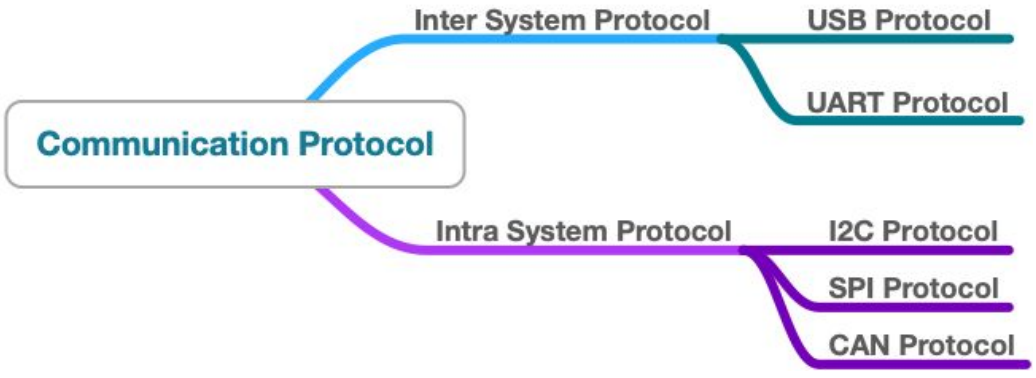


Figura 13.4: Protocolos de comunicação em redes cabeadas (Fonte: [4]).

Rápidos avanços das tecnologias de sensores e de comunicação impulsionaram o acelerado desenvolvimento de **redes de sensores sem fio**, em inglês *Wireless Sensor Network* (WSN), capazes de coletar as amostras obtidas pelos *smart* sensores dispersos numa área monitorada através de conexões sem fio. Note na Figura 13.5 que esses dados coletados são enviados para uma estação base[5]

[5] Em uma rede de computadores ela é um transceptor que age como um roteador para computadores conectados a uma rede de área local e/ou a uma *internet*.

provida de uma estação de transceptores (BST, *Base Station Transceiver*) e uma estação controladora (BSC, *Base Station Controller)* para recepção/transmissão, em radiofrequência, de sinais apropriadamente decodificados/codificados. O BSC, por sua vez, está conectado a redes sem fio e a uma rede cabeada. Através destas redes, as amostras coletadas são enviadas para um **Centro de Gerenciamento de Dados**, outras estações de processamento e diversos dispositivos móveis, entre eles um assistente digital personalizado, em inglês *Personal Digital Assistant* (PDA), e um *smartphone*.

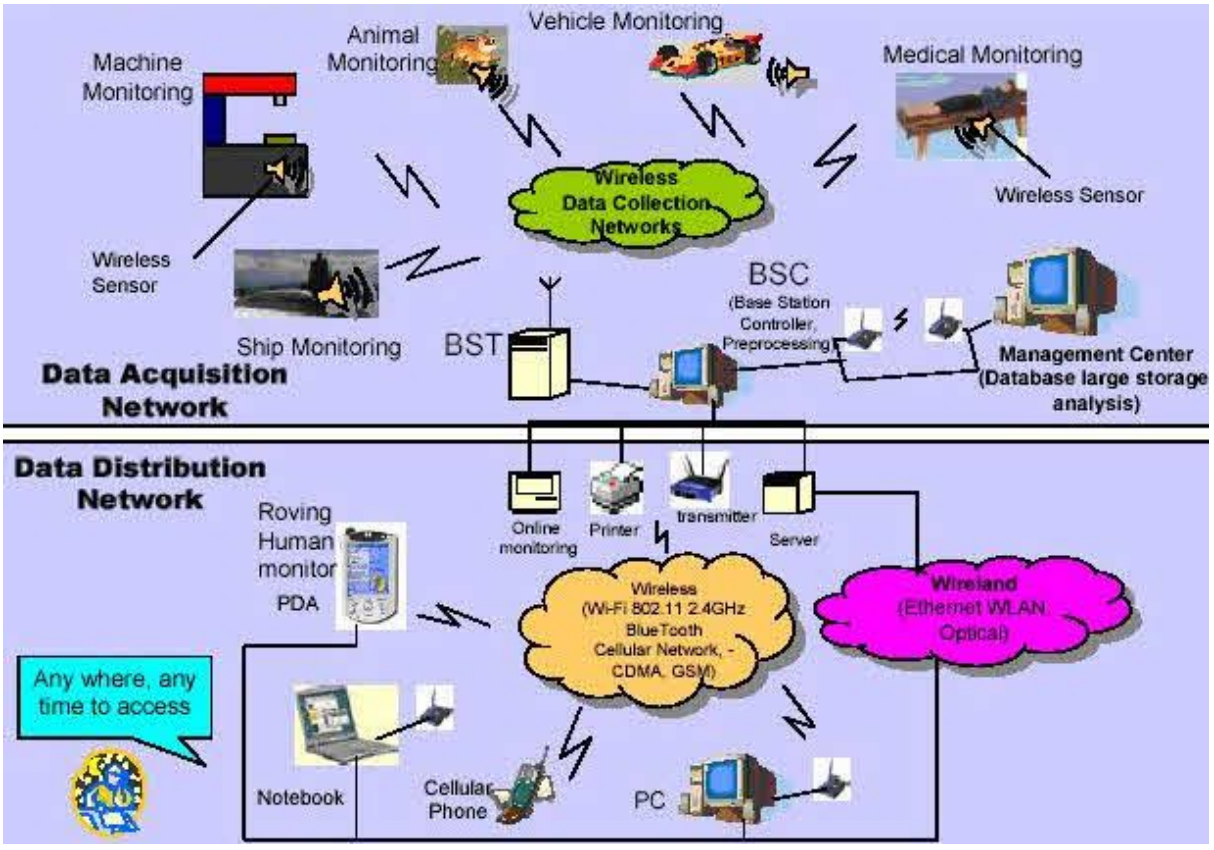


Figura 13.5: Comunicação com uma rede de sensores sem fio (Fonte: [6]).

Para um cenário de rede embarcada sem fio mostrado na Figura 13.5, os protocolos de comunicação sem fio, junto com um *gateway* sem fio, passam a ocupar um papel importante numa rede embarcada móvel (Figura 13.6). Observe que as amostras de cada *smart sensor* são enviadas ao *gateway* sem fio, que é um roteador[6] capaz de rotear pacotes de dados de uma LAN sem fio para uma outra **rede de longa distância**, em inglês *Wide Area Network* (WAN) com ou sem fio. Vale ressaltar aqui que, por questão de segurança, todos os *gateways* sem fio

[6] Roteador é um equipamento que conecta diferentes (duas ou mais) redes de computadores e é capaz de redirecionar a rota dos pacotes de dados para uma outra rede onde se encontra o **endereço de Protocolo da Internet**, em inglês *Internet Protocol address* (IP), do destino (Seção 13.4.2).

adotam alguma técnica de criptografia[7], como *Wired Equivalent Privacy* (WEP), *Wi-Fi Protected Access* (WPA) e *Wi-Fi Protected Setup* (WPS), na transferência dos pacotes de dados.

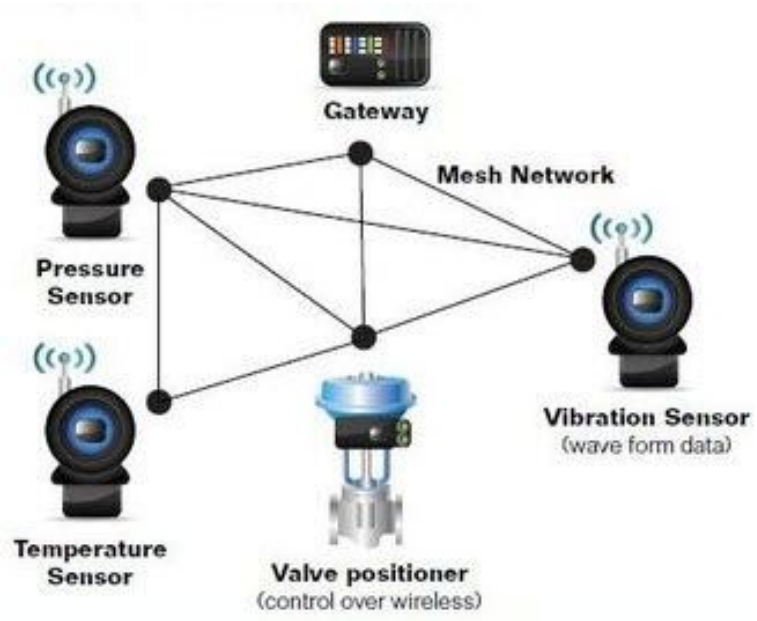


Figura 13.6: Rede de sensores com um roteador sem fio (Fonte: [7]).

Hoje em dia já se encontram no mercado microcontroladores com funcionalidades de conectividade wi-fi integradas [9], facilitando cada vez mais a implementação de um projeto de *internet* das coisas [10]. Vamos ver na Seção 13.2 como os protocolos de comunicação existentes [19] se relacionam na implementação de uma rede de comunicação de dados. Figura 13.7 apresenta o diagrama de blocos do microcontrolador ESP8266 com o módulo de conexão por radiofrequência integrado.

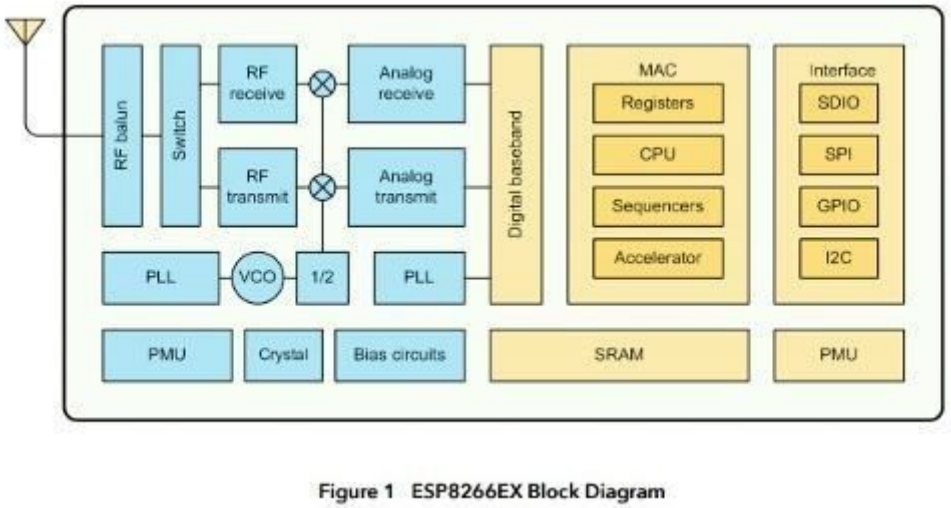


Figure 1 ESP8266EX Block Diagram

Figura 13.7: Microcontrolador com módulo de wi-fi integrado.

[7] Criptografia é uma prática de codificar e decodificar dados de forma que eles não tenham mais o formato original e de difícil entendimento.

13.2 Modelo OSI

(baseado em [11])

O modelo de Interconexão de sistemas abertos, em inglês *Open Systems Interconnection* (OSI), é um modelo de referência, padronizado pela ISO em 1984, para descrever a comunicação de uma aplicação com uma rede de sistemas digitais. O objetivo deste modelo é prover aos fabricantes de *hardware* e aos desenvolvedores de *software* as diretrizes para assegurar a interoperabilidade de um novo produto e para descrever este novo produto de forma universal. A sua evolução começou a partir das experiências com os projetos de rede governamentais, ARPANET (Estados Unidos) e CYCLADES (França), e com os padrões proprietários, como *System Network Architecture* (SNA) da IBM e DECnet da *Digital Equipment Corporation*. A abstração de uma rede de computadores em 7 camadas se deve ao Charles Bachman da *Honeywell Information Systems*.

De acordo com o modelo ISO, uma rede de computadores pode ser desdobrada em 7 diferentes camadas de serviços, desde o nível físico (nível 1) até o nível de aplicação (nível 7), como sintetiza a Tabela 13.1. O modelo só especifica o que cada camada deve fazer, mas não impõe como os serviços e os protocolos devem ser implementados em cada camada. Além disso, o modelo define diretivas genéricas para a construção de redes de comunicação de sistemas heterogêneos de arbitrárias distâncias, mas não estabelece nenhuma restrição sobre a tecnologia empregada em cada camada.

Tabela 13.1: Modelo OSI (Fonte: [11]).

OSI model				
Layer			**Protocol data unit (PDU)**	**Function**
Host layers	7	Application	Data	High-level APIs, including resource sharing, remote file access
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption

	5	Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing	
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control	
	2	Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer	
	1	Physical	Symbol (bitstream)	Transmission and reception of raw bit streams over a physical medium	

Contextualizando um sistema de comunicações no modelo OSI tem ajudado não só nas avaliações comparativas dos protocolos de comunicação como também no entendimento do fluxo de dados numa rede de comunicação. Figura 13.8 ilustra as 7 camadas envolvidas na transmissão e recepção de uma mensagem conforme o modelo OSI.

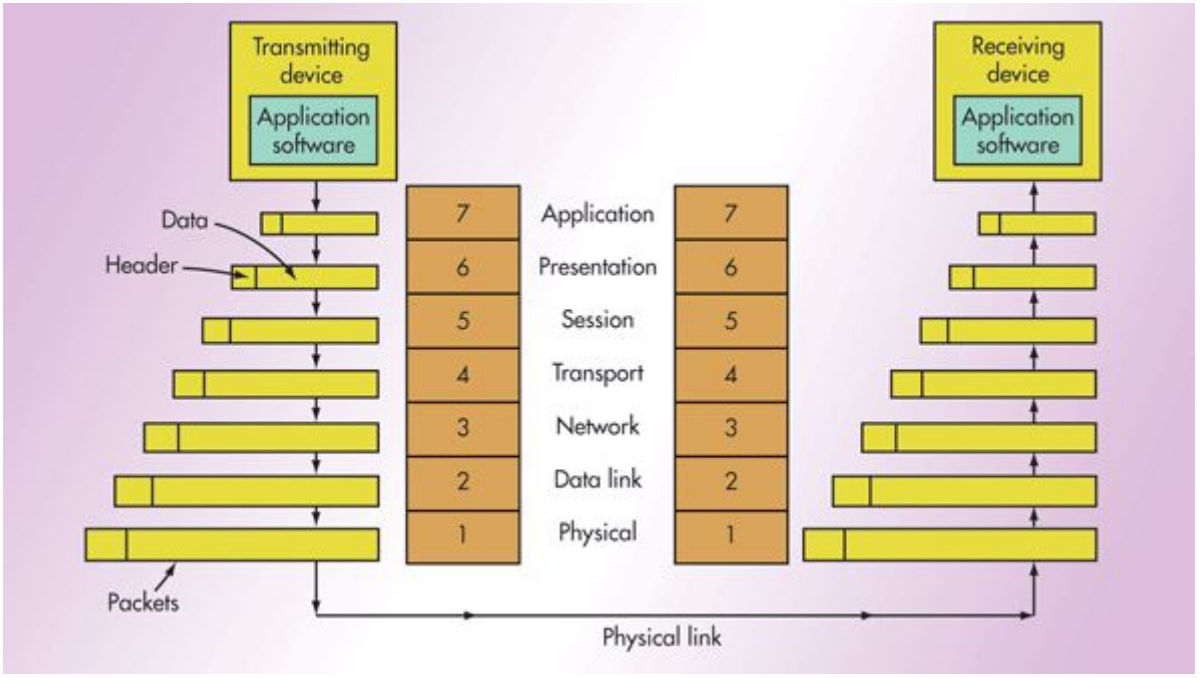


Figura 13.8: Transmissão e recepção conforme o modelo OSI (Fonte: [16]).

