

**Universidade de São Paulo**

**Escola de Engenharia de São Carlos**

**Departamento de Engenharia Elétrica**

**Trabalho de Conclusão de Curso**

# **Uso de Ethernet em Automação Industrial**

**Autor:**

**Guilherme Serpa Sestito**

**Número USP: 5716647**

**Orientador:**

**Prof. Dr. Dennis Brandão**

**São Carlos, Novembro de 2011.**



**Guilherme Serpa Sestito**

# **Uso de Ethernet em Automação Industrial**

Trabalho de Conclusão de Curso apresentado à  
Escola de Engenharia de São Carlos,  
da Universidade de São Paulo.

Curso de Engenharia Elétrica com  
ênfase em Sistemas de Energia e  
Automação

ORIENTADOR: Prof. Dr. Dennis Brandão

São Carlos, 2011

AUTORIZO A REPRODUÇÃO E DIVULGAÇÃO TOTAL OU PARCIAL DESTE TRABALHO, POR QUALQUER MEIO CONVENCIONAL OU ELETRÔNICO, PARA FINS DE ESTUDO E PESQUISA, DESDE QUE CITADA A FONTE.

Ficha catalográfica preparada pela Seção de Tratamento  
da Informação do Serviço de Biblioteca – EESC/USP

Sestito, Guilherme Serpa.

S494u      Uso da *Ethernet* em automação industrial ; orientador  
Dennis Brandão -- São Carlos, 2011.

Monografia (Graduação em Engenharia Elétrica com  
ênfase em Sistemas de Energia e Automação) -- Escola de  
Engenharia de São Carlos da Universidade de São Paulo,  
2011.

1. *Ethernet*. 2. *PROFINET*. 3. Automação industrial. 4.  
Profibus. 5. Protocolo. I. Título.

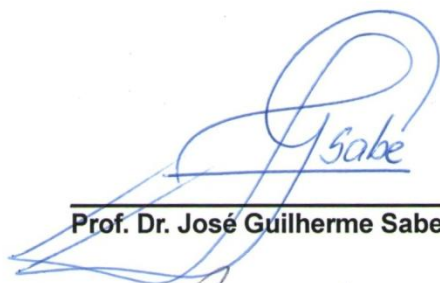
# FOLHA DE APROVAÇÃO

Nome: Guilherme Serpa Sestito

Título: "Uso de Ethernet em Automação Industrial"

Trabalho de Conclusão de Curso defendido e aprovado  
em 25 / 11 / 2011,

com NOTA 9,70 (nove , setenta), pela comissão julgadora:



Prof. Dr. José Guilherme Sabe - EESC/USP



MSc. Paulo Henrique Toledo de Oliveira e Souza - EESC/USP



Prof. Associado Homero Schiabel  
Coordenador da CoC-Engenharia Elétrica  
EESC/USP



## Dedicatória

Aos meus pais, Moacir e Silvia, obrigado por todo carinho, suporte e presença que tiveram durante toda a minha vida, pois, sem tudo o que vocês me proporcionaram, eu não teria chegado até aqui. Com imensa gratidão, muito obrigado!





## Agradecimentos

Este trabalho caracteriza-se como o primeiro trabalho destinado ao estudo do padrão de comunicação PROFINET do Laboratório de Automação Industrial (LAI). Enfrentou as dificuldades inerentes à falta de domínio da tecnologia e à falta de equipamentos. Ainda que sejam fadadas aos primeiros as críticas, também é destinado aos pioneiros o reconhecimento.

Chegar até aqui implicou em muitas horas de estudo, dedicação, dúvidas e incertezas. Agradeço assim:

- ao meu amigo e meu orientador, professor Dr. Dennis Brandão. Pelas oportunidades e pelos ensinamentos durante esses anos de graduação.

- ao professor Dr. José Guilherme Sabe, por gentilmente permitir a minha entrada na empresa Equitron.

- ao engenheiro Guilherme Fernandes, que soube de forma brilhante adequar a realidade da empresa às necessidades do projeto.

- aos amigos Carlos Henrique Juliano e Rui Bertho Junior, pelo incomensurável apoio.

- aos amigos de graduação: Juliana Aramizu, Alexandre Luis Matas e Vinícius de Cillo Moro, Bruno de Almeida, Daniel Ferreira e Oureste Batista, pela amizade e principalmente pelos momentos agradáveis que partilhamos.

- a todos os funcionários do departamento de Engenharia Elétrica da USP – São Carlos que me ajudaram na elaboração deste trabalho, em especial ao Rui Bertho, Vera e a Jussara.

- aos amigos e pesquisadores do *Automation Research Centre*, em Limerick na Irlanda: Declan, Peter e Hassan, obrigado por tudo.

- aos amigos Nathália e Luis, não saberia expressar a gratidão pelo apoio durante os longos meses em Limerick.

- aos pesquisadores do LAI EESC- USP: Guilherme Rossi e André Cavalcanti, pela amizade e companheirismo.

- aos amigos André F. Sabe, Herivelto Cordeiro dos Santos e Paulo Henrique Toledo de Oliveira e Souza, pelos ensinamentos e pela amizade.

- aos amigos Pedro Soares, Daniela Terenzi e Marcos Puydinger, pelos bons momentos juntos.

- a Maria Clementina, pelo carinho dado em toda minha vida.

- aos meus irmãos Rodrigo e Marília, por estarem presentes em minha vida.

- aos meus amigos: Guilherme, Marcelo, Maurício, Leonardo, Gabriel, Renato, Marcos e Mário pelos bons momentos juntos e pela amizade.

Enfim, a todos que, de alguma forma, vieram a contribuir para a concepção deste trabalho. Valeu pessoal!!!

# Sumário

<b>Capítulo 1</b>	<b>1</b>
Introdução	1
1.1 Organização do trabalho	2
<b>Capítulo 2</b>	<b>5</b>
Revisando conceitos	5
2.1 O modelo OSI	5
2.1.1 Camada física	24
2.1.2 Camada de Enlace	25
2.1.3 Camada de Rede	25
2.1.4 Camada de Transporte	26
2.1.5 Camada de Sessão	26
2.1.6 Camada de Apresentação	26
2.1.7 Camada de Aplicação	26
2.2 TCP/IP	27
2.2.1 Camada de aplicação	27
2.2.2 Camada de Transporte	28
2.2.3 Camada de Internet	28
2.2.4 Camada de Interface com a Rede	28
2.2.5 Endereçamento IP	28
2.2.6 Máscara de Rede	30
2.3 Ethernet30	
2.3.1 A camada física	32
2.3.1.1 CSMA /CD	32
2.3.1.2 Transmissão de dados.	33
2.3.1.3 Codificação NRZ	34
2.3.1.4 Codificação Manchester	35
2.3.1.5 Codificação MLT-3	35
2.3.1.6 Codificação 4B/5B	36
2.3.1.3 Placa de Rede	37
2.3.1.4 Cabeamento	37
2.3.2 A camada MAC	38
2.3.2.1 Endereçamento MAC	38
2.3.2.2 Quadro Ethernet	39
2.3.3 A camada LLC	40
<b>Capítulo 3</b>	<b>25</b>
O protocolo PROFINET	25
3.1 Introdução	25
3.2 As versões do PROFINET	28
3.2.1 PROFINET IO	28
3.2.1.1 Integração	30
3.2.1.2 O modelo de comunicação	30
3.2.1.3 Identificação	33

3.2.1.4 Arquivo GSD	33
3.2.1.5 Endereçamento do dispositivo no campo	34
3.2.1.6 Parametrização	34
3.2.1.7 Diagnóstico	35
3.2.1.8 Detecção da topologia	36
3.2.2 PROFINET CBA	37
3.3 Componentes da rede	38
3.3.1 Conectores para ambientes internos	38
3.3.2 Conectores para ambientes externos	40
3.3.2 Meios de transmissão	41
3.3.2.1 Cabos de cobre	41
3.3.2.1 Fibra Ótica	42
3.3.3 A switch	43
3.4 Conformance Classes	45
3.5 Topologias de rede	47
3.6 Wireless	48
3.6.1 PROFINET com comunicação WLAN	49
3.6.2 Comunicação PROFINET via Bluetooth	49
3.7 Segurança	51
<b>CAPÍTULO 4</b>	<b>55</b>
O estudo de caso	55
4.1 Introdução	55
4.2 A arquitetura	56
4.3 As análises	57
4.4 Comparação dos protocolos	61
4.4.1 Jitter	61
4.4.2 A comparação	62
<b>CAPÍTULO 5</b>	<b>69</b>
Conclusão	69
<b>Referências Bibliográficas</b>	<b>71</b>

## Índice de Figuras

Figura 1: As camadas do modelo OSI. Fonte [1]	24
Figura 2: Arquitetura TCP/IP. Fonte [1]	27
Figura 3: Campos de um endereço IP. Fonte [2]	29
Figura 4: Classes de endereços IP. Fonte [2]	29
Figura 5: Switch (a) simples e (b) com buffer. Fonte [7]	31
Figura 6: Modelo da arquitetura Ethernet. Fonte [2]	32
Figura 7: Codificação do sinal em Ethernet e no protocolo Profibus. Fonte [23]	34
Figura 8: Nível lógico alto e baixo da codificação Manchester. Fonte [23]	35
Figura 9: Estrutura do endereço MAC. Fonte [2]	39
Figura 10: Estrutura do frame Ethernet. Fonte [2]	39
Figura 11: Estrutura do quadro Ethernet com a camada de Controle do Link Lógico (LLC). Fonte [2]	41
Figura 12: Curvas de crescimento de nós instalados Profibus e PROFINET. Fonte [10]	26
Figura 13: Divisão do mercado dos protocolos baseados em Ethernet.	26
Figura 14: Modelo de comunicação em PROFINET. Fonte: [4]	29
Figura 15: Integração via proxy com PROFINET IO. Fonte [14]	30
Figura 16: Tempo de ciclo e jitter para cada classe de comunicação. Fonte [15]	31
Figura 17: Os quatro graus de determinismo. Fonte [23]	32
Figura 18: Canais de comunicação em PROFINET. Fonte [11]	32
Figura 19: Detecção da topologia. Fonte [11].	37
Figura 20: Subdivisão dos processos usando PROFINET CBA. Fonte [14]	38
Figura 21: Conector RJ45 para ambientes internos.	39
Figura 22: Conector de fibra ótica.	39
Figura 23: Conector RJ45 para ambientes externos.	40
Figura 24: Conector M12 para ambientes externos.	40
Figura 25: Modos de operação da switch via serviço de rede. Fonte [18]	44
Figura 26: Os parâmetros da switch. Fonte [18]	45
Figura 27: Exemplos de topologias de rede. Fonte: [11]	48
Figura 28: Vários sinais wireless presentes em uma planta industrial. Fonte [19]	50
Figura 29: Rede Profibus.	56
Figura 30: Rede PROFINET.	57
Figura 31: Aquisição dos dados com o software Wireshark.	58
Figura 32: Quantidade de bytes por frame do protocolo PROFINET- PTCP.	58
Figura 33: Quantidade de bytes por frame do protocolo LLDP.	59
Figura 34: Quantidade de frames enviados por cada protocolo.	60
Figura 35: Quantidade de bytes enviados por cada protocolo.	60
Figura 36: Situações de Jitter.	61
Figura 37: Mensagem de multicast da rede PROFINET.	62
Figura 38: Histograma do jitter nas mensagens LLDP	64
Figura 39: Histograma do jitter visto nas mensagens PROFINET PTCP.	65
Figura 40: Bytes transmitidos pelo Profibus.	66
Figura 41: Histograma do jitter nas mensagens Profibus.	66