Vamos ver como o modelo OSI agrupa os mais diversos protocolos de comunicação usados na conexão de dois ou mais sistemas:

- **Camada física**: é a camada de dispositivos físicos responsáveis pela passagem de pacotes de dados, como *hubs* [12], e dos meios de transmissão, como os cabos de rede. Alguns autores consideram que os protocolos RS-232, camada física do protocolo USB [19], I2C e SPI incluem esta camada de descrição, pois eles especificam as conexões físicas entre os dispositivos e os sinais elétricos.
- **Camada de enlace ou ligação de dados**: é a camada que controla o fluxo de dados da camada física, assegurando a integridade dos dados para que as camadas superiores possam assumir uma transmissão sem erros e garantindo que os dados sejam entregues ao destinatário correto. É nesta camada em que cada dispositivo transmissor tem um endereço físico denominado o endereço de **controle de acesso ao meio**, em inglês *Media Access Control* (MAC) *address*, e em que vários protocolos de rede podem ser multiplexados por meio do **controle de enlace lógico**, em inglês *Logic Link Control* (LLC) e podem "conviver" dentro de uma mesma rede multiponto. Dispositivos como *switches* [12] podem estar presentes nesta camada. Para os sistemas embarcados, os protocolos mais usados nesta camada são Ethernet, Wi-Fi, PPP, GSM, 3G e 4G [18].
- **Camada de rede**: é nesta camada que temos o endereçamento de **Protocolo da Internet**, em inglês *Internet Protocol* (IP) address, para cada máquina da rede. Assim, os pacotes de dados podem ser roteados correta e eficientemente entre a sua origem (IP de origem) e o seu destino (IP de destino) via o **protocolo da Internet**. Integrado a este protocolo temos o **protocolo de mensagem de controle da Internet**, em inglês, *Internet Control Message Protocol* (ICMP), que é transmitido toda vez que uma situação de erro é detectada no envio de um pacote IP. É a camada de rede mais popular. A conversão dos endereços IP para o endereço MAC da camada de enlace de dados pode ser feita pelo **protocolo de resolução de endereço**, em inglês *Address Resolution Protocol* (ARP).
- **Camada de transporte**: é nesta camada que ocorre de fato o transporte dos pacotes vindos da camada da rede, assegurando a qualidade do serviço de maneira que os dados sejam entregues com consistência. Porém, nem todos os protocolos nesta camada garantem a entrega de uma mensagem. O protocolo de controle de transmissão, em inglês *Transmission Control Protocol* (TCP), provê confiabilidade, entrega na sequência correta e verificação de erros dos pacotes de dados, entre os diferentes nós da rede. Enquanto o **protocolo do pacote de usuário**, em inglês *User Datagram Protocol* (UDP), utiliza os serviços básicos de IP, sem verificar se pacote chega ao seu destino corretamente.

- **Camada de sessão**: esta é a camada responsável por estabelecer a conexão entre os *hosts* (nós de uma rede). Inclui, portanto, serviços de autenticação e de reconexão.
- **Camada de apresentação**: esta é a camada responsável pela apresentação dos dados encapsulados nos pacotes numa forma acessível pelos usuários de aplicação, conforme a sintaxe e a semântica pré-definidas. É nesta camada que ocorre a compressão e criptografia dos dados.
- **Camada de aplicação**: é nesta camada que temos de fato interações entre os usuários e os dados transferidos em redes. São inclusos nesta camada os **protocolos de transferência de hipertextos**, em inglês *Hypertext Transfer Protocol* (HTTP), **de transferência de arquivos**, em inglês *File Transfer Protocol* (FTP) e os serviços de **sistema de domínio de nomes**, em inglês *Domain Name System* (DNS). É nesta camada em que o nome de domínio de uma máquina é convertido para o endereço de protocolo da internet.

Em cada camada é definida uma unidade de informação, composta de dados específicos de controle para transmissão e dados de aplicação. Esta unidade de informação é conhecida por **unidade de dados protocolares**, em inglês *Protocol Data Unit* (PDU). Tipicamente, elas correspondem aos *bits* (0 e 1) na camada física (camada 1), *frames* na camada de enlace de dados (camada 2), pacotes, em inglês *packets*, na camada de rede (camada 3), segmentos ou datagramas na camada de transporte (camada 4). Nas camadas de aplicação, a unidade de informação depende diretamente das aplicações.

É importante ressaltar que os produtos relacionados com a rede de comunicação raramente seguem às riscas o modelo OSI na sua implementação. O modelo OSI é um modelo de referência de comunicação entre uma aplicação e uma rede de sistemas digitais. Quando se trata de um aplicativo que envolve as interações humanas, como *World Wide Web*, correios eletrônicos, redes sociais e ftp (*Internet* dos humanos), vimos que eles são implementados em cima dos protocolos das camadas de rede e de transporte TCP/IP. E quando se trata de trocas de dados entre transdutores *smart* via uma rede de computadores (*Internet* das coisas), como coleta de amostras climáticas numa estação, veremos nas próximas seções como podemos transferir, com a tecnologia do estado-da-arte, os sinais físicos dos circuitos eletrônicos através das camadas do modelo OSI [18].

13.3 Camada de Enlace de Dados

A camada de enlace de dados, ou camada 2 das sete camadas do modelo de referência OSI, fica entre a camada física (camada 1), abstraindo os detalhes de conexões dos componentes físicos, e a camada de rede (camada 3), provendo uma interface lógica dos endereços dos nós e dos controles das ligações intermediárias

entre um par nós em comunicação. Isso facilita a troca de dados, em **quadros** ou em ***frames***, entre duas máquinas interconectadas numa rede. Figura 13.9 ilustra a interface da camada 2 em relação às camadas 1 e 3.

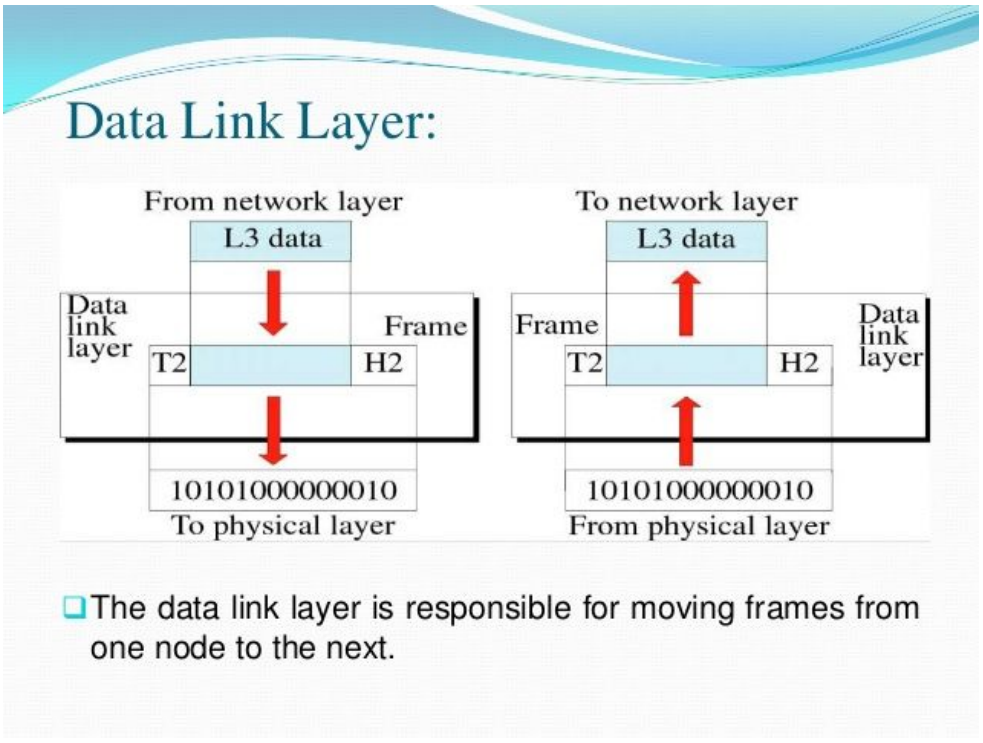


Figura 13.9: Camada de enlace de dados (Fonte: [17]).

A camada de enlace de dados inclui duas sub-camadas, como vimos na Seção 13.2:

- **sub-camada de controle de link lógico**, em inglês *Logical Link Control* (LLC), responsável por multiplexar os protocolos que competem o mesmo canal de transmissão alocado no nível físico e por controlar o fluxo de dados nos canais lógicos de conexão. Quando a transmissão é muito ruidosa e instável, é permitida nesta sub-camada requisição de retransmissões automáticas entre os nós na presença de **erros *node-to-node***.
- **sub-camada de controle de acesso ao meio**, em inglês *Media Access Control* (MAC), responsável pelo controle e pela multiplexação de dados nos meios físicos de conexão, incluindo o controle de acesso aos meios, o controle de erros na transmissão, e multiplexação dos dados nos meios físicos.

Vamos apresentar nesta seção as técnicas de controle de acesso ao meio (de comunicação) apropriadas para sistemas embarcados. Em seguida, faremos uma descrição breve de dois protocolos da camada de enlace de dados mais aplicados em sistemas embarcados [18].

13.3.1 Técnicas de Controle de Acesso ao Meio

(baseado em [3])

Vimos na Seção 9.3 diferentes técnicas de arbitragem quando temos vários mestres solicitando o controle de um barramento compartilhado. Numa rede onde os meios de comunicação tem uso compartilhado, é também necessário arbitrar um transmissor para acessar os meios de transmissão disponíveis. O controle de Acesso ao Meio, em inglês *Media Access Control* (MAC), da **camada de *enlace***, também conhecida como a camada de ligação de dados ou a camada número 2 do modelo OSI (Seção 13.2), é responsável por essa arbitragem assegurando a correta transmissão de ***frames* de dados** entre dois nós da rede (Figura 13.9). Vamos apresentar, de forma genérica, as diferentes técnicas de acesso a um meio numa rede embarcada que procuram satisfazer as características listadas na Seção 13.1 [3]. Tabela 13.2 sintetiza as técnicas a serem detalhadas.

Tabela 13.2: Quadro comparativo das técnicas de controle de acesso ao meio (Fonte: [3])

↑ Good - OK ↓ Poor	Efficiency Light Traffic	Efficiency Heavy Traffic	Deter-minacy	Priori-tization	Robust-ness	Physical Layer Flexibil.	Low Cost/ Node
Connection	-	↓	↑	-	↑	↓	-
Polling	↓	-	↑	↓	↓	↑	-
TDMA	↓	↑	↑	↓	↓	↑	↓
Token Ring	↑	↑	↑	↑	-	-	-
Token Bus	-	↑	↑	-	-	↑	-
Binary Cnt.	↑	↑	-	-	↑	↓	↑
CSMA/CD	↑	↓	↓	-	↑	↑	-
CSMA/CA	↑	↑	↑	↑	↑	↑	↑

13.3.1.1 Controle Orientado para a Conexão

A técnica **orientada para a conexão** foi bastante utilizada na conexão dos terminais remotos com os *mainframes*. Caracteriza-se (1) por estabelecer uma conexão entre os dois nós antes do envio de qualquer pacote de dados, de forma que um nó possa enviar dados para o outro nó em modo *full-duplex*, e (2) por manter a ordem dos dados recebidos em relação aos dados enviados. Neste esquema, é comum o nó

receptor enviar um aviso de recepção ou uma requisição pelo reenvio no caso da perda de dados ou da detecção de erros. Portanto, os serviços deste protocolo são considerados confiáveis. O protocolo de controle de transmissão, em inglês *Transmission Control Protocol* (TCP), é um exemplo de protocolo orientado para a conexão.

13.3.1.2 *Polling*

Polling é um dos protocolos mais utilizados em sistemas embarcados por causa da sua simplicidade e por ser determinístico. Há um mestre que periodicamente seleciona um dos nós escravos e envia para ele uma mensagem de escolhido, delegando-o explicitamente o poder de assumir o controle dos meios para fazer transmissões (Figura 13.10). É um sistema pouco eficiente e pouco robusto em relação às falhas no mestre. Este protocolo foi aplicado na comunicação de subsistemas de aeronaves militares (MIL-STD-1553B).

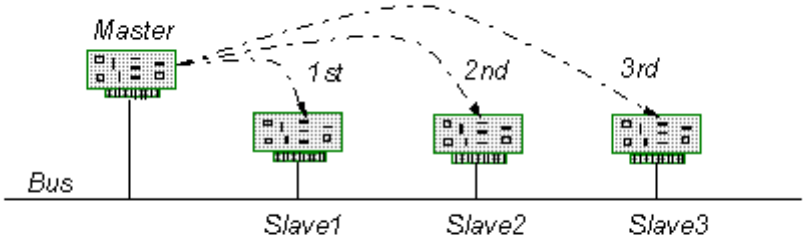


Figura 13.10: Rede com o controle de acesso por *polling* (Fonte: [3]).

13.3.1.3 Acesso Múltiplo por Divisão de Tempo (TDMA)

TDMA é um protocolo bastante utilizado em comunicações de satélites. Como *polling*, há um dispositivo mestre para controlar o acesso aos meios de comunicação (Figura 13.11). Porém, diferente do *polling*, não é enviado uma mensagem de escolha. No lugar, o chaveamento de acessos é baseado nas fatias de tempo de transmissão atribuídas a cada escravo. Para assegurar o sincronismo dos escravos com o mestre, o mestre envia um sinal de sincronismo antes de iniciar as transmissões. Por requer sincronismo, os circuitos do escravo precisam ter uma base de tempo mais estável do que os de *polling*. Este protocolo foi muito popular entre as aplicações aeroespaciais (NASA e Boeing). E foi adotado no protocolo de telefonia móvel de segunda geração (2G) e no protocolo de Sistema Global de Comunicações Móveis, em inglês *Global System for Mobile Communications* (GSM).

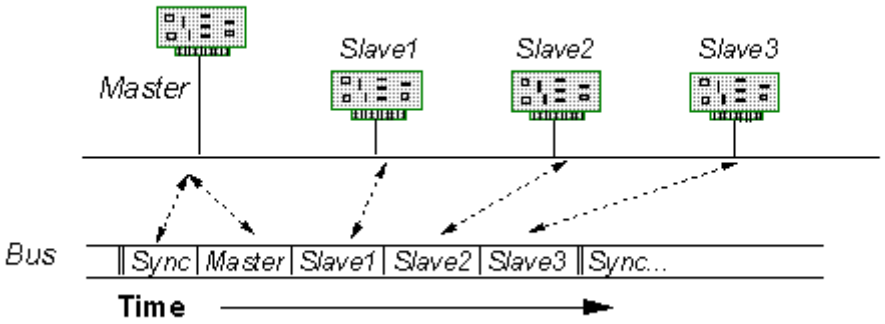


Figura 13.11: Rede com o controle de acesso por TDMA (Fonte: [3]).

13.3.1.4 Anel de Tokens

Numa rede de **anel de tokens**, em inglês *Token Ring*, os nós são conectados ponto a ponto como mostra a Figura 13.12. Um sinal de *token* especial circula pelo anel. Quando um nó tem algo para transmitir, ele pára a circulação deste sinal, envia a mensagem pelo anel e libera a circulação do sinal de *token* especial para passar o controle de acesso a outros nós. Uma estratégia muito aplicada é assegurar que em cada nó só ocorre atraso de 1 *bit*, de forma que um *token* de T *bits* consegue visitar todos os N nós de uma rede em (N+T) *bits* (em tempo). É uma técnica de controle de acesso determinística por podermos estimar o tempo no pior dos casos. Quando a rede está vazia, a sobrecarga (*overhead*) com a passagem do sinal de *token* especial é relativamente alta. Porém, numa rede sobrecarregada, este *overhead* diminui bastante. Há um campo no *token* reservado para setar a prioridade de acesso ao controle, de forma que quando ele circula pelo anel, somente os nós com prioridade maior consegue acessar o controle. É uma técnica frágil no sentido de que a comunicação é interrompida completamente quando ocorre um problema em qualquer conexão. Para aumentar a robustez, conexões com duplo anel são encontradas nas implementações. Esta técnica é encontrada nos protocolos de LANs, como o padrão *Fiber Distributed Data Interface* (FDDI) para comunicação em fibras ópticas.

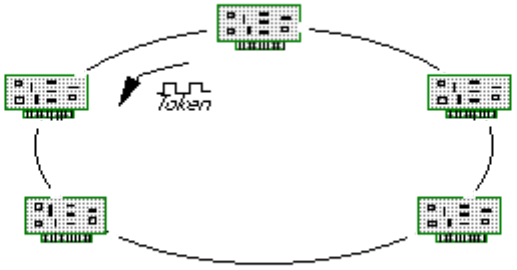


Figura 13.12: Rede com o controle de acesso por anel de tokens (Fonte: [3]).

13.3.1.5 Barramento de Tokens

A operação em **barramento de tokens**, em inglês *Token Bus*, é similar à operação em anel de *tokens* em termos do movimento circulatório do sinal de token especial. Porém, ao invés de circular a mensagem pelo anel como no anel de tokens, ela é *broadcasted* para todos os N nós de forma sequencial (Figura 13.13). Com isso, o sistema é mais robusto em termos de falhas em conexões locais. Como a sua estrutura linear é apropriada para o chão de fábrica, esta técnica de controle de acesso é adotada no protocolo MAP (*Manufacturing Automation Protocol*). O protocolo ARCnet (*Attached Resource Computer Network*) inclui esta técnica para conexão LAN e controle de processo.

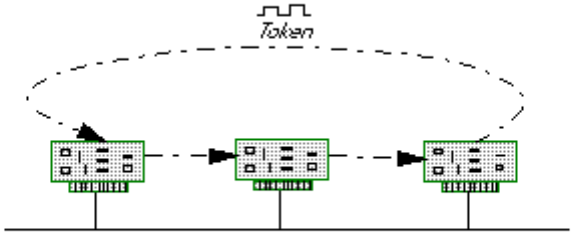


Figura 13.13: Rede como o controle de acesso por barramento de tokens (Fonte: [3]).

13.3.1.6 Contagem Regressiva Binária

Contagem regressiva binária, em inglês *Binary Countdown*, consiste numa técnica em que todos os nós de uma rede aguardem pela ociosidade de um canal antes de iniciar uma transmissão por ela. É também conhecida por **técnica de *bit* dominante**, em inglês *Bit Dominance*, porque os nós concorrentes a uma transmissão resolvem a contenção de um barramento baseado no valor da sua

identificação conforme ilustra a Figura 13.14. Todos nós colocam, *bit* a *bit*, a sua identificação. Quando há 0 e 1, aquele que estiver com 1, sai da concorrência. O procedimento é repetido até que sobre somente um, chamado dominante, para assumir o controle de acesso. Na Figura 13.14, o ganhador foi o nó 72. É uma técnica de alta taxa de transferência e eficiência. Não há nenhuma ordenação implícita no atendimento nem são considerados os nós inativos durante o processo de arbitragem. É uma técnica adotada no protocolo *Controller Area Network* (CAN) da Bosch e no padrão SAE J-1850 da Sociedade de Engenheiros Automotivos.

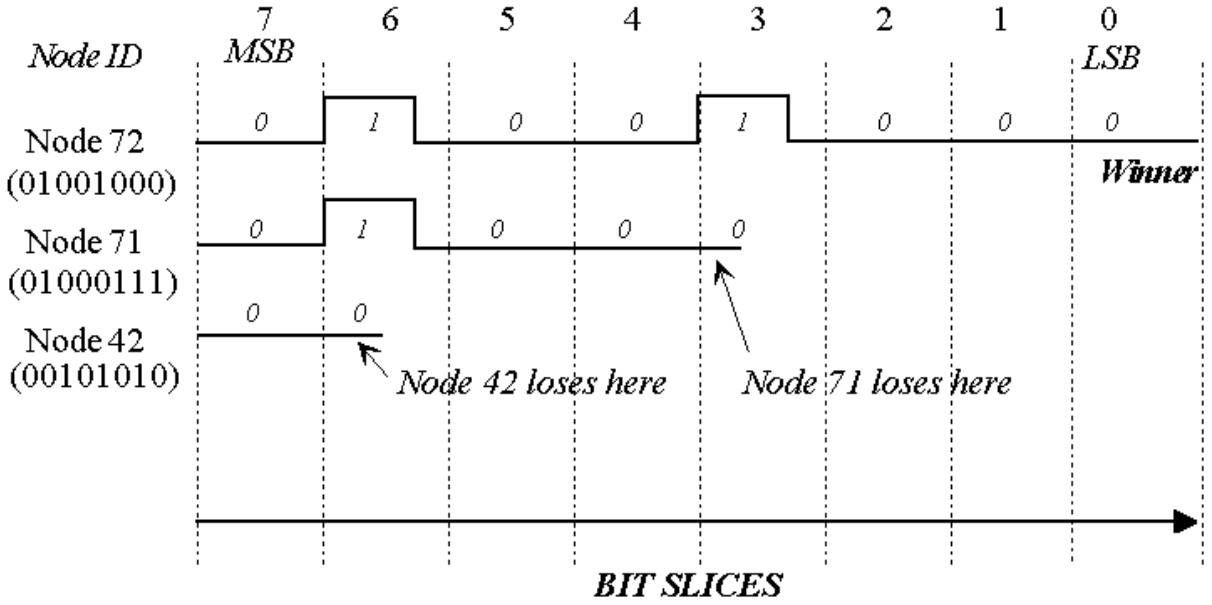


Figura 13.14: Arbitragem na técnica de controle de acesso por *bit* dominante (Fonte: [3]).

13.3.1.7 Controle de Múltiplo Acesso Sensível ao Portador com Detecção de Colisão (CSMA/CD)

Controle de Múltiplo Acesso Sensível ao Portador com Detecção de Colisão, em inglês *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD), é uma técnica bastante investigada com inúmeros variantes. Como em *Bit Dominance*, os nós aguardam pelo estado ocioso de um canal antes de iniciar uma transmissão. Quando múltiplas estações começam as suas transmissões (quase simultaneamente), as mensagens podem colidir, como ilustra a Figura 13.15. Quando isso acontece, o nó retira a sua mensagem assim que detecta a colisão e aguarda por um período de tempo aleatório antes de fazer uma nova tentativa de reenvio. Espera-se que essa aleatoriedade (não-determinística) faça que os nós não re-acessem o meio físico simultaneamente. Se, por acaso, ocorrer uma re-colisão, o tempo é aumentado exponencialmente antes de novas tentativas. A principal

vantagem desta técnica é que ela não impõe nenhum limite à quantidade de nós pré-alocados à rede e a passagem de *tokens* entre os nós. Os nós podem ser adicionados ou removidos de uma rede sem uma reinicialização ou reconfiguração. Por outro lado, a técnica não é determinística e pode apresentar um baixo desempenho em redes muito carregadas, com muito ruído e conexão de baixa qualidade. O protocolo Ethernet aplica esta técnica para controlar acesso aos recursos de transmissão.

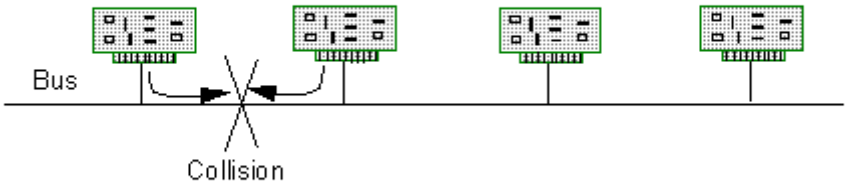


Figura 13.15: Detecção de colisão de mensagens na técnica de controle de acesso por CSMA/CD (Fonte: [3]).

13.3.1.8 Controle de Múltiplo Acesso Sensível ao Portador com Evasão de Colisão (CSMA/CA)

Controle de Múltiplo Acesso Sensível ao Portador com Evasão de Colisão, em inglês *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA), é resultado de esforços em combinar a eficiência de CSMA/CD em redes pouco carregadas e a eficiência de técnicas baseadas em passagem de *token* em redes carregadas. Como em CSMA/CD, os transmissores competidores só iniciam a sua transmissão quando o canal se encontra no estado ocioso. Porém, diferente de CSMA/CD, um sinal de congestionamento, em inglês *jam*, é enviado para a rede para notificar todos os nós que sincronizem os seus relógios e iniciem o seu intervalo de tempo de contenção, tipicamente deslocado de um atraso em relação ao nó anterior. Todos os nós podem, então, transmitir a sua mensagem no seu intervalo de tempo de contenção. Figura 13.16 ilustra uma situação em que dois nós, CPU2 e CPU3, competem por um canal e provoca um congestionamento. Foi alocado a cada nó um *slot* de contenção de barramento. O nó 1 não o usou porque não tem nada para transmitir. O nó 2 iniciou a sua transmissão assim que chegou no seu *slot*. O nó 3, ao detectar uma mensagem no canal, pára a contagem do tempo do seu slot, aguardando a liberação do canal. Somente quando o canal é liberado, passa-se o processamento para o nó seguinte.

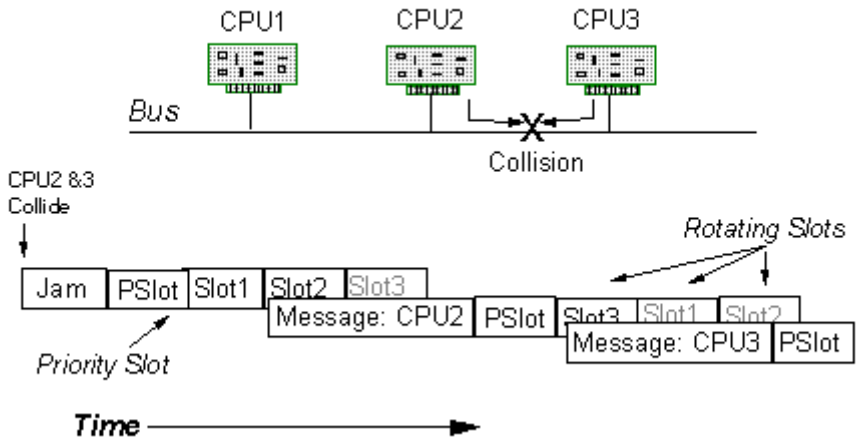


Figura 13.16: Rede com a técnica de controle de acesso por CSMA/CA (Fonte: [3]).

Para assegurar a equidade e o determinismo, a estratégia de circular os *slots* é muito aplicada após uma transmissão. Além disso, para incluir a funcionalidade de prioridade global, é permitido que os *slots* dos nós prioritários possam ser antecedidos dos *slots* dos outros nós menos prioritários. Há essencialmente duas variantes da técnica CSMA/CA:

- quando o número de *slots* é igual a número de nós: que presenta um bom desempenho em qualquer condição de operação da rede. A desvantagem é que a técnica não é escalável. O protocolo Reservation CSMA (RCSMA) adota esta técnica.
- quando o número de *slots* é menor que o número de nós: tendo menos slots, a alocação é aleatória quando há muitos nós em conflito. Tipicamente, usa-se o fluxo esperado dos dados para otimizar a alocação. O protocolo Echelon's *Local Operating Network* (LON) aplica esta técnica na sua arbitragem.

13.3.2 Protocolos de Comunicação

Nesta seção vamos apresentar dois protocolos de comunicação mais aplicados na camada de enlace de dados de uma rede de sistemas embarcados [18]: Ethernet (com fio) e Wi-Fi (sem fio). Vale, porém, mencionar que os protocolos *Synchronous Data Link Protocol* (SDLC), *High Level Data Link Control* (HDLC), *Serial Line Interface Protocol* (SLIP) e *Point-to-Point Protocol* (PPP) são também protocolos da camada de enlace de dados, pois eles incluem técnicas de controle de erros, controle de fluxo de dados no canal e o envelopamento dos dados, em inglês *data framing*. O envelopamento consiste em "envelopar" os dados com alguns *bits* adicionais, incluindo os *bytes* de sincronização, endereços de origem e de destino, identificador do quadro, e códigos detectores de erros na transmissão.

Os protocolos mais amplamente difundidos para interconexões em redes locais (**LAN**) são a rede cabeada Ethernet (padrão IEEE 802.3) e a rede sem fio Wi-Fi (padrão IEEE 802.11).

Os padrões 802 se focam na camada física (camada 1) e a sub-camada MAC da camada de enlace de dados (camada 2) do modelo OSI. Com o surgimento de dispositivos pessoais, como computadores pessoais, smartphones, tablets e assistentes digitais pessoais, surgiram **redes de área pessoal**, em inglês *personal area network* (**PAN**), dedicadas para conexões em redes doméstica tipicamente dentro de uma residência. Elas podem ser cabeadas, via por exemplo USB (Seção 9.10), ou sem fio, via uma rede sem fio (*wireless PAN*, WPAN) de baixo consumo de energia e de baixas taxas de transmissão (IEEE 802.15).