## Índice de Tabelas

Tabela 1: Divisão dos endereços IP em classes. _____	29
Tabela 2: Codificação de grupos de 4 bits para grupos de 5 bits. _____	36
Tabela 3: Relação de pinos dos conectores RJ45 para ambientes internos. _____	39
Tabela 4: Relação de pinos dos conectores M12 para ambientes externos. _____	40
Tabela 5: Parâmetros do cabo de cobre tipo A. _____	42
Tabela 6: Comprimento máximo da fibra ótica conforme seu tipo. _____	43
Tabela 7: Propriedade das Conformances Classes. _____	46
Tabela 8: Checklist visual da rede. _____	52
Tabela 9: Tempo entre dois eventos sucessivos iguais dos respectivos protocolos. _	63
Tabela 10: Variação do tempo em torno dos valores de referencia. _____	63





## Resumo

SESTITO G. S. *Uso de Ethernet em Automação Industrial*. 2011. Trabalho de Conclusão de Curso – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2011.

Este trabalho propõe um estudo do uso do padrão de comunicação Ethernet para automação industrial. Serão apresentadas primeiramente as características do protocolo Ethernet. Houve necessidade de expor os conceitos do modelo OSI para que fossem revistos. O foco principal do trabalho é estudar o protocolo baseado em Ethernet denominado PROFINET. Por isso, optou-se por mostrar as particularidades do protocolo TCP/IP para que a base teórica do protocolo estudado fosse ressaltada. No capítulo destinado ao estudo do protocolo PROFINET, são definidos aspectos do modelo de comunicação, regras de instalação, segurança, configuração, parametrização e diagnóstico. Todos baseados nas normas internacionais que regem o padrão. Não obstante, a fim de enriquecer o trabalho, foi realizado um estudo de caso que possibilita a comparação do protocolo estudado com o protocolo Profibus. Foram comparados aspectos importantes que possibilitam a compreensão da teoria apresentada anteriormente. Comparando-se o *jitter* em porcentagem do tempo de ciclo dos protocolos Profibus e PROFINET, verificou-se que o primeiro apresentou resultado mais satisfatório, todavia, conclui-se o trabalho ressaltando que ambos os padrões de comunicação industrial são alternativas viáveis para o exigente ambiente industrial, diferenciando-se em suas particularidades.

**Palavras-chaves:** Ethernet, PROFINET; Automação Industrial; Profibus; Protocolo.



## Abstract

SESTITO G. S. *The Usage of Ethernet in Industrial Automation*. 2011. Course Conclusion Work – Engineering School of São Carlos, University of São Paulo.

This paper proposes a study of the usage of the Ethernet communication protocol for Industrial Automation. At first, the features of this protocol will be presented. It was thought about presenting the concept of ISO model in order to review them. The main goal is to study an Ethernet based protocol denominated PROFINET. Then, it was chosen to show the TCP/IP protocol features to improve the theoretical base needed to understand the PROFINET protocol. In the chapter about the PROFINET protocol, aspects about the communication model, install rules, safety, configuration, parameterization and diagnostic are defined. All of them based on international rules that give the directives for the standard. Notwithstanding, in order to improve the paper, a case study was done to enable the comparison between the communication standard and the Profibus protocol. Important aspects were analyzed and compared, which turned able the understanding of the theory shown before. Comparing the jitter in function of its cycle time percentage of both protocols, it was verified that the Profibus one has the most satisfying results, but to sum up the paper, it's emphasized that both protocols are viable to the demanding factory environment, varying only from theirs peculiarities.

**Key-words:** Ethernet, PROFINET; Industrial Automation; Profibus; Protocol.



# Capítulo 1

## Introdução

Nos últimos 20 anos, as redes de automação industrial têm se tornado cada vez mais complexas pela sofisticação dos protocolos utilizados e pelo considerável aumento do número de atuadores e sensores. A tendência proposta é elevar cada vez mais o nível de automação fabril e minimizar a atuação humana nos processos a fim de reduzir custos, atenuar erros e ampliar o nível de complexidade dos equipamentos produzidos. [1]

Na década de 90, surgiram os primeiros protocolos de campo, também denominados *fieldbuses*, como o Modbus, HART, Profibus FMS, e o Fieldbus Foundation. Com eles, também veio à redução do cabeamento e a consequente redução dos custos referentes à instalação das redes industriais. [1]

Depois de implementados e testados, a robustez, praticidade e eficiência apresentadas pelos protocolos de campo geraram um tema de pesquisa antes não existente. Criaram-se associações entre universidades e empresas, além disso, empresas, por si mesmas, começaram a desenvolver produtos, tecnologias, novos protocolos e revisar, periodicamente, os protocolos já existentes, com a finalidade de aprimorá-los.

A complexidade dos sistemas de automação atuais é tão grande que, em aplicações industriais modernas, deve-se compreender o sistema de automação como um sistema de controle hierárquico de múltiplas camadas, composto por uma série de equipamentos e dispositivos. [2]. Tradicionalmente, uma rede de comunicação industrial é composta por três níveis de comunicação: o nível de controle, o de campo e o de sensores. A rede de controle é geralmente uma rede Ethernet, ao passo que a rede de campo é tipicamente um barramento serial de alta velocidade como o RS485. Já em níveis de sensores, a comunicação é majoritariamente ditada por sinais discretos como o 4-20 mA ou sinais elétricos de 24V [1]. No entanto, o foco das novas gerações de protocolos é baseado no uso de Ethernet.

Contrária à tendência original, há esforço para utilizar a Ethernet em todos os níveis, com a intenção de usar a simples tecnologia de rede, desde o do nível de sensores até o escritório das empresas. [3]

Inicialmente, a Ethernet era considerada inadequada para ambientes industriais agressivos pela insuficiente imunidade a ruídos, conectores inadequados e comunicação em tempo real. Porém, muitas organizações começaram a desenvolver seus próprios padrões baseados em Ethernet e houve melhorias decorrentes do investimento em pesquisa do protocolo. Deste modo, surgiram protocolos como o *Modbus Transmission Control Protocol*, Modbus TCP, financiado pela Schneider Electric, o Ethernet /IP financiado pela Allen Bradley, o EtherCat que é financiado pela Beckhoff e o PROFINET, financiado pela Siemens [4].

Porém, a existência de vários protocolos competindo entre si, gera a fragmentação do mercado. Como consequência, apenas alguns têm oportunidade de destaque, enquanto que os demais permanecem como protocolos sob a propriedade de seus criadores. De acordo com [4], PROFINET é o protocolo de maior importância, visto que é incentivado pela Siemens. Considerando a sua posição de líder mundial em automação, espera-se que PROFINET adquira importância no mercado, assim como Profibus o fez.

A princípio, o objetivo deste trabalho é apresentar características do protocolo Ethernet, e também, desenvolver uma análise geral teórica e prática a cerca do protocolo PROFINET, a fim de evidenciar suas características e funcionalidades e, por fim, comparar este último com Profibus, através de estudo de caso.

## **1.1 Organização do trabalho**

A organização do trabalho procede da seguinte forma:

- Capítulo 2: Apresenta as características do protocolo Ethernet, expõe o modelo OSI e mostra as particularidades do protocolo TCP/IP a fim de fortalecer a base teórica do protocolo PROFINET.

- Capítulo 3: Como foco principal do trabalho, o protocolo PROFINET é abordado neste capítulo.
- Capítulo 4: Análise e estudos referentes ao estudo de caso.
- Capítulo 5: Apresenta algumas conclusões provenientes do trabalho.





## Capítulo 2

### Revisando conceitos

A princípio, este capítulo destina-se a apresentar conceitos que ajudarão a entender o protocolo PROFINET. O embasamento teórico dar-se-á no estudo do protocolo Ethernet e nas particularidades dos modelos OSI e TCP/IP. O nível de detalhamento apresentado é suficiente para a finalidade deste trabalho.

#### 2.1 O modelo OSI

O desenvolvimento de redes de computadores foi iniciado por redes experimentais como ARPANET E CYCLADES e, imediatamente, contou com o apoio de fabricantes de computadores. As redes experimentais eram criadas de forma heterogênea, uma vez que cada fabricante usava *softwares*, *hardwares* e tecnologias distintos [5] para desenvolver seus próprios equipamentos e referiam-se a eles como sendo suas “arquiteturas de rede”. Em 1977, a *International Organization for Standardization* (ISO) percebeu que havia necessidade de padronização das incipientes redes. [6]

A necessidade de interconectar sistemas de diferentes fabricantes rapidamente se tornou aparente, levando a ISO a criar um comitê para o estudo dos requisitos necessários para a criação do “Open System Interconnection”. A palavra “open” foi escolhida para enfatizar o fato de que se um sistema obedece a padrões internacionais, estará aberto a todos os demais sistemas que aceitarem aos mesmos padrões no mundo [6]. Em outras palavras, o padrão propicia que diferentes tecnologias sejam utilizadas em conjunto em ambiente heterogêneo. [5]

As primeiras discussões mostraram que arquitetura em camadas seria a mais viável para o “Open System Interconnection” com a capacidade de expandi-las se preciso. Este modelo seria a base para a criação de novos protocolos padronizados. A idéia básica de se dividir em camadas é que cada uma adiciona valor aos serviços provenientes do conjunto de camadas inferiores, de forma que as superiores oferecem um conjunto de serviços necessários para processar aplicações distribuídas, além de dividir um problema em várias partes menores.

Ao chamar uma camada de N, pode-se mencionar que a mesma agrega valor aos serviços da camada N-1 e entrega com valor agregado para a camada N+1. A cooperação entre as camadas são definidas pelos protocolos.

O modelo OSI está estruturado em sete camadas como pode ser visto pela Figura 1.