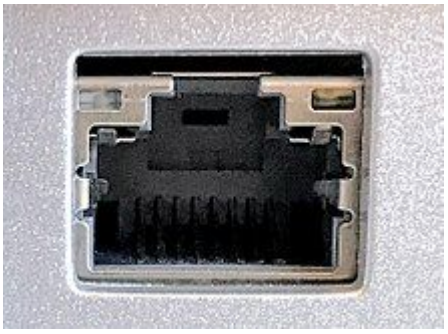
Nesta seção vamos apresentar algumas características da Ethernet e Wi-Fi. Na Seção 13.5 retomaremos o protocolo IEEE 802.15

13.3.2.1 Ethernet

(Texto extraído de [21] com adaptações)

Entre 1973 e 1974, a Ethernet foi desenvolvida pela Xerox Corporation no seu Centro de Pesquisa Palo Alto na Califórnia (PARC). A idéia foi documentada em um memorando que foi escrito por Metcalfe em 1973, onde ele cunhou-o após o éter luminífero uma vez postulado para existir como um meio onipresente, completamente passivo para a propagação de ondas eletromagnéticas. A Ethernet competiu com o *Token Ring*, FDDI, ARCnet, e outros protocolos proprietários. Com isso, ele foi capaz de se adaptar às realidades do mercado e mudar para um cabo coaxial fino e barato e, em seguida, escrita onipresente de par trançado (Figura 13.17). No ano de 1980, a Ethernet era claramente a tecnologia de rede dominante. Foi padronizada como IEEE 802.3 em 1983.

(a) Cabo de pra trançado com o conector 8P8C

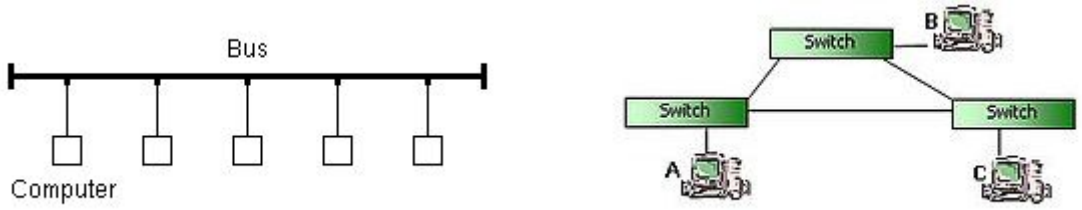


(b) Porta de um par trançado da Ethernet

Figura 13.17: Camada física da Ethernet (Fonte: [22]).

Desde então, essa tecnologia Ethernet evoluiu para atender às novas necessidades de largura de banda e de mercado. Agora, a Ethernet é usada para interconectar aparelhos e outros dispositivos pessoais. No ano de 2010, o mercado de equipamentos da Ethernet totalizou mais de US$ 16 bilhões por ano.

Como vimos na Seção 13.3.1.7, a Ethernet adota a técnica CSMA/CD para arbitrar um canal de transmissão. Portanto, é flexível a adição ou remoção de um nó na rede em termos de inicialização e configuração. Como todas as mensagens são transmitidas por um mesmo meio ocioso, todos os nós conectados à rede as recebem (Figura 13.18(a)). As interfaces da placa de rede precisam monitorar os endereços dos pacotes recebidos para decidir se deve gerar ou não interrupções alertando o processador da recepção. Além disso, sob o ponto de vista de cada nó, a largura de banda do meio de transmissão é bem menor do que a sua capacidade física. Isso levou a uma implementação moderna da Ethernet baseada nas conexões dos nós com a rede através de *switches*[8], denominada a versão *Switch Ethernet*, de forma que as potenciais colisões fiquem reduzidas somente na conexão nó-*switch* (Figura 13.18(b)). Porém, foi introduzido o modo *full-duplex* na versão Fast Ethernet (10 Mbps a 100 Mbps), que tornou o padrão de fato com a Gigabit Ethernet (1000Mbps). Isso permitiu que os *switches* e nós da rede transmitam simultaneamente os dados em meios físicos distintos sem colisões.



(a) Ethernet original (b) Ethernet moderna

Figura 13.18: Evolução da topologia da Ethernet (Fonte: [22]).

Os dados na Ethernet são envelopados em quadros, em inglês *frames*. São, de fato, inseridos alguns *bytes* antes e depois dos dados DATA, conforme mostra a Figura 13.19, para ajudar no controle do fluxo de dados pelo canal de comunicação.

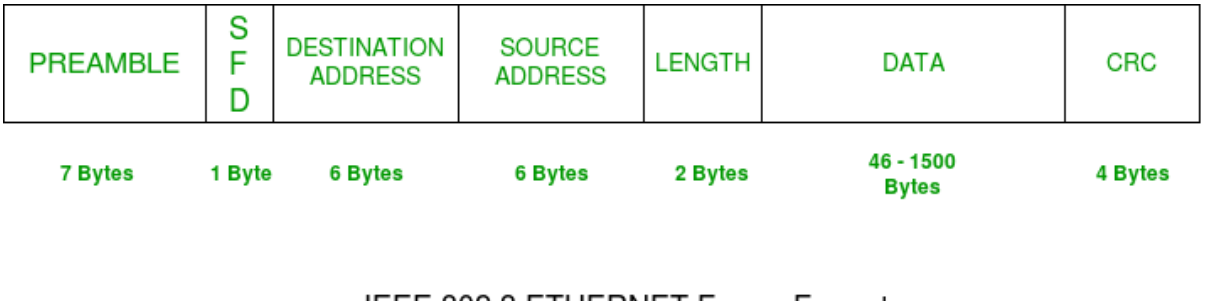


Figura 13.19: Formato básico dos dados no protocolo Ethernet (Fonte: [35]).

Os significados dos campos são:

[8] *Switches* são capazes de controlar o fluxo de dados determinando o destino de cada pacote de dados e direcionando-o diretamente ao nó endereçado. Com isso, ajuda na redução do tráfego de dados na rede.

- **Preâmbulo** (7 *bytes*): para indicar o início de um frame.
- **Início de Limite de Frame**, em inglês *Start of Frame Delimiter* (**SFD**) (1 *byte*): 10101011 para indicar que os próximos bits são do início do frame.
- **Endereço de destino** (6 *bytes*) : endereço MAC da máquina receptora.
- **Endereço de origem** (6 *bytes*): endereço MAC da máquina transmissora.
- **Comprimento** (2 *bytes*): tamanho do frame em *bytes*.
- **Dados** (tamanho variável até 1500 bytes).
- **CRC** (*Cyclic Redundancy Check*[9]) (4 *bytes*): código corretor de erros, gerado a partir dos campos de endereços, de tamanho e de dados.

Em relação ao modelo OSI, a Ethernet ocupa as duas últimas camadas da base. Usualmente sobre ela vêm a camada TCP/IP e os aplicativos baseadas da Internet como mostra a Figura 13.20.

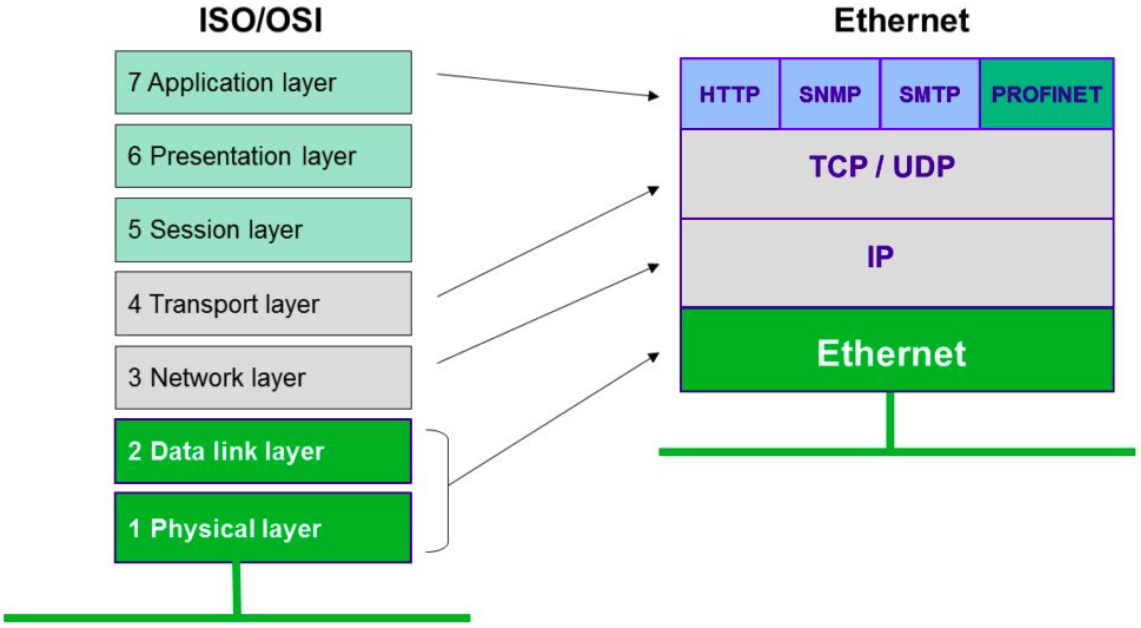


Figura 13.20: Ethernet mapeada no modelo OSI (Fonte: [23]).

13.3.2.2 Wi-Fi

(extraído de [24] com algumas adaptações)

Wi-Fi é um conjunto de especificações para **redes locais sem fio**, em inglês *Wireless Local Area Network* (**WLAN**) baseada no padrão IEEE 802.11. O nome "Wi-Fi" é tido como uma abreviatura do termo inglês "*Wireless Fidelity*", embora a Wi-Fi Alliance, entidade responsável principalmente pelo licenciamento de produtos baseados na tecnologia, nunca tenha afirmado tal conclusão. É comum encontrar o

[9] CRC é o código detector de erros usado

nome Wi-Fi escrito como *WiFi*, *Wi-fi* ou até mesmo *wifi*. Todas estas denominações se referem à mesma tecnologia.

A ideia de redes sem fio não é nova. A indústria se preocupa com esta questão há tempos, mas a falta de padronização de normas e especificações se mostrou como um empecilho. Vários grupos de pesquisas trabalhavam com propostas diferentes. Por esta razão, algumas empresas, como 3Com, Nokia, Lucent Technologies (atualmente Alcatel-Lucent) e Symbol Technologies (adquirida pela Motorola) se uniram para criar um grupo para lidar com este tema e, assim, nasceu, em 1999, a *Wireless Ethernet Compatibility Alliance* (WECA), que passou a se chamar Wi-Fi Alliance em 2003. O número de empresas que se associam à *Wi-Fi Alliance* aumenta constantemente. E a WECA passou a trabalhar com as especificações IEEE 802.11 que, na verdade, não são muito diferentes das especificações da Ethernet (IEEE 802.3) (Seção 13.3.2.1). Essencialmente, o que muda de um padrão para o outro são suas características de conexão: um tipo funciona com cabos, o outro, por radiofrequência. Além disso, devido às fortes atenuações, mesmo em curta distância, colisões não eram detectadas, tornando a estratégia CSMA/CD (Seção 13.3.17) impraticável. Por isso, a técnica CSMA/CA que aloca fatias de tempo de espera antes de retransmissões é aplicada para arbitrar um canal de transmissão. A vantagem disso é que não foi necessária a criação de nenhum protocolo específico para a comunicação de redes sem fios baseada nesta tecnologia. Com isso, é possível inclusive contar com redes que utilizam ambos os padrões, como mostra o posicionamento destes padrões em relação ao modelo OSI na Figura 13.21. Note que a Ethernet e a Wi-Fi se integram sob o padrão IEEE 1905.1 acerca redes domiciliares com e sem fio integradas.

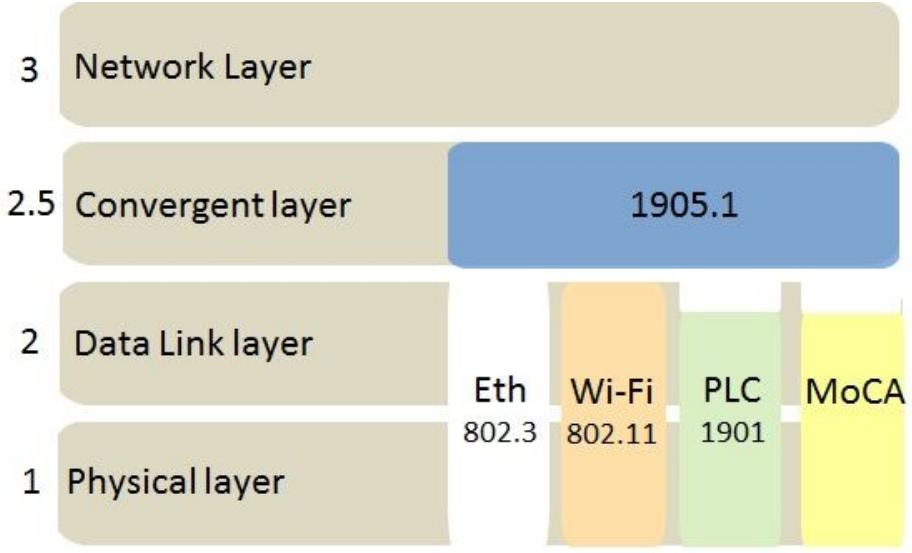


Figura 13.21: Posição relativa de Wi-Fi no modelo OSI (Fonte: [25]).

O padrão IEEE 802.11 estabelece normas para a criação e para o uso de redes sem fio. A transmissão deste tipo de rede é feita por sinais de radiofrequência, que se propagam pelo ar e podem cobrir áreas na casa das centenas de metros. Como existem inúmeros serviços que podem utilizar sinais de rádio, é necessário que cada um opere de acordo com as exigências estabelecidas pelo governo de cada país. Esta é uma maneira de evitar problemas, especialmente interferências. Há, no entanto, algumas bandas de frequência que podem ser usadas sem necessidade de aprovação direta de entidades apropriadas de cada governo: as faixas ISM[10], que podem operar, entre outros, com os seguintes intervalos: 902 MHz - 928 MHz; 2,4 GHz - 2,485 GHz e 5,15 GHz - 5,825 GHz (dependendo do país, esses limites podem sofrer variações). São justamente estas duas últimas faixas que o Wi-Fi utiliza. No entanto, tal característica pode variar conforme a versão do padrão 802.11.