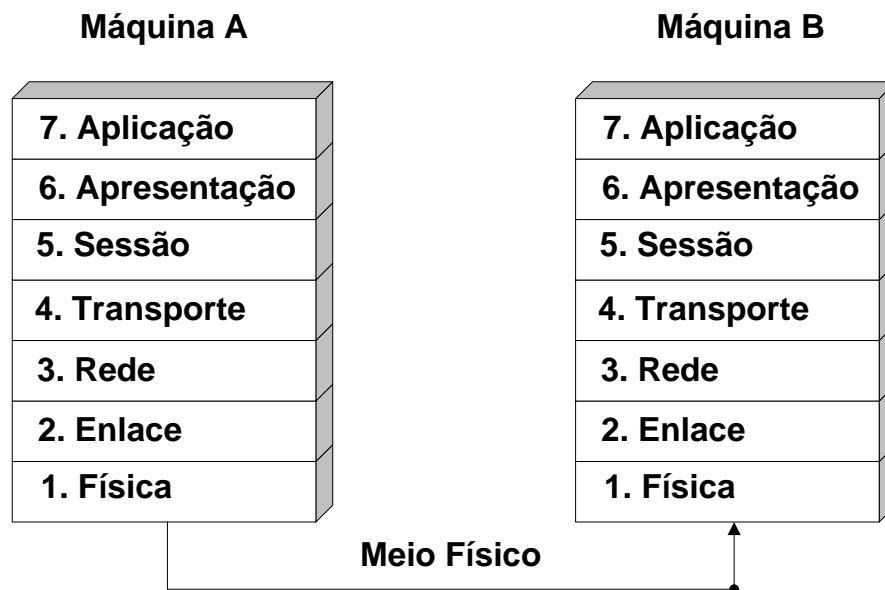


Figura 1: As camadas do modelo OSI. Fonte [1]

### 2.1.1 Camada física

De acordo com [5], a primeira camada do modelo OSI é responsável pela transmissão de bits de uma máquina para outra através do meio de transmissão. Por isso, lida com sinais elétricos que representam os estados 0 (desativado) ou 1 (ativado) de um bit que viaja pelo cabeamento da rede. Além de lidar com interfaces mecânicas, elétricas e funcionais do meio físico de comunicação. Por exemplo:

- Interfaces mecânicas: determinam a quantidade de pinos do conector.
- Interfaces elétricas: especificam valores de tensão que definem os bits 1 ou 0, além de estabelecerem a duração dos bits em segundos.
- Interfaces funcionais: explicitam a função dos pinos do conector da rede e determinam como a conexão é estabelecida e terminada.

Apresenta ainda as seguintes características:

- Topologias físicas: estrela, anel e barramento.
- Tipos de meios de transmissão: par trançado, cabo coaxial, fibra ótica.
- Sentido de transmissão: *simplex*, *half duplex* e *full duplex*,
- Métodos de codificação: Manchester, Manchester diferencial.

### 2.1.2 Camada de Enlace

É responsável por lidar com o tráfego de “frames”, ou seja, palavra de dados transmitida pela rede. Esta palavra é formada por um conjunto de *bytes*. A camada organiza as palavras de dados, transmitindo-as sequencialmente e processa os *frames* de confirmação mandados pelo receptor.

Ela assegura que os dados enviados pela rede sejam recebidos e se necessários os envia novamente, pois aqui é que são especificadas as técnicas de detecção de erros ocorridos no meio físico e, em alguns casos, corrigidos.

Há ainda o controle de fluxo que regula a conexão entre máquinas de diferentes velocidades de comunicação. E, por fim, especifica as formas de controlar o acesso ao meio de transmissão.

### 2.1.3 Camada de Rede

Esta permite a interconexão de redes heterogêneas (redes com endereçamento, tamanho de pacotes e protocolos diferentes). Ainda é função desta camada lidar com o congestionamento de dados e definir serviços de rede como:

- Serviços com conexão, endereços e rotas que são definidos durante o estabelecimento da conexão.
- Serviços sem conexão, o endereçamento e o roteamento que são definidos para cada pacote.

### **2.1.4 Camada de Transporte**

Caracteriza-se pela transmissão fim a fim, ou seja, desde a origem até o destino. Um programa na máquina de origem conversa com outro similar na máquina destino.

Esta camada assegura que os dados viajarão entre as máquinas sem que sejam perdidos, se estabelecerá conexão e, se necessário, organiza o reenvio das mensagens.

### **2.1.5 Camada de Sessão**

Permite que usuários em máquinas diferentes estabeleçam sessões entre si (por exemplo: login, transferência de dados). Estabelece, também, uma sessão entre aplicativos que estão sendo executados em máquinas diferentes, além disso, trata do sincronismo de comunicação e, por fim, determina pontos de sincronização para restabelecer conexões após uma eventual interrupção.

### **2.1.6 Camada de Apresentação**

Fornece serviços de vários aplicativos diferentes, utilizando recursos, tais como criptografia, compressão ou conversão de caracteres. Define o padrão de codificação de dados a ser utilizado, para que a mensagem codificada durante o envio possa ser decodificada no momento da recepção.

### **2.1.7 Camada de Aplicação**

É a camada que lida com as solicitações dos aplicativos que requerem comunicações de rede, como o acesso a um banco de dados ou o envio de um correio eletrônico.

## 2.2 TCP/IP

É o protocolo mais usado em redes locais. Uma das razões dessa popularização deve-se à arquitetura aberta que possibilita qualquer fabricante adotar sua própria versão do TCP/IP em seu sistema operacional, sem a necessidade de pagamento de direitos autorais. Com isso, houve proliferação do consumo pelos desenvolvedores de sistemas operacionais, universalizando o uso do protocolo TCP/IP. A arquitetura é composta por quatro camadas. A Figura 2 faz comparação entre o modelo OSI e o protocolo TCP/IP.

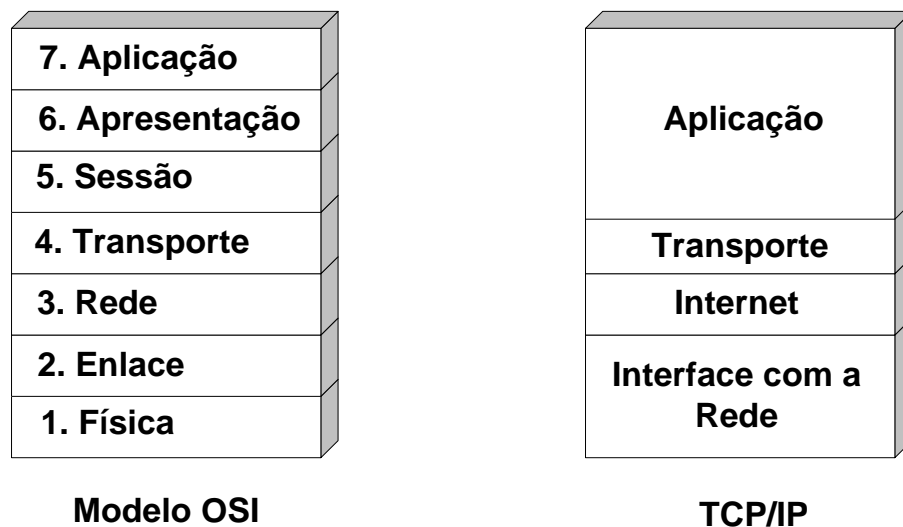


Figura 2: Arquitetura TCP/IP. Fonte [1]

### 2.2.1 Camada de aplicação

Equivalente às camadas 5, 6 e 7 do modelo OSI, tem por função fazer a comunicação entre os aplicativos e o protocolo de transporte. Existem vários protocolos que nela trabalham. Os mais conhecidos são HTTP (*Hypertext Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), o FTP (*File Transfer Protocol*), o SNMP (*Simple Network Management Protocol*), o DNS (*Domain Name System*) e o Telnet.

### 2.2.2 Camada de Transporte

Esta camada é a correspondente direta da camada de transporte do modelo OSI. Sua finalidade é colher os dados enviados pela camada de aplicação e transformá-los em pacotes, que serão repassados na Internet. Nesta camada operam dois protocolos: o TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*). O primeiro verifica se o dado chegou ao destino corretamente, já o segundo não possui esta função.

### 2.2.3 Camada de Internet

A camada de Internet do modelo TCP/IP é equivalente à camada de rede (camada três) do modelo OSI. Há vários protocolos que podem operar nesta camada: IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*), ARP (*Address Resolution Protocol*) e RARP (*Reverse Address Resolution Protocol*).

### 2.2.4 Camada de Interface com a Rede

Equivalente às camadas 1 e 2 do modelo OSI, tem por finalidade enviar o pacotes de informação recebidos pela camada Internet em formas de *frames* através da rede.

### 2.2.5 Endereçamento IP

O protocolo TCP/IP foi concebido com a finalidade de interligar diversas redes, pois desta forma haveria bastante caminhos entre transmissor e receptor. Por isso, ele utiliza o esquema de endereçamento lógico denominado endereçamento IP. Em uma rede TCP/IP, cada dispositivo conectado necessita usar pelo menos um endereço IP.

Este endereço possibilita identificar o dispositivo e a qual rede ele pertence. Isto é possível porque o endereço IP divide-se em duas partes conforme pode ser visto pela Figura 3.

<b>Identificação da Rede</b>	<b>Identificação da Máquina</b>
------------------------------	---------------------------------

Figura 3: Campos de um endereço IP. Fonte [2]

O endereço IP é constituído de um número de 32 bits, representado em decimal e em forma de quatro números de 8 bits separados por um ponto, no formato a.b.c.d., sendo que, o menor endereço IP possível é 0.0.0.0 e o maior 255.255.255.255.

Por isso, em teoria uma rede TCP/IP pode ter até 4.294.967.296 endereços IP ( $256^4$ ). Todavia, alguns endereços são reservados e não podem ser usados.

Cada dispositivo de uma rede TCP/IP precisa ter um endereço IP único, para que o pacote de dados possa ser entregue corretamente. Para facilitar a distribuição dos endereços IP, foram especificadas cinco classes, conforme mostra a Figura 4.

<b>Classe A</b>	<b>0</b>	<b>Identificação da rede (7 bits)</b>	<b>Identificação da máquina (24 bits)</b>
<b>Classe B</b>	<b>10</b>	<b>Identificação da rede (14 bits)</b>	<b>Identificação da máquina (16 bits)</b>
<b>Classe C</b>	<b>110</b>	<b>Identificação da rede (21 bits)</b>	<b>Identificação da máquina (8 bits)</b>
<b>Classe D</b>	<b>1110</b>	<b>Endereçamento multicast</b>	
<b>Classe E</b>	<b>1111</b>	<b>Reservado para uso futuro</b>	

Figura 4: Classes de endereços IP. Fonte [2]

Nota-se a presença de alguns bits fixos no início de cada classe de endereço IP, fazendo com que cada classe de endereços seja dividida conforme a Tabela 1.

Tabela 1: Divisão dos endereços IP em classes.

<b>Classe</b>	<b>Endereço mais baixo</b>	<b>Endereço mais alto</b>
A	1.0.0.0	126.0.0.0

B	128.1.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.254

### 2.2.6 Máscara de Rede

É formada por 32 bits no mesmo formato que o endereçamento IP e cada bit 1 informa a parte do endereço IP que é usada para o endereçamento da rede, além disso, cada bit 0 o faz para o endereçamento de máquinas. Desta forma, as máscaras de rede são:

Classe A: 255.0.0.0

Classe B: 255.255.0.0

Classe C: 255.255.255.0

O valor 255 equivale a um grupo de oito bits com todos seus bits em 1.

## 2.3 Ethernet

Durante duas décadas, os sistemas de comunicação a nível de chão de fábrica evoluíram e passaram da comunicação serial tradicional aos *fieldbuses*. Houve muitos esforços dos meios competentes para a criação de um único protocolo de campo, mas eles não obtiveram sucesso.

Por outro lado, Ethernet tem sido largamente utilizada em escritórios desde que apareceu. Por muitos anos, tem sido utilizada em plantas industriais conectando diferentes áreas, mas sua aplicação a níveis de chão de fábrica era proibitiva por uma soma de diversos fatores como carácter não determinístico, considerada inapropriada para ambientes agressivos, falta de imunidade a ruídos, conectores impróprios. [4] Na versão original, a operação era afetada pelas colisões que ocorriam sempre que havia envio simultâneo de duas ou mais estações para o mesmo endereço. A ocorrência de colisões tornava o protocolo não determinístico e desencorajava seu uso. [7]



Entretanto, recentemente, as redes Ethernet ganharam melhorias no seu desempenho. Duas novas versões permitem que se opere a uma taxa de 100Mbit/s (utilizada pelo PROFINET) ou 1Gbit/s. Uma versão de 10Gbit/s estará disponível em breve.

A melhoria mais significativa deve-se ao uso de “switches”. Estas são capazes de reconhecer os endereços das estações que nelas estão conectadas e redirecionar as mensagens somente para a estação de destino e não para todas as demais. A introdução da *switch* eliminou consideravelmente o número de colisões. No entanto, colisões ainda podem ocorrer se duas ou mais estações transmitem para o mesmo destino, conforme pode ser visto pela Figura 5 (a).

Para melhorar ainda mais o desempenho, faz-se o uso de *switches* com buffer, uma vez que o buffer estoca as mensagens e as envia para seus destinos ordenadamente. [7] Conforme pode ser visto na Figura 5 (b), há um redirecionamento correto das mensagens feito pela switch com buffer e nota-se a presença de colisões na switch sem buffer.

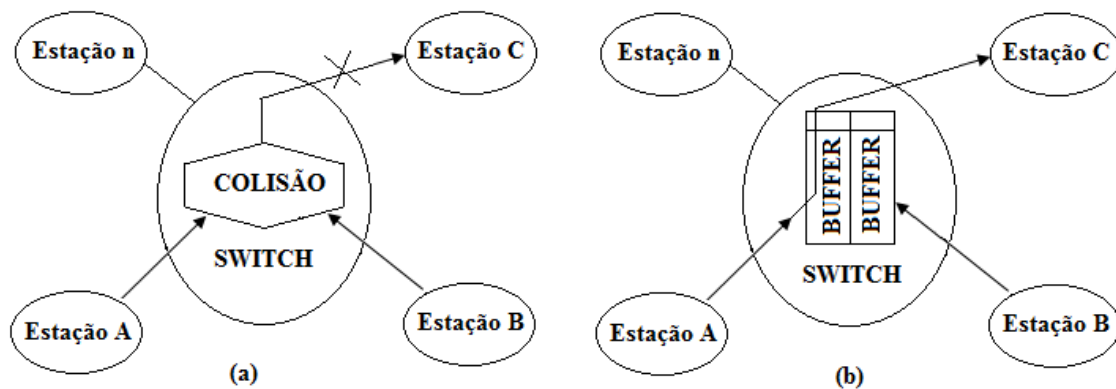


Figura 5: Switch (a) simples e (b) com buffer. Fonte [7]

Além do uso de hardwares especialmente projetados, há uma grande quantidade de softwares dedicados a cuidar do transporte de dados, gerenciamento da rede, endereçamento, redundância e segurança disponíveis no mercado, o que faz da Ethernet uma tecnologia madura e já dominada. [8]

Uma representação da arquitetura do padrão Ethernet é mostrada pela Figura 6, juntando a arquitetura do padrão Ethernet com o modelo OSI.

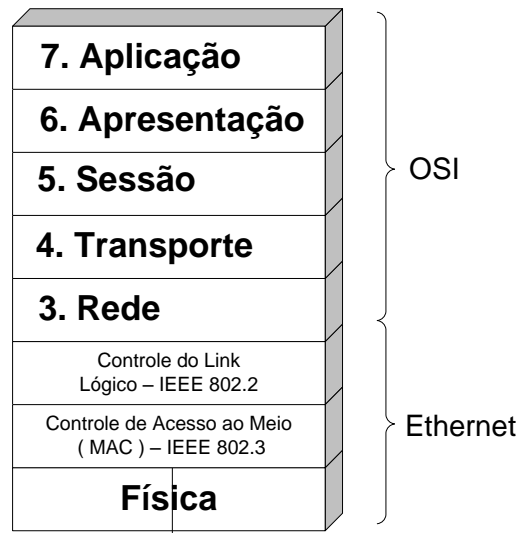


Figura 6: Modelo da arquitetura Ethernet. Fonte [2]

A seguir, há breve descrição das três camadas da arquitetura Ethernet.

### 2.3.1 A camada física

Para entender um pouco mais sobre a camada física, será abordado o padrão CSMA/CD, a codificação de dados e a placa de rede de acordo com [9].

#### 2.3.1.1 CSMA /CD

O compartilhamento do mesmo meio de transmissão de dados por todos dispositivos é fato característico de redes Ethernet. No entanto, quando um dispositivo está enviando uma mensagem, automaticamente exclui a comunicação dos demais aparelhos pertencentes à rede.

O primeiro passo para a transmissão de dados é verificar se o cabo está livre, ou seja, se não há a presença de portadoras. Isto é função da placa de rede, por isso o nome *Carrier Sense* (detecção de portadora). Caso a placa de rede não detecte a presença de portadora, ela inicia a transmissão de dados. Caso contrário, espera até que o cabo fique livre.

No entanto, o protocolo CSMA/CD não gera nenhuma prioridade entre as placas. Deste modo, pode ocorrer de duas ou mais placas perceberem a ausência de portadoras no cabo e transmitirem simultaneamente. Quando isso ocorre, há uma colisão e nenhuma das placas consegue transmitir dados.

Quando há uma colisão, todas as placas param de transmitir dados, esperam um tempo aleatoriamente e tentam a retransmissão. Como o tempo de espera das placas é aleatório, dificilmente ocorrerá outra transmissão.

O desempenho de redes Ethernet está fortemente relacionado com o número de dispositivos existente na mesma. Quanto maior o número de máquinas, maior a probabilidade de ocorrer colisões e o desempenho da rede diminui.

Quando um pacote de informações é enviado, todas as máquinas recebem este *frame* ao mesmo tempo, já que compartilham igual meio de transmissão. Todas as placas de rede possuem um endereço único chamado MAC, com isso, mesmo que todas as placas recebam o telegrama de informações, somente a placa que possuir o endereço de destino do *frame* receberá a mensagem.

### 2.3.1.2 Transmissão de dados.

Um sinal digital consiste em uma sequência de pulsos retangulares de mesma largura. A temporização desses pulsos é controlada por um *clock* e a informação a ser transmitida é uma sequência de valores altos e baixos desses pulsos.

A princípio em Ethernet, o bit 0 e o bit 1, a serem transmitidos, não são substituídos por valores de tensão, 0V e 5V respectivamente. Há uma modulação que varia conforme a taxa de transmissão utilizada.

- Para taxas de 10 Mbps (Ethernet padrão: 10 Base-T), é utilizada a codificação Manchester.
- Para taxas de 100 Mbps (Fast Ethernet: 100 Base-TX), são utilizadas as codificações MLT-3 e a 4B/5B.
- Para taxas de 1 Gbps (Gigabyte Ethernet), usa-se codificação 4d-PAM5.

A Figura 7 possibilita visualizar como se dá codificação Manchester e a MLT-3 usadas para Ethernet a 10Mbps e a 100Mbps. Além disso, é possível compará-las à codificação NRZ aplicada no protocolo Profibus.[23] A explicação de cada codificação será feita nos tópicos 2.3.1.3, 2.3.1.4 e 2.3.1.5 respectivamente. É oportuno citar que a Figura 7 tem caráter puramente explicativo, ela representa sistemas variantes no tempo, as formas de onda dependem dos bits que são transmitidos e assim, assumem formas diferentes do que é representado.

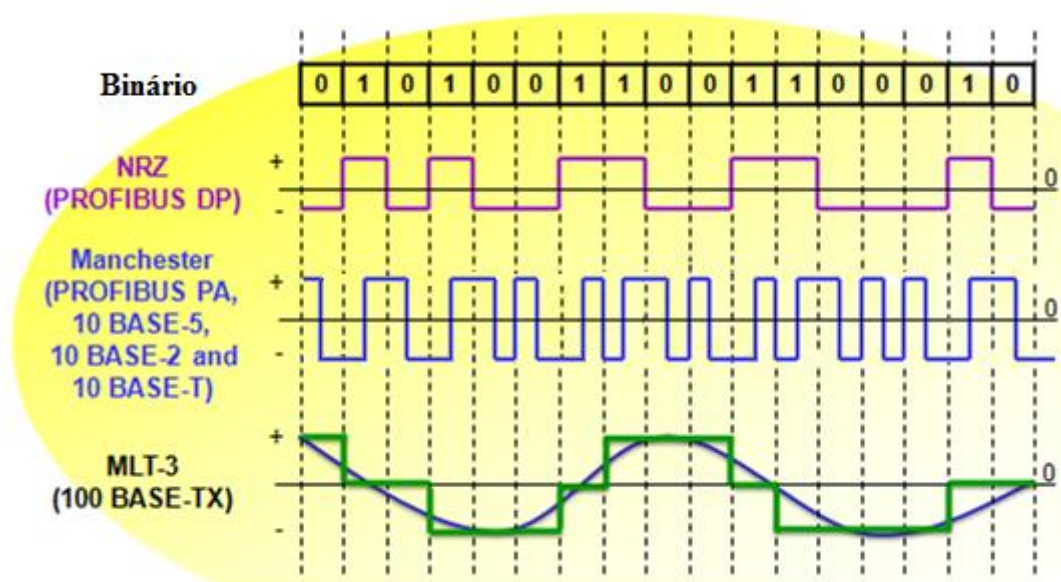


Figura 7: Codificação do sinal em Ethernet e no protocolo Profibus. Fonte [23]