Com a tecnologia Wi-Fi, é possível implementar redes que conectam computadores e outros dispositivos compatíveis (*smartphones*, *tablets*, consoles de videogame, impressoras, etc) que estejam próximos geograficamente. Estas redes não exigem o uso de cabos, já que efetuam a transmissão de dados por meio de radiofrequência, mas é necessário que esses dispositivos, chamados **estações**, em inglês *station* (STA), se conectem a aparelhos que forneçam acesso, genericamente denominado **Ponto de Acesso**, em inglês *Access Point* (AP). Quando um ou mais STAs se conectem a um AP, tem-se uma rede que é denominada um **conjunto de serviços básicos**, em inglês *Basic Service Set* (*BSS*). Figura 13.22 ilustra uma estação composta por 5 estações e um ponto de acesso. Por questões de segurança e de univocidade nos acessos, é atribuído a cada conjunto um **identificador do conjunto de serviços**, em inglês *Service Set Identifier* (SSID). Este identificador é uma sequência de caracteres, que, após definido, é inserido no cabeçalho de cada pacote de dados da rede para o endereçamento do pacote.

[10] ISM é acrônimo de *Industrial*, *Scientific and Medical* (*radio bands*)

Figura 13.22: Conjunto de Serviço Básico (BSS) numa Rede Wi-Fi (Fonte: [24]).

Se você tem uma rede Ethernet com dez pontos de acesso onde todos estão em uso, não será possível adicionar outro computador, a não ser que mais um cabo seja disponibilizado. Nas redes Wi-Fi, isso já não acontece, pois basta a qualquer dispositivo ter compatibilidade com a tecnologia para se conectar à rede. Mas, e se uma pessoa não autorizada conectar um computador à rede de maneira oculta para aproveitar todos os seus recursos, inclusive o acesso à internet? É para evitar problemas como estes que as redes sem fio devem contar com esquemas de segurança. Um deles é a **Privacidade Equivalente ao Cabeado**, em inglês *Wired Equivalent Privacy* (WEP).

O WEP existe desde o padrão 802.11 original e consiste em um mecanismo de autenticação que funciona, basicamente, de forma aberta ou restrita por uso de chaves. Na forma aberta, a rede aceita qualquer dispositivo que solicita conexão, portanto, há apenas um processo de autorização. Na forma restrita, é necessário que cada dispositivo solicitante forneça uma chave (combinação de caracteres, como uma senha) pré-estabelecida. Esta mesma chave é utilizada para cifrar os dados trafegados pela rede. O WEP pode trabalhar com chaves de 64 *bits* e de 128 *bits*. Naturalmente, esta última é mais segura. Há alguns equipamentos que permitem chaves de 256 *bits*, mas isso se deve a alterações implementadas por algum fabricantes, portanto, o seu uso pode gerar incompatibilidade com dispositivos de outras marcas. A utilização do WEP, no entanto, não é recomendada por causa de suas potenciais falhas de segurança (embora seja melhor utilizá-lo do que deixar a rede sem proteção alguma). Acontece que o WEP faz uso de vetores de inicialização que, com a aplicação de algumas técnicas, fazem com que a chave

seja facilmente quebrada. Uma rede utilizando WEP de 64 *bits*, por exemplo, tem 24 *bits* como vetor de inicialização. Os 40 *bits* restantes formam uma chave muito fácil de ser vencida. Mesmo com o uso de uma combinação de 128 *bits*, é relativamente fácil quebrar todo o esquema de segurança.

Diante deste problema, a Wi-Fi Alliance aprovou e disponibilizou em 2003 outra solução: o **Acesso Protegido pelo Wi-Fi**, em inglês *Wi-Fi Protected Access* (WPA). Tal como o WEP, o WPA também se baseia na autenticação e cifragem dos dados da rede, mas o faz de maneira muito mais segura e confiável. Sua base está em um protocolo chamado **Protocolo de Integridade Temporal da Chave**, em inglês *Temporal Key Integrity Protocol* (TKIP), que ficou conhecido também como WEP2. Nele, uma chave de 128 *bits* é utilizada pelos dispositivos da rede e combinada com o endereço *MAC* de cada estação (Seção 13.2). Como cada endereço MAC é diferente do outro, acaba-se tendo uma sequência específica para cada dispositivo. A chave é trocada periodicamente (ao contrário do WEP, que é fixo), e a sequência definida na configuração da rede, conhecida como senha de frase, em inglês *passphrase*, é usada, basicamente, para o estabelecimento da conexão. Assim sendo, é expressamente recomendável usar WPA no lugar de WEP.

Apesar de o WPA ser bem mais seguro que o WEP, a *Wi-Fi Alliance* buscou um esquema de segurança ainda mais confiável. Foi aí que surgiu o *802.11i*, que em vez de ser um padrão de redes sem fio, é um conjunto de especificações de segurança, sendo também conhecido como WPA2. Este utiliza um padrão de criptografia denominado **Padrão de Criptografia Avançada**, em inglês *Advanced Encryption Standard* (AES), que é muito seguro e eficiente, mas tem a desvantagem de exigir bastante processamento. Seu uso é recomendável para quem deseja alto grau de segurança, mas pode prejudicar o desempenho de equipamentos de redes não tão sofisticados (geralmente utilizados no ambiente doméstico). É necessário considerar também que equipamentos mais antigos podem não ser compatíveis com o WPA2, portanto, sua utilização deve ser testada antes da implementação definitiva.

A partir de 2007, começou a aparecer no mercado dispositivos wireless que utilizam *Wi-Fi Protected Setup* (WPS), um recurso desenvolvido pela *Wi-Fi Alliance* que torna muito mais fácil a criação de redes Wi-Fi protegidas por WPA2. Com o WPS é possível fazer, por exemplo, com que uma sequência numérica chamada PIN (*Personal Identification Number*) seja atribuída a um roteador ou equipamento semelhante. Basta ao usuário conhecer e informar este número em uma conexão para fazer com que seu dispositivo ingresse na rede. No final de 2011, tornou-se pública a informação de que o WPS não é seguro e, desde então, sua desativação em dispositivos compatíveis passou a ser recomendada.

13.4 Modelo TCP/IP: Camada de Transporte e de Rede

(extraído de [26] e [28] com algumas adaptações)

Antes da *internet* se tornar tão popular os protocolos de comunicação mais importantes eram o TCP/IP, NETBEUI, IPX/SPX, *Xerox Network System* (XNS) e o *Apple Talk*. Em maio de 1974, o IEEE publicou um artigo intitulado *A Protocol for Packet Network Interconnection* de co-autoria Vinton G. Cerf e Robert Kahn. Eles descreveram um protocolo de interconexão para compartilhamento de recursos usando comutação de pacotes ao longo dos nós. Um componente central de controle deste modelo foi o *Transmission Control Program*, que incorporou os elos e serviços orientados para datagrama entre os computadores hospedeiros.

Em 1978, o programa de controle de transmissão monolítico foi dividido depois dentro de uma arquitetura modular formada de um *Protocolo de controle de transmissão*, em inglês *Transmission Control Protocol* (TCP), na camada orientada a conexão e o *Protocolo de internet, em inglês Internet Protocol* (IP), na camada de interconexão. O modelo se torna informalmente conhecido como *TCP/IP*, embora formalmente tenha sido chamado de *Internet Protocol Suite* [28]. Em 1979, a versão 4 do IP foi concluída. O TCP/IP representa um conjunto de protocolos que permitem que diversos equipamentos que constituem uma rede possam comunicar entre si. É um protocolo estruturado também por camadas na qual cada camada utiliza e presta serviços às camadas adjacentes. Cada camada apenas trata das informações que correspondem à sua função.

O modelo TCP/IP quando comparado com o modelo OSI, tem duas camadas que se formam a partir da fusão de algumas camadas do modelo OSI, elas são (Figura 13.22): as camadas de Aplicação (Aplicação, Apresentação e Sessão) e Acesso à Rede (Ligação de dados e Física). Além disso, com a conclusão da migração da **Rede da Agência para Projetos de Pesquisa Avançada**, em inglês *Advanced Research Projects Agency Network* (ARPAnet)**,** financiada pelo departamento de defesa dos Estados Unidos, para o modelo TCP/IP em 1983, o modelo TCP/IP tem uma concretização em redes operacionais. Apesar da capacidade limitada do modelo TCP/IP no endereçamento dos dispositivos interconectados numa rede (Seção 13.4.2) e do problema de segurança dos dados, os protocolos TCP e IP são ainda os protocolos sobre os quais assenta a maioria das aplicações como se pode observar na Figura 13.23.

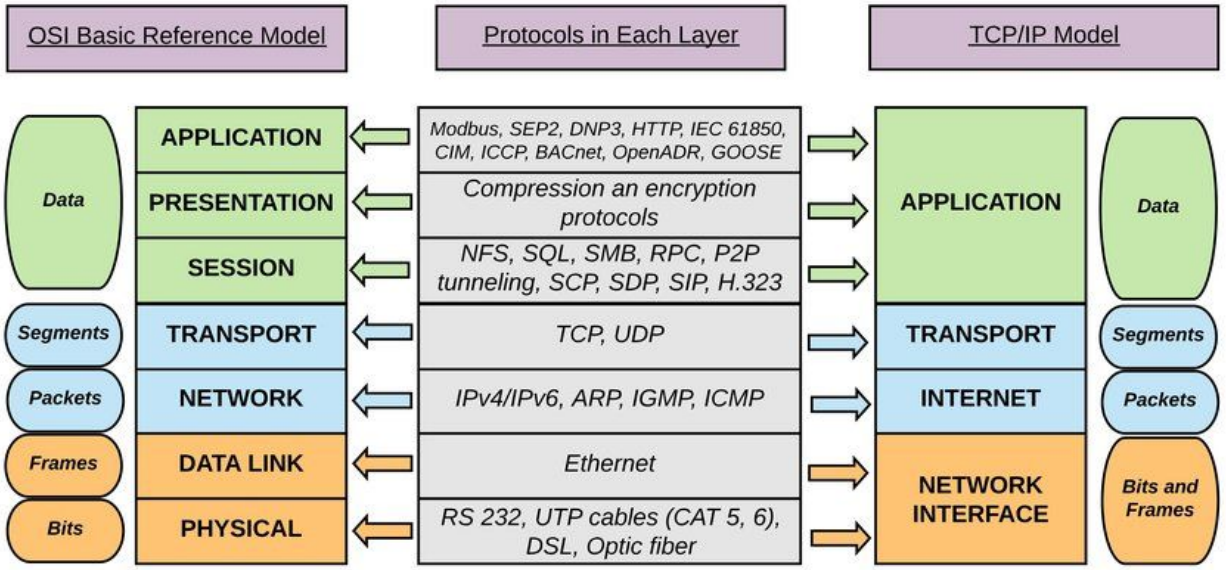


Figura 13.23: Modelos TCP/IP e OSI (Fonte: [15]).

O modelo TCP/IP é hoje o núcleo da *Internet*. Os dados são envelopados/encapsulados em diferentes formatos em cada camada, a fim de apoiar a tarefa de cada camada e aumentar a confiabilidade e a segurança nas transmissões dos dados através dos meios físicos. Figura 13.24 sintetiza os *bits* (cabeçalhos) adicionais inseridos nos dados em cada camada. Vimos na Seção 13.3.2.1 o significado dos *bits* adicionados para suportar o controle de fluxo e de detecção de erros. Nesta seção vamos ver os dados adicionais na camada de rede (camada 3), representado pelo protocolo IP, para executar a tarefa de roteamento de caminho para envio de um pacote de dados e de controle de congestionamento do tráfego dos dados. Alguns algoritmos muito aplicados no roteamento é o algoritmo de roteamento pelo menor caminho, pelo vetor de distância e pela quantidade de nós no caminho. E para o controle de congestionamento são aplicados os algoritmos cientes do tráfego, controle de admissão e remoção de pacotes “congestionadores”. E vamos ver os *bits* inseridos na camada de transporte, representado pelo protocolo TCP, para garantir a integridade dos segmentos de dados recebidos. Algoritmos de detecção e estratégias de correção de erros podem ser integrados como protocolos nesta camada.

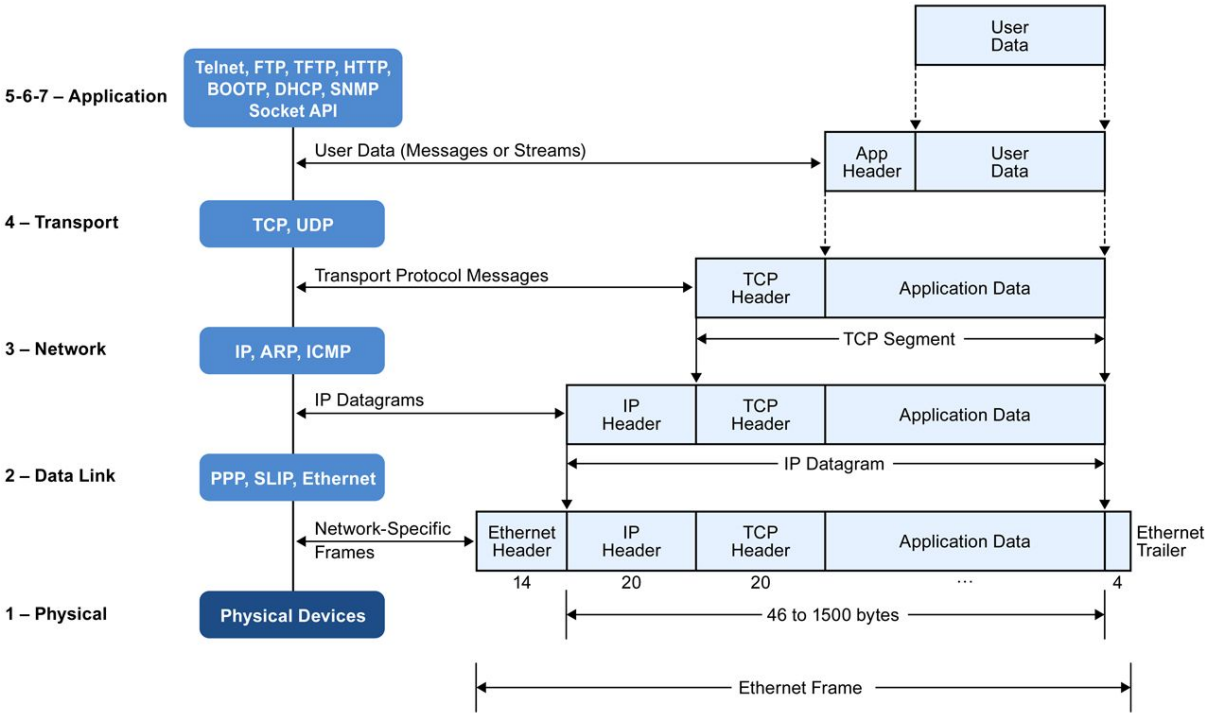


Figura 13.24: Formatos de dados numa implementação das camadas do modelo OSI (Fonte: [18]).

13.4.1 Protocolo TCP

(extraído de [27] e [28] com algumas adaptações)

O **TCP** é um dos principais protocolos da camada de transporte do modelo TCP/IP. Ele permite gerenciar os dados vindo da (ou com destino à) camada inferior do modelo (ou seja, o protocolo IP). Quando os dados são fornecidos ao protocolo IP, este encapsula-os em datagramas[11], fixando o campo do protocolo em 6 (para saber que o protocolo ascendente é o TCP). Como já comentamos na Seção 13.3.1.1, o TCP é um protocolo orientado para a conexão, isto é, ele permite que duas máquinas se comuniquem através dela, além de controlar o estado da transmissão.

As características do protocolo TCP são **entregar ordenadamente os datagramas** provenientes do protocolo IP, verificar o fluxo de dados para **evitar uma saturação** da rede, **formatar os dados em segmentos/datagramas de comprimento variável** para 'entregá-los' ao protocolo IP, permitir a **multiplexação dos dados**, ou seja, fazer circular, simultaneamente, as informações de fontes distintas na mesma linha e permitir o início e o fim de uma comunicação de maneira correta. Graças ao protocolo TCP, os aplicativos podem se **comunicar com segurança** (**pelo sistema de avisos de recepção** do protocolo TCP), independentemente das camadas

[11] De acordo com a Wikipedia, datagrama é "uma entidade de dados completa e independente que contém informações suficientes para ser roteada da origem ao destino sem precisar confiar em trocas anteriores entre essa fonte, a máquina de destino e a rede de transporte".

inferiores. Isto significa que os roteadores (que trabalham na camada da *Internet*) têm, como papel fundamental, o encaminhamento dos dados em forma de datagramas, sem se preocuparem com o controle dos dados, pois este é realizado pelo protocolo TCP. Caso o TCP detecte um segmento corrompido (**erro *end-to-end***), ele pode solicitar uma **retransmissão**.

Durante uma comunicação através do protocolo TCP, as duas máquinas devem estabelecer uma conexão. A máquina emissora (a que pede a conexão) chama-se **cliente**, enquanto que a máquina receptora se chama **servidor**. Dizemos, então, que estamos num ambiente Cliente-Servidor. As máquinas em tal ambiente se comunicam em **modo *full-duplex***. Para permitir o bom desenvolvimento da comunicação e de todos os controles que a acompanham, os dados são encapsulados, isto é, junto ao pacote de dados vai um cabeçalho que sincroniza as transmissões e assegura a sua recepção. Outra particularidade do TCP é poder controlar o débito dos dados graças à sua capacidade de emitir mensagens de dimensão variável. Estas mensagens são chamadas de **segmentos** ou **datagramas**. Um segmento TCP contém os campos mostrados na Figura 13.25.

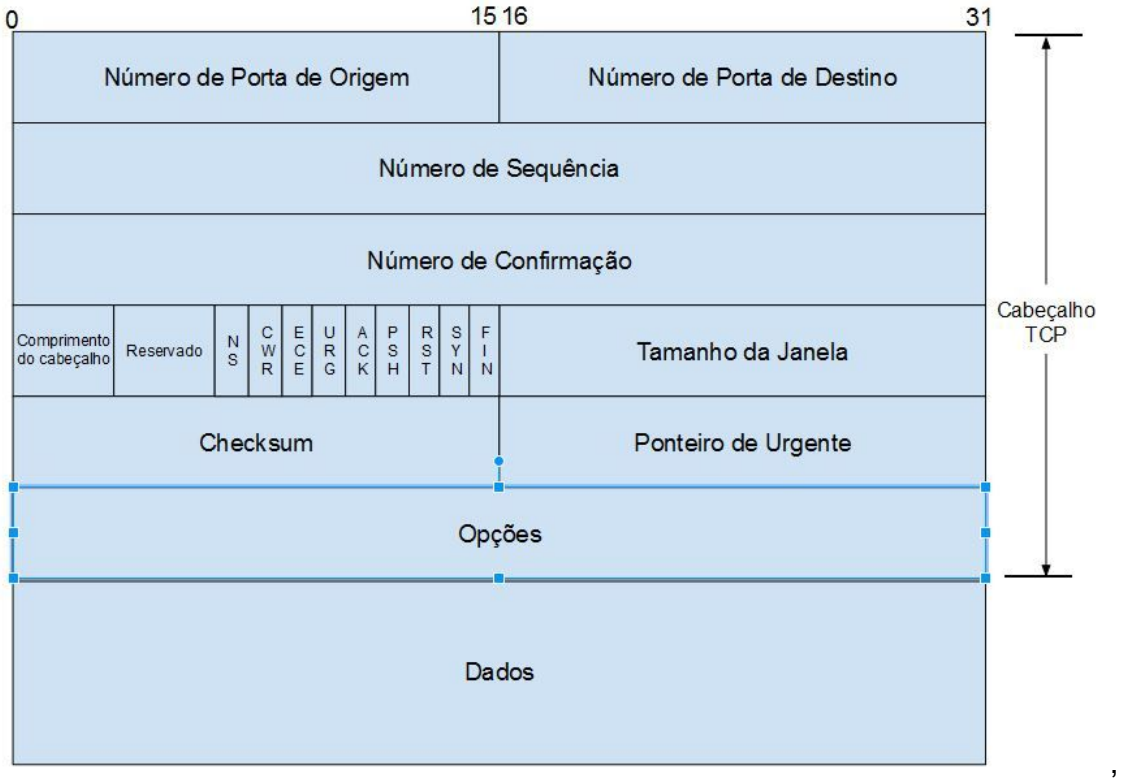


Figura 13.25: Formato de dados do protocolo TCP.

Os significados dos campos são:

- **Porta de Origem** (16 *bits*): porta relativa ao aplicativo em andamento na máquina fonte.

- **Porta de Destino** (16 *bits*): porta relativa ao aplicativo na máquina de destino.
- **Número de Sequência** (32 *bits*): quando a bandeira SYN é 0, o número de sequência é o da primeira palavra do segmento em andamento. Quando SYN é 1, o número de sequência será igual ao número de sequência inicial utilizado para sincronizar os números de sequência (ISN).
- **Número de Confirmação** (32 *bits*): o número de aviso de recepção, também chamado de **número de pagamento**, corresponde ao número (de sequência) do próximo segmento esperado, e não o número do último segmento recebido.
- **Comprimento de Cabeçalho** (4 *bits*): localiza o início dos dados no pacote. Aqui, o campo é essencial porque o campo de opções é de dimensão variável.
- **Reservada** (6 *bits*): campo não usado atualmente, mas previsto para o futuro.
- **URG**: se esta bandeira estiver em 1, o pacote deve ser tratado com urgência.
- **ACK**: se esta bandeira estiver em 1, o pacote representa um aviso de recepção.
- **PSH** (PUSH): se esta bandeira estiver em 1, o pacote funciona de acordo com o método PUSH.
- **RST**: se esta bandeira estiver em 1, a conexão é reiniciada.
- **SYN**: a bandeira **TCP SYN** indica um pedido de estabelecimento de conexão.
- **FIN**: se esta bandeira estiver em 1, a conexão é interrompida.
- **Tamanho da Janela** (16 *bits*): campo que permite conhecer o número de *bytes* que o receptor quer receber, sem aviso de recepção.
- Checksum ou CRC: a soma de controle é realizada fazendo a soma dos campos de dados do cabeçalho, para poder verificar a sua integridade.
- **Ponteiro de Urgência** (16 *bits*): indica o número de sequência a partir do qual a informação se torna urgente.
- **Opções** (dimensão variável): opções diversas.
- **Dados** (dimensão variável).

Através da multiplexação/demultiplexação, o TCP permite transitar, na mesma linha, dados de diversos aplicativos ou, em outras palavras, pôr em série as informações que chegam paralelamente. Estas operações são realizadas graças ao conceito de portas (ou *sockets*), ou seja, é o número associado a um aplicativo particular que, junto com um endereço IP, determina, de maneira única, um aplicativo que roda em uma determinada máquina.

Detalhes sobre o protocolo de estabelecimento de uma conexão antes do início de transmissão dos segmentos por uma técnica conhecida por aperto de mãos em três tempos, em inglês *three ways handshake* e de transmissão confiável dos segmentos podem ser encontrados em [27] e [28].

13.4.2 Protocolo IP

(extraído de [29] com algumas adaptações)

O protocolo de Internet, em inglês *Internet Protocol* (IP), é um protocolo de comunicação usado em todas as máquinas em rede para endereçamento e encaminhamento dos pacotes de dados. Figura 13.23 mostra que tanto no modelo OSI quanto no modelo TCP/IP, ele fica na camada de rede (modelo OSI)/camada de Internet (modelo TCP/IP). Os **pacotes** da Internet são divididos em duas partes: o cabeçalho, que, como um envelope, possui as informações de endereçamento da correspondência, e dados, que é a mensagem a ser transmitida propriamente dita. Na Figura 13.26 é ilustrado o formato de cabeçalho da versão 4 do protocolo IP. Note que os primeiros quatro *bits* do cabeçalho são reservados para a especificação da versão.

+	0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Versão	Tamanho do cabeçalho	*Tipo de Serviço* (ToS) (agora DiffServ e ECN)	Comprimento (pacote)	
32	Identificador			*Flags*	*Offset*
64	*Tempo de Vida* (TTL)		Protocolo	*Checksum*	
96	Endereço origem				
128	Endereço destino				
160	Opções				
192	*Dados*				

Figura 13.26: Formato do Cabeçalho do protocolo IPV4 (Fonte: [13]).

Os significados dos campos são:

- **Versão** (4 *bits*):versão do protocolo.
- **Tamanho do Cabeçalho** (4 *bits*): comprimento do cabeçalho em *bytes* até onde se iniciam os dados.
- **Tipo de Serviço (ToS)** (8 *bits*): serviços (segurança, confiabilidade, etc) requeridos no manuseio dos dados.
- **Comprimento (pacote)** (16 *bits*): tamanho do datagrama, incluindo o cabeçalho e os dados, em *bytes*.

- **Identificador** (16 *bits*): identificação dos fragmentos identificativos do datagrama IP original.
- **Flags** (3 *bits*): controle e identificação dos fragmentos.
- **Offset** (13 *bits*): permite que um receptor determine o local de um fragmento em particular no datagrama IP original.
- **Tempo de vida (TTL)** (8 *bits*): contagem de nós caminhados numa transmissão, evitando circuitos fechados sem fim.
- **Protocolo** (8 *bits*): protocolo seguinte usado.
- ***Checksum*** (16 *bits*): verificação do cabeçalho do datagrama.
- **Endereço de origem** (32 *bits*): endereço IP do nó transmissor numa conexão.
- **Endereço de destino** (32 *bits*): endereço IP do nó receptor.
- **Opções** (dimensão variável): opções diversas.
- **Dados** (dimensão variável).

Os roteadores são elementos distribuídos por toda a rede. Eles são como as estações de distribuição de correspondências, distribuindo os pacotes para outros roteadores mais próximos do destino final ou do próprio destino, se for o último elemento do caminho. A descoberta do caminho é realizada automaticamente pelos roteadores, através dos protocolos de roteamento. Esses protocolos, de maneira geral, se baseiam no anúncio dos vizinhos de um roteador para os seus adjacentes na rede. Assim, os roteadores descobrem todos os caminhos na Internet e para qual vizinho ele deve entregar cada pacote. Dentre os protocolos de roteamento mais usados, pode-se citar o RIP (*Route Information Protocol*), o OSPF (*Open Shortest Path First*) e o BGP (*Border Gateway Protocol*).

O endereço usado no Protocolo da Internet é o endereço IP. Atualmente, a versão mais utilizada do protocolo é a versão 4, que possui 32 *bits* no campo de endereço. Assim, existem quatro bilhões de endereços, aproximadamente. Esse número de endereços, embora grande, está próximo de ser totalmente utilizado e, a cada ano, aumenta-se a especulação sobre o uso da versão 6 do protocolo. A nova versão, por possuir 128 *bits* no campo de endereço, possibilita a inclusão na Internet de aproximadamente 256.000.000.000.000.000.000.000.000.000 trilhões de dispositivos na Internet, ou seja, seria como se pudéssemos endereçar, por exemplo, todos os grãos de areia de um deserto.

O endereço da versão 4 do protocolo IP, é dividido em quatro grupos de 8 *bits*, denominados octetos, ou seja, quatro números de 0 a 255, separados por pontos. O endereço IP é distribuído de forma hierárquica, formando sub-redes. Inicialmente, classificou-se as redes da Internet em 3 tipos: classe A, classe B e classe C. Essas classes eram definidas pelo seu tamanho. Quando uma empresa adquiria uma rede classe A, ela recebia o primeiro octeto fixo e tinha a liberdade de atribuir

internamente todos os endereços nos três últimos octetos. A classe C, por outro lado, dava para a empresa apenas 256 endereços diferentes, pois fixava os 3 últimos octetos. Tal estrutura se mostrou limitada, pois rapidamente usou-se todas as redes de classe B, pois considerava-se a classe C pequena para uma empresa e a classe A, grande demais. Na classe A, podia-se ter aproximadamente 16 milhões de estações.

A solução para o problema de endereçamento foi a criação da máscara de rede, adicionada ao IP com a tecnologia CIDR (*Classless InterDomain Routing*). A máscara de rede estabelece até qual dígito define a sub-rede e a partir de qual, tem-se os endereços de estações dentro das sub-redes. A máscara de rede possui 32 *bits*, assim como os endereços e são definidas como 1 para os *bits* correspondentes à rede e como 0 para as estações. Assim, possibilitou-se a criação de diversas redes fragmentando uma classe A ou agregando diversas classes C. Normalmente, expressa-se a máscara pelo número decimal correspondente aos 8 *bits*, por exemplo, o octeto 11111111 é apresentado como 255 e o octeto 11110000 é apresentado como 240.

No IP, no entanto, existem alguns endereços reservados. Toda a rede classe A, 127.0.0.0, com máscara de rede 255.0.0.0, é reservada para endereços locais na mesma máquina. Os endereços das redes 10.0.0.0/255.0.0.0, 172.16.0.0/255.240.0.0 e 192.168.0.0/255.255.0.0 são reservados para redes privadas, ou seja, não são vistos na Internet nem encaminhados pelos roteadores. Esses endereços costumam ser usados em redes internas, que utilizam o NAT (*Network Address Translation*) para compartilhar um endereço de IP público com diversos equipamentos, que utilizam endereços privados. Por fim, os endereços 224.0.0.0/240.0.0.0 são reservados para *IP Multicast*.

13.4.3 Interoperação entre TCP e IP

(extraído de [29])

Como vimos na Seção 13.4.1, o TCP recebe mensagens da **camada de aplicação** (camada 7 do modelo OSI), divide-as em datagramas de tamanho fixo e inserindo-lhes um cabeçalho e enviando-os de seguida para a camada IP. Estes dados não são tratados pela camada IP sendo que a principal função do IP consiste em encontrar um caminho que faça com que o datagrama chegue ao extremo da ligação. Para que os sistemas intermédios da rede retransmitam o datagrama, é adicionado um cabeçalho no pacote IP, que consiste principalmente num endereço IP de origem e de destino do datagrama e um número que corresponde ao protocolo usado na **camada de transporte**. Os pacotes IP à medida que passam por sub-redes são fragmentados em unidades menores.