### 2.3.1.3 Codificação NRZ

É a mais simples representação digital do sinal, utiliza somente dois níveis de tensão para codificar o sinal. O nível lógico alto é representado por 1 e o nível lógico baixo é representado por 0. Esta codificação chamada NRZ (*Non-Return to Zero*) é utilizada no protocolo Profibus DP. Todavia, este modelo de codificação traz consigo defeitos como a dificuldade em se distinguir entre uma sequência de zeros e a ausência de sinal. O protocolo Profibus resolveu este problema elevando o nível de tensão apresentado pela rede quando ela não está transmitindo dados para aproximadamente 1,5V e não, mas 0V. Assim, pode-se distinguir facilmente entre um período ocioso da rede ou a ruptura do cabo, por exemplo. [23]

### 2.3.1.4 Codificação Manchester

Este método de codificação é utilizada em redes Ethernet a 10Mbps. A codificação Manchester já não apresenta os defeitos da codificação NRZ. No entanto, este modelo de codificação não é indicado para frequências acima de 10Mbps. A aquisição do sinal é feito a cada ciclo de *clock* e determinada pela borda de subida, nível lógico alto representado por 1, ou de descida do pulso, nível lógico baixo representado por 0. Conforme representado pela Figura 8. [23]



Figura 8: Nível lógico alto e baixo da codificação Manchester. Fonte [23]

### 2.3.1.5 Codificação MLT-3

A codificação MLT (*Multi Level Threshold*) é usada em Ethernet 100Base TX (Fast Ethernet). Ela utiliza três níveis determinados por -1, 0 e 1. Se o sinal move para o próximo estado o bit 1 é transmitido, se o sinal permanece no mesmo estado o bit 0 é transmitido. O que leva a Ethernet a transmitir uma alta taxa de bits (100Mbit/s) em um sinal de frequência bem menor. Isto leva a redução das características elétricas e mecânicas do meio de transmissão, por consequente uma redução de custo do cabeamento. A modulação MLT é apontada como uma das vantagens da Ethernet.

Um ciclo completo leva quatro ciclos de *clock*, o que limita a frequência máxima de transmissão do sinal a um quarto da *baudrate*. Isto torna essa codificação apropriada para cabos de cobre, visto que, conforme a taxa de comunicação aumenta, os problemas da rede são amplificados, como por exemplo, interferências no sinal causadas por reflexão de onda acentuam-se.

Porém, esta codificação ainda não é a mais confiável. Se muitos bits 0 forem transmitidos, o sinal do cabo não muda e pode levar a problemas de decodificação.

Para solucionar isso, Ethernet 100Base-TX usa a codificação 4B/5B para assegurar que há bits 1 o suficiente para não causar problemas conforme descrito. [23]

### 2.3.1.6 Codificação 4B/5B

Este sistema de codificação separa os dados a serem transmitidos em grupos de 4 bits e cada bloco desses é então transformado em blocos de 5 bits de dados. O processo de transformação de grupos de 4 bits em grupos de 5 bits não será explicado, todavia a Tabela 2 mostra a relação já pronta.

**Tabela 2: Codificação de grupos de 4 bits para grupos de 5 bits.**

Valor (hexadecimal)	Valor binário (4B)	Valor transmitido (5B)
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01001
6	0110	01110
7	0111	01111
8	1000	10010
9	1001	10011
A	1010	10110
B	1011	11011
C	1100	11010
D	1101	11011
E	1110	11100
F	1111	11101

Esta codificação foi elaborada com o objetivo de evitar a presença de três zeros consecutivos em um mesmo bloco de dados, o que aumenta a força do efeito diferencial do sinal através do cabo de par trançado. Em outras palavras, este é um sistema muito elaborado contra ruídos.

Com quatro bits, pode-se representar 16 números ( $2^4$ ). Adicionando esse quinto bit, a quantidade de números possíveis passa a ser 32 ( $2^5$ ). Com isso, cada bloco de

dados pode transmitir 16 números de dados (os 4 bits do quadro original) e mais 16 dados de controle. Na realidade, apesar de existirem 16 dados para serem usados como controle, apenas quatro são usados. Esses dados são os seguintes: [9]

- Idle (ocioso): esse dado é enviado sempre que não há dados a serem enviados na rede. É importante citar que as placas de rede ignoram esses dados sempre que verificam a presença de portadora.
- Delimitador de início do *frame*: indica o início de um telegrama.
- Delimitador de fim do *frame*: indica o término do telegrama.
- Erro de transmissão: indica que houve erro na transmissão.

Fazendo breve comparação com o protocolo Profibus, o dado é transmitido por um conjunto de 8 bits (1 byte) e há a presença de 3 bits adicionais de controle: o bit delimitador de início de *frame*, o bit de fim do *frame* e o bit de paridade. Na configuração apresentada pela codificação 4B/5B utilizada na Fast Ethernet, há um controle mais rígido na transmissão de dados se comparado ao protocolo Profibus.

### 2.3.1.3 Placa de Rede

A principal função da placa de rede é receber os *frames* enviados pela MAC (Camada de Controle de Acesso ao Meio) e transmiti-los pelo cabeamento da rede. Com isso, a placa de rede não só é responsável pela codificação, mas também pelo uso do protocolo CSMA/CD.

Atualmente, encontram-se placas de rede com conectores RJ 45, BNC, AUI e conectores para o uso de fibra ótica (ST, MIC, VF-45).

### 2.3.1.4 Cabeamento

Com foco na Fast Ethernet que opera a 100Mbps, será exposto somente os cabeamentos referentes a esta taxa de comunicação. Todavia, é importante ressaltar que o tipo de cabeamento varia conforme a taxa de transmissão de dados adotada, havendo vários tipos diferentes de cabeamento para Ethernet 10 Mbits e Ethernet 1Gbit.

Em relação à Ethernet com taxa de comunicação de 100 Mbit/s, pode-se usar dois meios distintos de cabos:

- 100BaseT: par trançado sem blindagem com comprimento máximo de 100 metros por segmento.
- 100BaseFX: fibra ótica de modo múltiplo, possui limite de 412 metros por segmento, caso seja usada apenas uma fibra e comunicação full duplex. Se forem utilizadas duas fibras, a comunicação útil é a full duplex e o limite de comprimento passa a ser 2 km por segmento. Pode-se ainda utilizar fibras ópticas de modo único no padrão 100 Base FX, nesse caso o limite sobre para mais de 20 km.

### 2.3.2 A camada MAC

O papel desta camada é gerar os frames Ethernet. Para isto, pega os dados transmitidos pela camada imediatamente superior a ela (Controle do Link Lógico, LLC) e lhes acrescentam os cabeçalhos. No frame são inseridas as informações de qual placa de rede está enviando o quadro e para qual placa de rede o quadro será enviado. Quando o frame está pronto, esta camada envia para a camada Física, que é responsável pela sua transmissão através do cabeamento.

#### 2.3.2.1 Endereçamento MAC

Todas as placas de rede recebem um endereço único denominado MAC. Este endereço é físico, gravado na memória interna da placa. Não há duas placas de rede com o mesmo endereço MAC no mundo. Por isso, quando um *frame* é enviado para uma máquina, somente ela captura-o, uma vez que esta, exclusivamente, terá o MAC discriminado no campo Endereço MAC de destino do quadro Ethernet.

Conforme pode ser visto pela Figura 9, o endereço MAC consiste em seis bytes. Os três primeiros bytes são chamados OUI (*Organizationally Unique Identifier*) e identificam o fabricante da placa de rede. Estes são padronizados pelo IEEE. Para um fabricante conseguir um número OUI, precisa cadastrar-se no IEEE.

Os três últimos números são bytes definidos e controlados pelo fabricante.



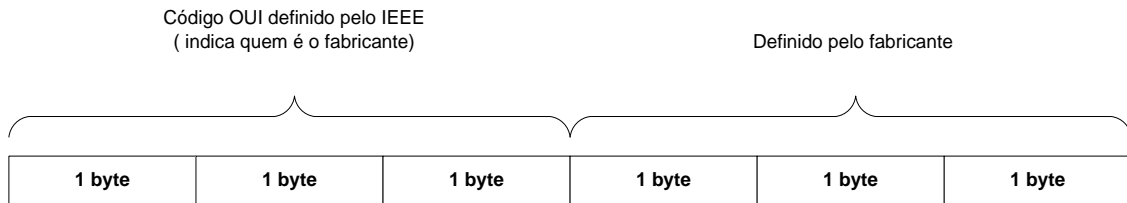


Figura 9: Estrutura do endereço MAC. Fonte [2]

### 2.3.2.2 Quadro Ethernet

A estrutura do quadro Ethernet pode ser vista pela Figura 10. Este possui um cabeçalho de 22 bytes, uma área de dados que varia entre 46 a 1500 bytes e um final de 4 bytes.

<b>Preâmbulo ( 7bytes )</b>	<b>SFD ( 1byte )</b>	<b>MAC Destino ( 6 bytes )</b>	<b>MAC origem ( 6bytes )</b>	<b>Comprimento (2 bytes )</b>	<b>Dados do PAD ( de 46 a 1500 bytes )</b>	<b>FCS ( 4 Bytes)</b>
---------------------------------	--------------------------	--	--------------------------------------	-----------------------------------	--	---------------------------

Figura 10: Estrutura do frame Ethernet. Fonte [2]

Resumidamente, os campos existentes no frame são:

- Preâmbulo: marca o início do frame;
- SFD (*Start Frame Delimiter*): é um byte 10101011;
- Endereço MAC de destino;
- Endereço MAC de origem;
- Comprimento: indica quantos bytes estão sendo transferidos no campo de dados;
- Dados: possui comprimento mínimo de 46 bytes e máximo de 1500 bytes;
- Pad: se a camada LLC enviar menos do que 46 bytes de dados, são inseridos os chamados Pad para que o campo de dados atinja o seu tamanho mínimo de 46bytes;

- FCS (*Frame Check Sequence*): responsável pelo controle de correção de erros.

O tamanho mínimo de um frame Ethernet é de 72 bytes e o máximo de 1526 bytes.

### 2.3.3 A camada LLC

A maneira mais simples de se explicar o funcionamento desta camada é através de um exemplo. Análises profundas não convêm neste momento.

Tendo uma rede baseada no protocolo TCP/IP, sabe-se que este protocolo é de alto nível e somente é encontrado nas máquinas da rede. Na parte física da rede, os dados circulam através de *frames* Ethernet. Quando a máquina receptora recebe um *frame*, ela precisa saber para qual protocolo de alto nível deverá entregar os dados. Se essa informação não estivesse escrita em algum lugar do quadro de dados, a máquina receptora não saberia o que fazer com esse pacote de informação.

A implementação da camada de Controle do Link Lógico (LLC) adiciona um cabeçalho de apenas três bytes aos dados recebidos do protocolo de alto nível: DSAP (*Destination Service Access Point*) indica o protocolo de destino e SSAP (*Source Service Access Point*) indica o protocolo de origem e Controle.

Todavia, essa implementação mostrou-se ineficiente para identificar corretamente os protocolos de origem e destino, pois havia poucos bytes para isso. A solução para este problema foi a criação de um campo chamado SNAP (*Sub Network Access Protocol*), de cinco bytes. Três destes bytes são usados para identificar o fabricante do protocolo e os outros dois são definidos pelo fabricante internamente de maneira análoga ao MAC.

A Figura 11 apresenta um frame Ethernet. A camada de Controle do Link Lógico acrescenta dois cabeçalhos (LLC e SNAP), e o campo de dados contém os dados passados pelo protocolo de alto nível.

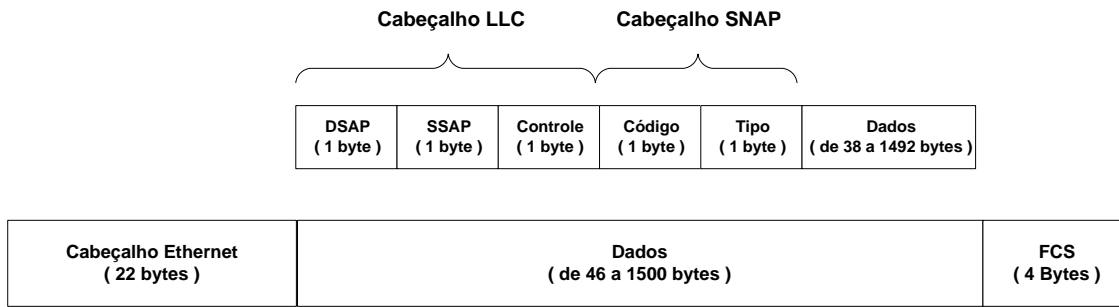


Figura 11: Estrutura do quadro Ethernet com a camada de Controle do Link Lógico (LLC). Fonte [2]

Os campos existentes no cabeçalho acrescentado pela camada de Controle de Link Lógico são:

- DSAP (*Destination Service Access Point*): indica o endereço SAP de destino;
- SSAP (*Source Service Access Point*): indica o endereço SAP de origem;
- Controle: também denominado CTL, pode assumir basicamente três valores:
  - ✓ UI (*Unnumbered Information*) quando se está transmitindo dados;
  - ✓ XID (*Exchange Identification*): usado para trocar dados de identificação entre o transmissor e o receptor;
- Código: é o código do fabricante do protocolo no IEEE;
- Tipo: é o código dado pelo fabricante ao protocolo.



## Capítulo 3

### O protocolo PROFINET

Este capítulo destina-se a introduzir os conceitos do protocolo de comunicação industrial PROFINET. O capítulo está dividido em tópicos a fim de facilitar a leitura e entendimento das particularidades do padrão abordado.

Além disso, de forma a aumentar ainda mais a compreensão, sempre que possível, serão feitas analogias e comparações ao protocolo Profibus, visto que, este apresenta grande aceitação do mercado e ambos são apoiados pela mesma entidade.

#### 3.1 Introdução

A possibilidade de padronização das redes de campo em um só protocolo aliado ao desejo de usar uma só rede do chão de fábrica até os escritórios, somado a características como diagnóstico estendido tem incentivado a adoção de Ethernet na indústria nos últimos anos. Acompanhando a tendência, a Siemens e posteriormente a PNO começaram a desenvolver seu próprio padrão baseado em Ethernet. Do resultado desse esforço, originou-se o protocolo PROFINET (***P**owerful **R**ead Time **O**pen **F**lexible **I**ntegrated **N**et **C**onvergence **E**nterprise Wide **T**ransparent*). Em 2002, a PNO fundou o primeiro Centro de Competência PROFINET, cinco anos após, em 2007, havia já 1 milhão de dispositivos instalados. De acordo com Figura 12 nota-se que a curva de crescimento de dispositivos instalados do padrão PROFINET é maior se comparado com a do Profibus no mesmo período de tempo. [10]

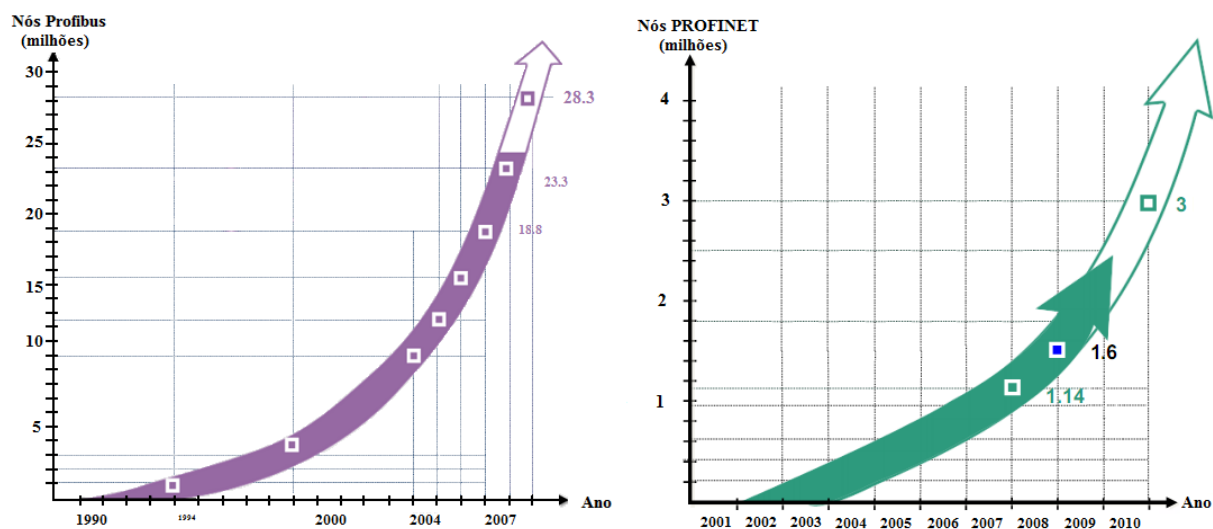


Figura 12: Curvas de crescimento de nós instalados Profibus e PROFINET. Fonte [10]

Adicionalmente à Figura 12, de acordo com a edição 2011 do *The World Market for Industrial Ethernet* do *IMS Research*, poucos anos após o surgimento do padrão PROFINET já foram o suficiente para deter 28% do mercado de protocolos baseados em Ethernet. A tendência é que em um futuro próximo, ele ocupe o primeiro lugar.

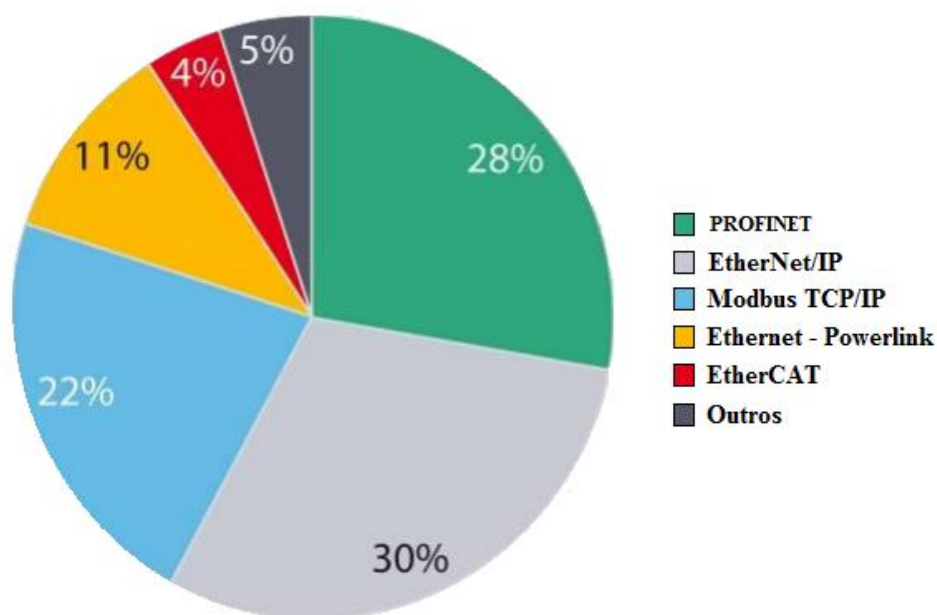


Figura 13: Divisão do mercado dos protocolos baseados em Ethernet.

O padrão PROFINET contém todas as funções de Ethernet por isso, pode ser integrada no escritório sem adição de interfaces. Além disso, foram inseridas algumas funções a mais para atender necessidades da indústria, por exemplo, uma comunicação TCP/IP pode ser estabelecida em paralelo à troca de dados habitual. [10]

Não obstante do acréscimo de recursos de comunicação, um dos pontos fortes do protocolo é a integração com outros padrões. O modelo da estação em PROFINET foi baseado no modelo do dispositivo Profibus, de modo que os módulos I/O de dispositivos periféricos existentes na planta são empregáveis aos dois protocolos. Esta medida preserva os investimentos já feitos, o que facilita a empregabilidade do protocolo e por consequente uma ascendente difusão do mesmo.

Sistemas existentes podem facilmente ser migrados para o novo ambiente PROFINET sem a necessidade de escrever novos programas ou mudar as estações Profibus. Ademais, a adoção de *proxys*<sup>1</sup> também é uma medida a ser considerada se for necessária a integração de outros protocolos. [10]

Somando-se à fácil integração com outros protocolos, a flexibilidade de topologias de rede é outra vantagem da Ethernet Industrial. Sejam elas em árvore ou em anel, óticas, elétricas ou wireless o projetista facilmente atende aos requisitos do projeto. [10]

Quanto ao tempo, as altas taxas de transmissão (100 Mbits/s) fazem do padrão baseado em Ethernet absolutamente ideal para comunicação em campo. Os tempos de resposta rápidos e a transmissão determinística dos dados são pontos muito importantes.

Para comunicação em tempo real, PROFINET adicionalmente oferece um canal em tempo real paralelo para comunicação via TCP/IP. Este método usa o *hardware* padrão Ethernet nos equipamentos e possibilita a priorização dos telegramas nas *switches*. Isto possibilita um tempo de resposta na faixa de 5 a 10 ms, comparável à resposta dos protocolos de campo existentes.

Aplicações sincronizadas demandam uma precisão no *jitter*<sup>2</sup> de menos de 1  $\mu$ s e tempo de ciclo na faixa de 1 ms para garantir o determinismo. Para ser capaz de operar nesse tipo de aplicação, a comunicação Ethernet no PROFINET foi estendida

---

<sup>1</sup> Proxy: vide subtópico 3.2.1.1.