Quando os pacotes IP chegam ao destino, são eventualmente reagrupados e enviados à camada TCP que é responsável pela verificação da integridade dos dados. Caso o *checksum* do pacote não coincida com o valor esperado e não seja possível recuperar o pacote, este é descartado e é enviada uma mensagem ao nó transmissor a pedir o reenvio deste pacote. Note que o TCP e o IP têm checksums separados por razões de eficiência e segurança.

13.5 *Internet* das Coisas

Quando se fala em Internet das Coisas, pensa-se imediatamente em interações máquina para máquina, em inglês machine-to-machine (M2M), e na complexa rede de comunicações que interconectam os *smart* dispositivos como discutimos na Seção 13.1. Do primeiro dispositivo conectado com a rede, que era uma máquina de venda automática de coca-cola no campus da Universidade Carnegie Mellon em 1982, até os dias de hoje, as coisas interconectadas se avolumaram tanto que os 32 *bits* previstos para os endereços IP já não são mais suficientes como vimos na Seção 13.4.2. Figura 13.27 ilustra um cenário de monitoramento dos indicadores do estado de saúde dos pacientes de um serviço médico.

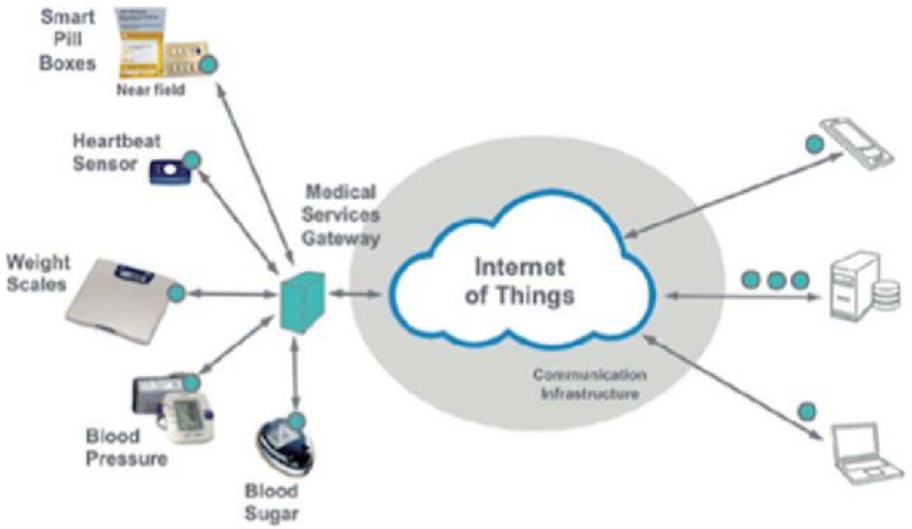


Figure 1: M2M Architecture

Figura 13.27: Arquitetura M2M (Fonte: [34]).

Junto com a rápida pervasividade das *smart* coisas, novos padrões, novos protocolos e novos barramentos estão sempre pipocando para atender demandas específicas [31], tornando difícil avaliar a interoperabilidade entre as novas tecnologias até para um conhecedor do assunto. Por exemplo, uma simples análise comparativa das características das três tecnologias de rede, Bluetooth (1994), Wi-Fi (1997) e ZigBee (2004), não é suficiente para tecermos conclusões sobre a interoperabilidade destas três tecnologias. Porém, se mapearmos as

funcionalidades que cada uma das tecnologias provê teremos uma ideia melhor das suas relações.

Tabela 13.3: Protocolos de comunicação sem fio (Fonte: [8]).

Parameter	Bluetooth® Low Energy (BLE)	Wi-Fi®	Zigbee®
Data Rate	1 – 3 Mbps	300 Mbps	20kb/s, 40 kb/s, 250kb/s
Frequency Band	2.4 GHz	2.4 GHz and 5 GHz	868/915 MHz, 2.4 GHz
Range	10m	190 m	100m
Security	E0 Stream cipher	WEP, WPA authentication, 128-bit Advanced Encryption Standard (AES), VPN, Firewall	128-bit AES
Risk of Data Collision	High		Medium
Maximum Number of Nodes	8	2,007	>65,000
Power Efficiency	Acceptable to Good	Varies	Excellent
Of Note	Once paired, connecting is automatic.	Connecting is automatic once it is set up.	Mesh capability creates greater signal reliability
Applications	To replace wiring in handheld devices.	The main connectivity resource for home, work, retail, and more.	Power-sipping applications; remote sensor and wireless controls
Benefits	Convenience, Cost, connect to Android, Blackberry, iOS, Tizen, and Windows.	Most widely used wireless connectivity solution. Connect to iOS and Android.	Reliable, Low Power, Cost effective, "Assemble and Forget"
Draw-backs:	Short range	Not always reliable. Higher power consumption	Not mainstream for connection to smartphones, etc.
IEEE	IEEE 802.15.1	IEEE 802.11n	IEEE 802.15.4
Markets	Mainly for portables. Widely adopted in consumer markets, retail	Ubiquitous; Widely adopted in nearly every market. Replaces cables in work areas or homes.	Better known in Industrial markets, smart homes, smart lighting.
Attractiveness as a hacking target:	Low to medium	High	Low
Find ready-to-connect modules at:	mouser.com, adafruit.com, sparkfun.com	mouser.com, adafruit.com, sparkfun.com	mouser.com, adafruit.com, sparkfun.com
Learn more at:	www.bluetooth.com	www.wi-fi.org	www.zigbee.com

13.5.1 Tecnologias em Rede sem Fio

Figura 13.28 sintetiza comparativamente as tecnologias desenvolvidas para *Internet* das Coisas em relação às tecnologias desenvolvidas para *Internet* dos Humanos no contexto do modelo OSI [31]. Observe que a comunicação sem fio já inicia desde a camada física na *Internet* das Coisas através do uso do protocolo IEEE 802.15.4. Este protocolo efetua o controle de acesso para redes sem fio pessoais (WPAN) de baixo custo e de baixas taxas de transmissão (até 250kbit/s) entre dispositivos próximos até uma distância média de 10 metros. Como o protocolo Wi-Fi, a técnica

CSMA/CA é aplicada para evitar colisões nos meios físicos. Na camada de rede, a versão 6 de IP é adotada principalmente por problema de endereçamento de trilhões de coisas espalhadas pelo mundo afora. Na camada de transporte, note que o protocolo UDP, que utiliza somente os serviços básicos de IP sem verificar se pacote chega ao seu destino corretamente (Seção 13.2), é preferido para as aplicações IoT. As maiores diferenças acontecem, porém, nas camadas de aplicações onde os conceitos de sessão, apresentação e aplicação por si, divergem muito nas interfaces homem-homem e máquina-máquina.

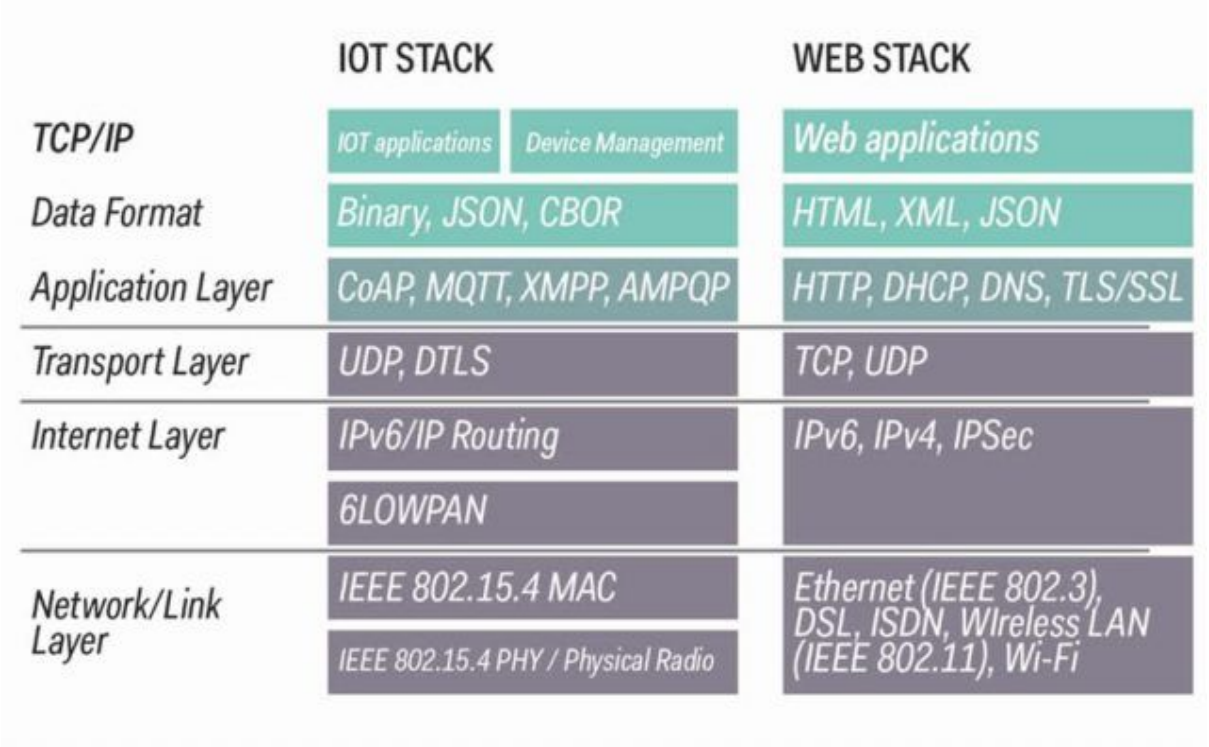


Figura 13.28: Internet das Coisas x Internet dos Humanos (Fonte: [31]).

13.5.2 Mapeamento no Modelo OSI

Na Seção 13.3.2.2 vimos a posição da tecnologia wi-fi no modelo OSI e na Figura 13.28 mostramos a posição da tecnologia MQTT (*Message Queuing Telemetry Transport*) no modelo OSI. MQTT é um protocolo de mensagens leve para sensores e pequenos dispositivos móveis otimizado para redes TCP/IP [32]. O protocolo é assíncrono, baseado no modelo *publish-subscribe*, e permite que os sensores clientes iniciem uma conexão como mostra a Figura 13.29. MQTT foi desenvolvido por dois engenheiros Andy Stanford-Clark (IBM) e Arlen Nipper (Eurotech) em 1999.

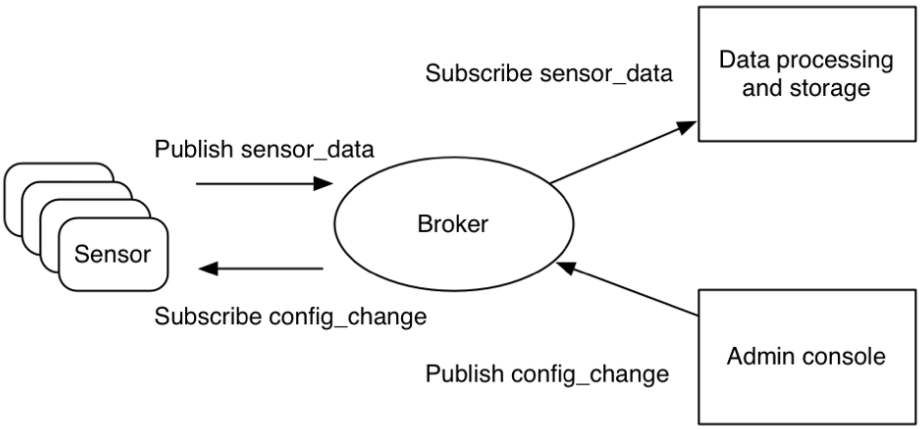


Figura 13.29: Protocolo MQTT: modelo publish-subscribe (Fonte: [33])

O dispositivo que inspirou o nome de *Internet* das Coisas é a tecnologia de identificação por radiofrequência, em inglês *Radio-Frequency Identification*, que tem suas raízes nos sistema de radares utilizados na Segunda Guerra Mundial. Uma etiqueta RFID é um transponder[12], implementado com um controlador e uma antena, tipicamente colocada em uma pessoa, animal, equipamento, embalagem ou produto, tornando-os capazes de responder aos sinais de radiofrequência enviados por uma base transmissora. Com isso, é possível identificar um produto a uma distância maior do que a dos *scanners* clássicos. Hoje em dia estas etiquetas já evoluíram para as semi-passivas e ativas, capazes de enviarem os seus próprios sinais. Na Figura 13.30 temos o mapeamento das funcionalidades de uma etiqueta RFID no modelo OSI. Essencialmente, ele tem a camada física constituída de uma antena de radiofrequência (leitor), um controlador responsável pelo processamento dos sinais de radiofrequência e a comunicação com o resto do sistema (*middleware*), incluindo a conversão de informações num formato interpretável pelo seu usuário se necessário (interface homem-máquina).

[12] Transponder é um aparelho **trans**mitter-res**ponder** que responde automaticamente a uma mensagem de identificação, ao sinal de um radar. É uma espécie de repetidor de radiofrequência.

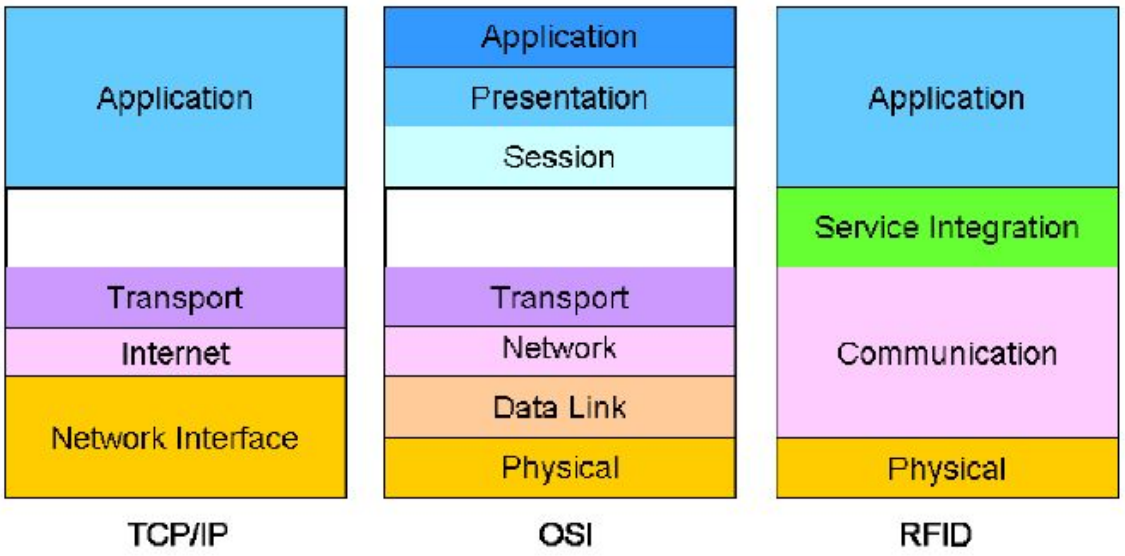


Figura 13.30: Etiqueta RFID mapeada no modelo OSI.