<sup>2</sup> Jitter: vide tópico 4.4

para uma comunicação isócrona. Contudo, essa mudança trouxe a necessidade de *hardware* especial integrado na rede e no equipamento, como por exemplo, o ERTEC (*Enhanced Real Time Ethernet Controller*) e *ASICs*. Os telegramas em tempo real são transferidos em um espaço de tempo reservado, obedecendo a uma sequência cíclica. O tempo restante é usado para comunicação padrão. [10]

O uso de Ethernet, porém, trouxe um grande risco de acesso acidental ou não autorizado aos dispositivos de automação, o que pode trazer consequências fatais. Todavia, vários fabricantes já desenvolveram componentes que garantem proteção confiável a acessos não autorizados, endereçamento errado e outras falhas. Este assunto será abordado no tópico 3.7

## 3.2 As versões do PROFINET

O padrão PROFINET divide-se em duas funções. Elas diferem, principalmente, no tipo de troca de dados para atender altas demandas de velocidade. Para este protocolo, existem duas versões PROFINET IO e PROFINET CBA. Ambas podem ser usadas separadamente ou em conjunto. [11]

### 3.2.1 PROFINET IO

Esta versão do padrão PROFINET conecta o sistema aos dispositivos de entradas e saídas distribuídos no campo. Ademais, os dispositivos I/O distribuídos no campo podem ser diretamente conectados à Ethernet. PROFINET IO descreve toda troca de dados, configuração e parametrização entre *IO Controllers* e *IO Devices*. [11]

Em geral, PROFINET IO distingue os dispositivos em três categorias. [12]

- **IO Controller:** representa principalmente o CLP, faz o papel do mestre no Profibus. Possui algumas tarefas como endereçamento, configuração, parametrização de todos os IO Devices conectados.
- **IO Device:** em sua maioria são dispositivos de campo ou remotas. Fazendo uma analogia, representam os escravos do padrão Profibus. É a Fonte de dados de



entrada do processo e destino dos dados de saída. Ademais, provem diagnósticos e alarmes. Podem ser controlados por um ou mais IO Controllers.

- **IO- Supervisor:** são ferramentas de engenharia para parametrização e diagnóstico de IO Devices. Analogamente ao Profibus, faz o papel do mestre classe 2.

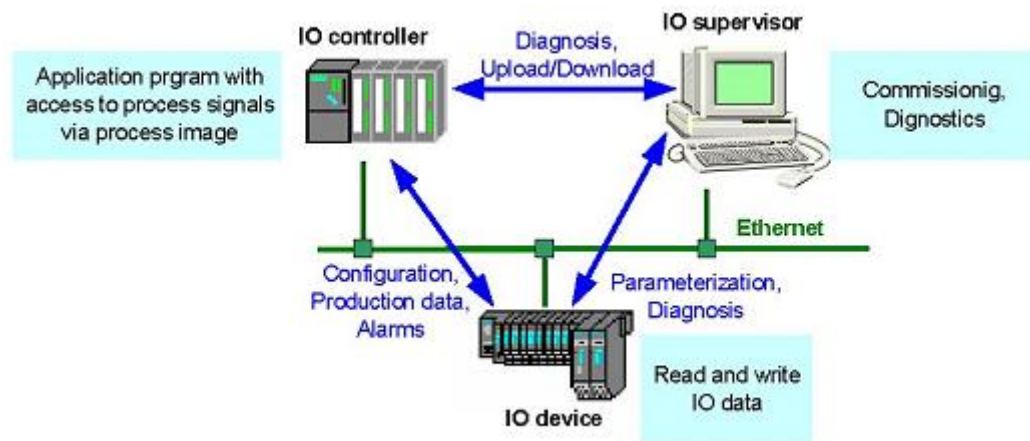


Figura 14: Modelo de comunicação em PROFINET. Fonte: [4]

Desde que todos os dispositivos operam com os mesmos direitos na rede, o sistema mestre escravo do padrão Profibus tornou-se o modelo *Provider-Consumer* nesta versão do PROFINET. O *Provider* é o transmissor que envia um dado sem o pedido de seus parceiros, já o *Consumer*, é aquele que processa o dado [11]. Não existe mais hierarquia. Somente a configuração atribui um dispositivo de campo a um controle central. [13]

Fazendo-se uma breve comparação, o protocolo Profibus na versão DP-V0 e DP-V1 utiliza o modelo mestre escravo, onde o escravo não possui autonomia de serviços de rede. O mestre, por sua vez, detém o controle da comunicação. Já na versão DP-V2 o Profibus apresenta um modelo que se assemelha muito ao *Provider-Consumer* denominado Publisher-Subscriber. Neste, o escravo possui mais liberdade na rede, como por exemplo, trocar dados com outros escravos.

### 3.2.1.1 Integração

O PROFINET IO permite a integração de subsistemas em uma única rede através do *Proxy*. Dispositivos de campo podem ser integrados ao sistema PROFINET IO. Analogamente a alguns acopladores (*couplers*) que são mestres para rede Profibus PA e escravos para rede PROFIBUS DP<sup>3</sup>, o *proxy* é IO Device para rede PROFINET IO e IO Controller para os dispositivos de campo de outros protocolos. Isto permite uma rápida integração dos sistemas já existentes à rede PROFINET. O *proxy*, por sua vez, não necessita de dupla configuração e duplo endereçamento. A troca de dados, diagnósticos e parametrização são transmitidas via rede conforme os *couplers* fazem. A Figura 15 ilustra a integração das redes. [11]

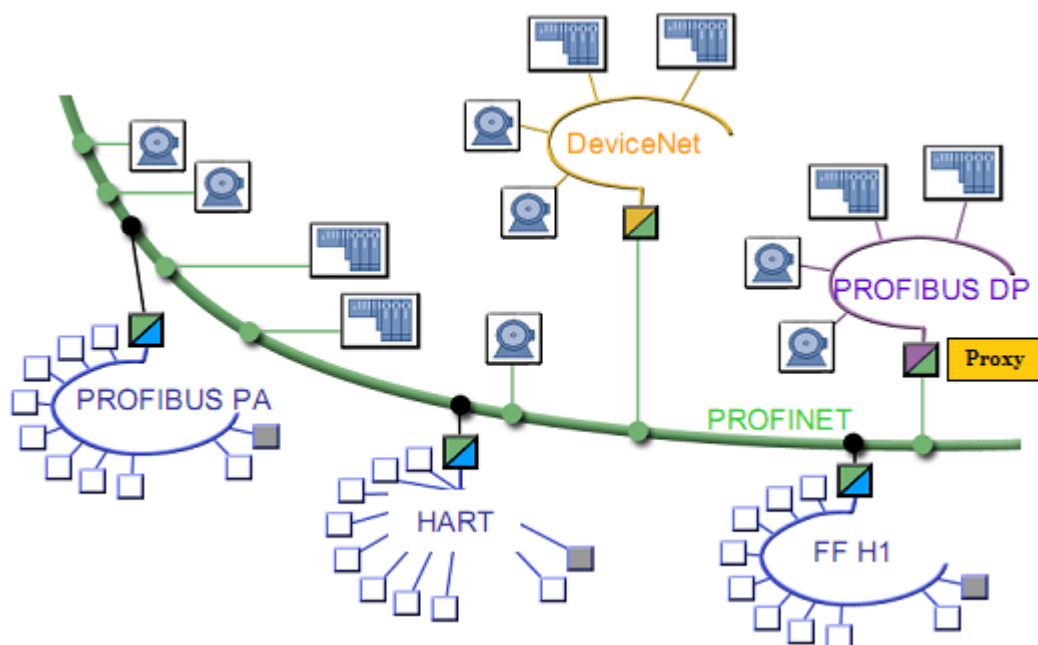


Figura 15: Integração via *proxy* com PROFINET IO. Fonte [14]

### 3.2.1.2 O modelo de comunicação

PROFINET IO possibilita um flexível e ao mesmo tempo sofisticado modelo de comunicação. Todas as demandas das mais modernas aplicações de automação

<sup>3</sup> Nem todos couplers exercem a função de mestre para o segmento PA e escravo para o segmento DP.

podem ser encontradas nessa versão do protocolo. Ao mesmo tempo, este modelo é tão flexível que dispositivos podem apenas usar a parte do padrão que for necessária para atender as especificações da aplicação. [11]

Para possibilitar tráfego de protocolos de tempo real e TCP/IP, a troca de dados cíclica do PROFINET IO se distingue em *Non- Real Time* e em dois modos de operação: PROFINET IO-RT e PROFINET IO IRT, não em relação a desempenho, mas em relação ao determinismo. IRT significa *Isochronous Real Time* e RT, *Real time*. Observa-se que ambos os modos podem operar em conjunto na mesma rede.

Cada protocolo tem um tempo alvo específico: *Non-RT* pode ser usado onde tempo de ciclos são maiores que 100ms e apresentam um *jitter* de mais de 100%, RT Classe 1 tem um tempo de ciclo de poucos milissegundos (da ordem de 10ms) e pouco *jitter* (da ordem de 15%) e por fim, RT Class 2 ou IRT tem um tempo de ciclo de da ordem de 250 $\mu$ s e virtualmente não possui *jitter*. [15]. Através de um método especial, IRT permite um alto sincronismo na rede, o que lhe confere alto determinismo em tarefas de posicionamento, conforme Figura 16.

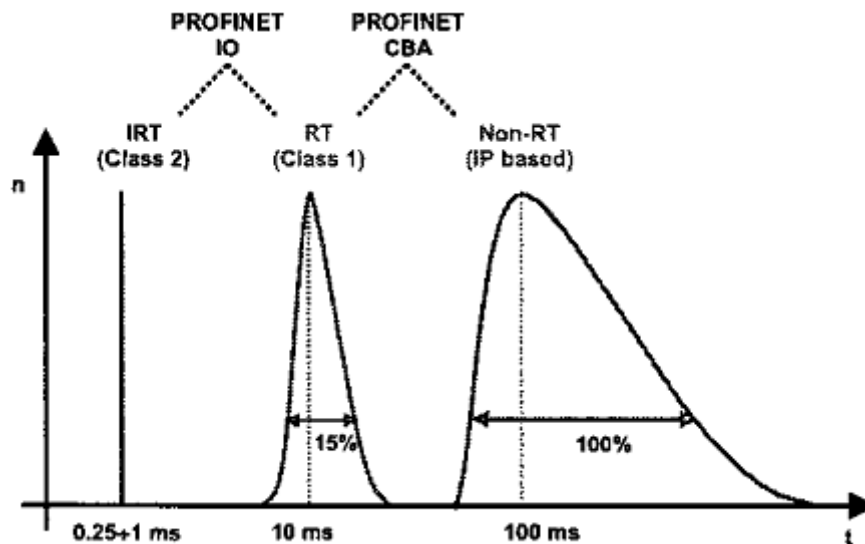


Figura 16: Tempo de ciclo e jitter para cada classe de comunicação. Fonte [15]

Ilustrando de outra maneira, as quatro classes descritas podem ser representadas conforme seu grau de determinismo de acordo com a Figura 17.