O protocolo ZigBee foi concebido na década 90 para uma rede sem fio auto-organizável de uso pessoal operando na faixa de frequência ISM, de 2.400 a 2.485 GHz. É um protocolo de comunicação definido em cima do padrão IEEE 802.15.4. Ele foi projetado para uma baixa taxa de transferência, baixo consumo de energia, baixa complexidade e uma rede de baixo alcance. O seu posicionamento em relação às camadas do modelo OSI é mostrado na Figura 13.31.

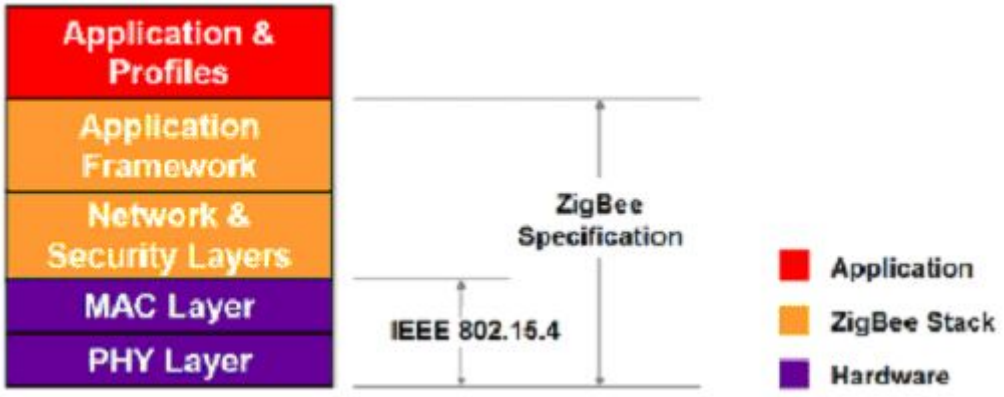


Figura 13.31: ZigBee mapeado no modelo OSI.

Bluetooth, por sua vez. é um padrão de tecnologia sem fio projetado para troca de dados entre dispositivos móveis e fixos numa distância pequena operando também na frequência ISM . Foi concebido originalmente pelo Dr. Jaap Haartsen da Ericsson em 1994, pensando numa alternativa, sem fio e de baixo consumo de energia, para comunicações cabeadas de sinais de áudio (voz) via o protocolo RS-232. Os dispositivos Bluetooth possuem obrigatoriamente seis elementos de *hardware*, como mostra a Figura 13.32:

- ***Host Controller***: responsável pelo código de processamento dos códigos de alto nível;
- ***Link Control Processor***: responsável pelo processamento das camadas inferiores de protocolos;
- ***Based Band Controller****:* responsável pelo controle do *transceiver* de rádio frequência;
- ***RF transceiver****:* responsável pela detecção de dados e síntese de radiofrequência;
- ***RF front-end****:* responsável pela troca de estados entre receptor e emissor; Antena: Responsável pela transmissão do sinal.

Figura 13.32 mostra um mapeamento das tecnologias envolvidas no Bluetooth no modelo OSI. Ela agrega ainda uma série de técnicas relacionadas com o processamento de sinais no nível físico e no nível algorítmico que fogem do escopo deste curso.

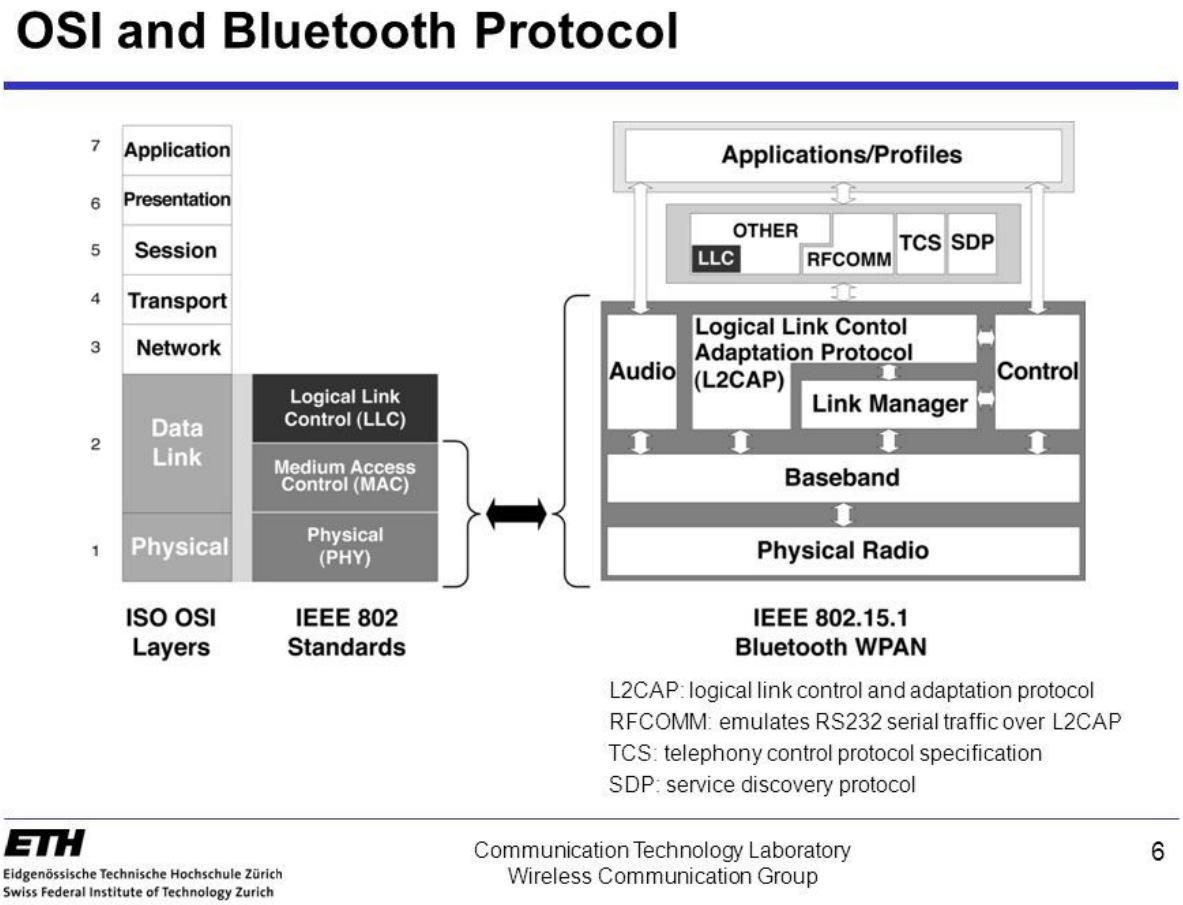


Figura 13.32: Mapeamento do protocolo Bluetooth em 7 camadas do modelo OSI.

13.6 Exercícios

1. Qual é a relação entre a tecnologia de computação, a tecnologia de rede e os processos físicos no desenvolvimento de um sistema ciber-físico? Há interações humanas?
2. O que você entende por uma arquitetura M2M? Há interações humanas?
3. O que você entende pelo modelo OSI? Quais são as 7 camadas consideradas neste modelo? E qual é a função de cada camada? Quais são as unidades de dados de cada camada?
4. Qual é a diferença entre *hubs*, *switches* e *roteadores*? Até qual camada do modelo OSI podem ser encontrados estes dispositivos?
5. A qual das camadas do modelo OSI você associaria os protocolos de comunicação serial (RS-232, I2C, SPI) e paralela (Centronics)? Justifique.
6. A qual das camadas do modelo OSI você associaria o protocolo Ethernet e o protocolo Wi-Fi? Justifique.
7. Quais são as camadas cobertas pelo padrão IEEE 802? Quais são as duas principais diferenças entre os protocolos IEEE 802.3, IEEE 802.11 e IEEE 802.15?
8. A camada de enlace de dados é dividida em duas sub-camadas: a sub-camada LLC e a sub-camada MAC. Qual das duas sub-camadas é responsável pelo controle do fluxo e pela multiplexação de dados nos transmissores e receptores? Justifique.
9. Como os dispositivos físicos são endereçados na camada de enlace de dados? Quais são as técnicas mencionadas no capítulo para arbitrar o acesso a um meio de comunicação?
10. Quais camadas do modelo ISO podem ter protocolos de controle de erros ARQ (*Automatic Repeat reQuest*)? Justifique.
11. Tanto a camada de transporte quanto a camada de enlace de dados conseguem detectar erros numa transmissão. Os erros detectáveis pelas duas camadas são de mesma natureza?
12. Quais são as diferenças e as semelhanças entre os modelos OSI e modelo TCP/IP?
13. Como os pacotes de dados da camada de rede são tratados pelo protocolo TCP e pelo protocolo UDP na camada de transporte do modelo OSI?
14. Qual das camadas do modelo OSI é responsável pela segurança/privacidade dos dados?
15. Quais são as técnicas de controle de congestionamento e roteamento aplicadas no protocolo IP?
16. Como você pode identificar a classe de um IP a partir do endereço?
17. Quais são os formatos de dados do protocolo Ethernet, TCP e IP?

18. Quais são os três principais componentes de um sistema de Internet das Coisas?
19. Como a capacidade de endereçamento do protocolo IPv4 pode limitar o crescimento de *smart* coisas?
20. Explique, com uso do modelo OSI, as principais diferenças entre a arquitetura de um sistema baseado em Web e a arquitetura de um sistema baseado em internet das coisa.
21. O que é uma banda ISM? A quais aplicações ela é destinada?
22. Cite 5 aplicações em que são predominantes as interfaces M2M.

13.7 Referências

[1] Micro Finance Journal. Automotive Systems: Technology in today's vehicle. http://microfinancejournal.com/2019/07/31/global-embedded-systems-market-2019-trends-renesas-electronics-stmicroelectronics-nxp/
[2] Renesas. In-Vehicle Networking Solutions. https://www.renesas.com/sg/en/solutions/automotive/technology/networking-solutions.html
[3] Bhargay P. Upender e Philip J. Koopman Jr. Communication Protocols for Embedded Systems. https://users.ece.cmu.edu/~koopman/protsrvy/protsrvy.html
[4] Anson He. Basic Eletronics: Wired Communication Protocols in Embedded Design. https://www.seeedstudio.com/blog/2019/07/03/basic-electronics-wired-communication-protocols-in-embedded-design/
[5] Abinayaa B. Communication Protocols in Embedded Systems - Types, Advantages & Disadvantages. https://electricalfundablog.com/communication-protocols-embedded-systems/
[6] Tarun Agarwal. Basic Concepts of Wireless Communication Systems. https://www.efxkits.co.uk/fundamentals-of-wireless-communication-system/
[7] Tarun Agarwal. Electronics Projects Kits on Wireless Sensor Networks for Electronics BEng. http://www.efxkits.co.uk/wireless-sensor-networks-based-projects-for-electronics-beng/
[8] Scott Thornton. Wireless and MCUs: Bluetooth, Wi-Fi, or Zigbee? https://www.microcontrollertips.com/wireless-mcus-bluetooth-wi-fi-zigbee/
[9] Wikipedia. List of Wi-Fi microcontrollers. https://en.wikipedia.org/wiki/List_of_Wi-Fi_microcontrollers
[10] Wikipedia. Internet of Things. https://en.wikipedia.org/wiki/Internet_of_things
[11] Wikipedia. OSI Model. https://en.wikipedia.org/wiki/OSI_model
[12] Yuri Matheus. Diferenças entre Hubs e Switches. https://www.alura.com.br/artigos/diferencas-entre-hubs-e-switches/
[13] Wikipedia. Protocolo de Internet. https://pt.wikipedia.org/wiki/Protocolo_de_Internet.
[14] Margaret Rouse. OSI model (Open Systems Interconnection). https://searchnetworking.techtarget.com/definition/OSI
[15] https://www.researchgate.net/figure/The-logical-mapping-between-OSI-basic-reference-model-and-the-TCP-IP-stack_fig2_327483011

[16] https://www.electronicdesign.com/what-s-difference-between/what-s-difference-between-osi-seven-layer-network-model-and-tcpip
[17] https://www.slideshare.net/00priya33/osi-model-25757020
[18] Micrium. People Internet vs. Device Internet. https://www.micrium.com/iot/internet-protocols/
[19] Wikipedia. List of Network Protocols (OSI model). https://en.wikipedia.org/wiki/List_of_network_protocols_(OSI_model)
[20] Wikipedia. Network performance. https://en.wikipedia.org/wiki/Network_performance
[21] Speedcheck. Ethernet. https://www.speedcheck.org/pt/wiki/ethernet/
[22] Wikipedia. Ethernet. https://en.wikipedia.org/wiki/Ethernet
[23] https://profinetuniversity.com/industrial-automation-ethernet/network-reference-model/
[24] InfoWester. O que é Wi-Fi (IEEE 802.11)? https://www.infowester.com/wifi.php
[25] https://en.wikipedia.org/wiki/File:OSI_layer_model_with_1905.1_sub-layer.jpg
[26] CCM. O Protocolo TCP. https://br.ccm.net/contents/284-o-protocolo-tcp
[27] https://ptolemy.berkeley.edu/projects/cps/
[28] Wikipedia. Transmission Control Protocol. https://pt.wikipedia.org/wiki/Transmission_Control_Protocol#Origem_hist%C3%B3rica
[29] Pedro Pisa. O que é IP? https://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-ip.html
[30] Pequena história da Internet. https://paginas.fe.up.pt/~mrs01003/TCP_IP.htm
[31] Nicolas Windpassinger. What is series (#1): what is the OSI reference model? https://nicolaswindpassinger.com/osi-reference-model
[32] MQTT. http://mqtt.org/
[33] https://developer.ibm.com/articles/iot-mqtt-why-good-for-iot/
[34] Priyanka Thota e Yoohwan Kim. Implementation and Comparison of M2M Protocols for Internet of Things. https://www.semanticscholar.org/paper/Implementation-and-Comparison-of-M2M-Protocols-for-Thota-Kim/a8436c087965afd23a99b2ea8805135ddbf2ddd8
[35] GeeksForGeeks. Ethernet Frame Format. https://www.geeksforgeeks.org/ethernet-frame-format/
[36] Wikipedia. Identificação por Radiofrequência. https://pt.wikipedia.org/wiki/Identifica%C3%A7%C3%A3o_por_radiofrequ%C3%AAncia