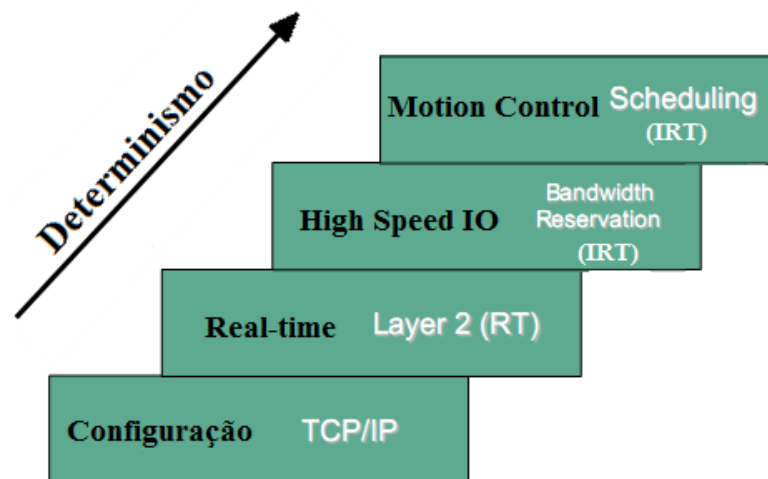


Figura 17: Os quatro graus de determinismo. Fonte [23]

Além da troca cíclica de dados, o modelo de comunicação também permite uma poderosa comunicação acíclica que excede todas as especificações dos fieldbuses. A área de endereço disponível e o tamanho do parâmetro são apenas limitados pelas áreas de memória nos *IO Devices* e *IO Controllers*.

Em adição a comunicação cíclica e acíclica cada dispositivo também suporta a comunicação TCP/IP. *Web Server* ou outra tecnologia baseada em IP pode ser usada. Em dispositivos que não suportam o padrão PROFINET (como câmeras, impressoras, computadores) podem também ser operados na rede.

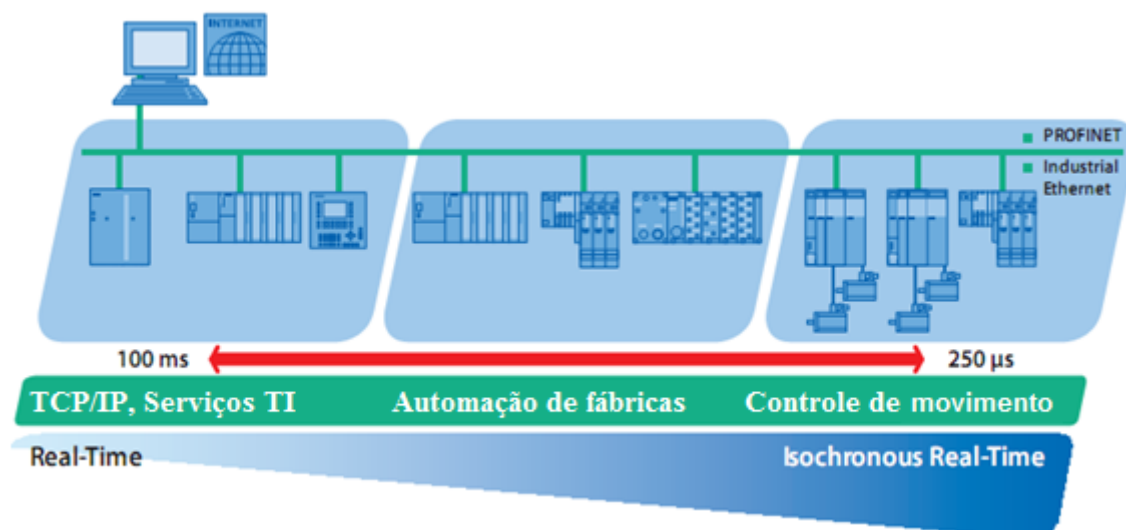


Figura 18: Canais de comunicação em PROFINET. Fonte [11]

A combinação desses serviços de comunicação torna possível a implementação de sofisticados sistemas que possam gerenciar todas essas informações de forma a obter apurados sistemas de diagnósticos, realizar manutenção preventivamente, dentre outros.

### 3.2.1.3 Identificação

Cada dispositivo de campo PROFINET IO é caracterizado por um número de identificação (*Device ID* – o mesmo ocorre no padrão Profibus). O *IO Controller* transmite o *Device ID* durante a fase de *start up*. Neste momento, ocorre uma checagem do ID transmitido pelo *IO Controller* e do ID que já estava gravado no *firmware* do dispositivo. Este procedimento ocorre da mesma maneira durante a fase de parametrização do escravo Profibus.

O número de identificação é único no mundo inteiro, é atribuído pela PNO. Existem dois tipos de números de identificação:

- ID do fabricante: é uma referência do fabricante na PNO e é atribuído uma única vez.
- ID do dispositivo: É usado para diferenciar *IO-Devices*.

### 3.2.1.4 Arquivo GSD

Fazer com que vários dispositivos diferentes trabalhem em conjunto em uma mesma rede não é tarefa fácil. Para isso, muita informação deve ser fornecida ao *IO Controller* para que a parametrização e a configuração dos *IO Devices* seja feita corretamente.

Analogamente ao Profibus, cada dispositivo do padrão PROFINET tem seu próprio *General Device Description* (GSD). Este arquivo contém todos os dados importantes para a engenharia e também para troca de dados com o *IO-Device*. Foi é padronizado pela ISO 15745.

A linguagem usada para fazer o arquivo GSD é GSDML (*GSD Markup Language*) – uma linguagem baseada em XML. Cada fabricante deve fornecer o

arquivo GSD de seu *IO-Device* aos clientes gratuitamente através de seu *web site* ou mesmo pelo da Associação Profibus.

O nome do GSD é padronizado da seguinte maneira.

GSD-[Versão do GSD]-[Nome do fabricante]-[Tipo de dispositivo]-[Data].xml

Por exemplo, o arquivo GSDML-V2.25-Siemens-Sinamics\_S\_CU3x0-20101103.xml indica que a fabricante é a Siemens, trata-se de um inversor de frequência Sinamics, fabricado no dia 03/11/2010 e a versão do arquivo é 2.25.

### 3.2.1.5 Endereçamento do dispositivo no campo

Para conectar todos os componentes da rede Ethernet, os dispositivos PROFINET possuem um endereço MAC. Este endereço é usado para identificar os dispositivos sem margem para erros, visto que cada endereço MAC é único no mundo inteiro.

Além do MAC, a comunicação em PROFINET requer que cada dispositivo tenha um nome único no projeto, de modo que todos os dispositivos na rede podem ser identificados por esse nome. Este nome é escrito no *IO-Device*. É prática comum atribuir um nome referente à aplicação e a área que o dispositivo se encontra [11], por exemplo: [16]:

- IO Device: “io”
- Drive: “drv”
- Switch: “swi”
- IO Panel: “ihm”

Complementando a atribuição dos nomes, é útil descrever a posição que o dispositivo se encontra na rede, por exemplo:

O segundo *IO Device* da planta de automação 1: “io-1-2”.

### 3.2.1.6 Parametrização

Depois da identificação do *IO-Device* na fase de *start up*, o *IO-Controller* transmite os parâmetros do projeto, assim como a configuração determinada pelo usuário para o *IO Device*. A troca cíclica de dados somente pode começar depois de o *IO Device* ter recebido essas informações e checado se elas são consistentes. Em seguida, o *IO Device* retorna um telegrama confirmando o sucesso da operação. Inicia-se posteriormente a troca de dados.

Também é parte da parametrização a atribuição dos parâmetros IP. Neles incluem-se o endereço IP, a submáscara e o endereço do *gateway*. Cada *IO Device* tem um único IP e é usado para endereçá-lo, por exemplo, quando se usa serviços de TI como *HTTP*, desde que ele suporte essas funções.

Segundo [16], é boa prática atribuir diferentes endereços IP para os componentes da rede. Por exemplo:

- *IO-Controller*: de 192.168.2.1 até 192.168.2.19
- *Switches*: de 192.168.2.20 até 192.168.2.49

#### *PROFINET IO Devices*

- *I/O*: de 192.168.2.50 até 192.168.2.99
- *Drives*: 192.168.2.100 até 192.168.2.149
- Painéis *I/O*: 192.168.2.150 até 192.168.199
- Funções adicionais/reservado (*IO Supervisor*, Câmeras de vídeo): de 192.168.2.200 até 192.168.2.254

### **3.2.1.7 Diagnóstico**

O padrão PROFINET disponibiliza um compreensível diagnóstico do *IO Device* e da rede. Além dos mecanismos de diagnósticos do PROFINET, padrões como SNMP e HTTP podem ainda integrar os conceitos de diagnósticos.

Diagnósticos baseados nos serviços web podem ser integrados ao dispositivo desde que ele tenha um endereço IP. O usuário pode através de um browser ir ao terminal do dispositivo e obter um diagnóstico local.

Este tipo de diagnóstico é quase sempre disponível na infraestrutura dos dispositivos. A riqueza de detalhes informada no terminal do dispositivo depende de cada fabricante. Vale lembrar que este recurso é opcional no padrão PROFINET.

Dentro de um telegrama de diagnósticos, *IO Devices* reportam um erro ciclicamente usando transferência IO ou aciclicamente usando alarmes. Por exemplo, um evento de queda de tensão provoca o envio de um alarme informando o evento ao controle do sistema.

Os alarmes são divididos, por sua vez, em duas categorias:

- Usuais, erros são transmitidos como alarmes de diagnósticos com parâmetros correspondentes.
- Indicadores de danos ou informações similares são codificados como alarmes de manutenção.

Vários softwares configuradores dos *IO Controllers* coletam as informações de diagnósticos e as apresentam de forma clara na topologia da rede, listando as causas dos erros através de, por exemplo, ferramentas como a detecção da topologia.

### **3.2.1.8 Detecção da topologia**

PROFINET IO usa o LLDP (*Link Layer Discovery Protocol*) para mostrar a localização exata das mensagens de diagnóstico. LLDP é uma camada independente do fabricante que pode ser usada para trocar informações entre dispositivos vizinhos. Eles informam seus nomes e seus endereços MACs com os componentes da rede através da LLDP quando a conexão está sendo estabelecida. Se todos os componentes da rede suportarem esse protocolo, uma topologia da rede precisa pode ser mostrada na ferramenta de diagnóstico. Deste modo, mensagens de diagnóstico podem ser mostradas diretamente no *IO Device*.

A Figura 19 mostra o mapeamento da rede característico do protocolo LLDP.



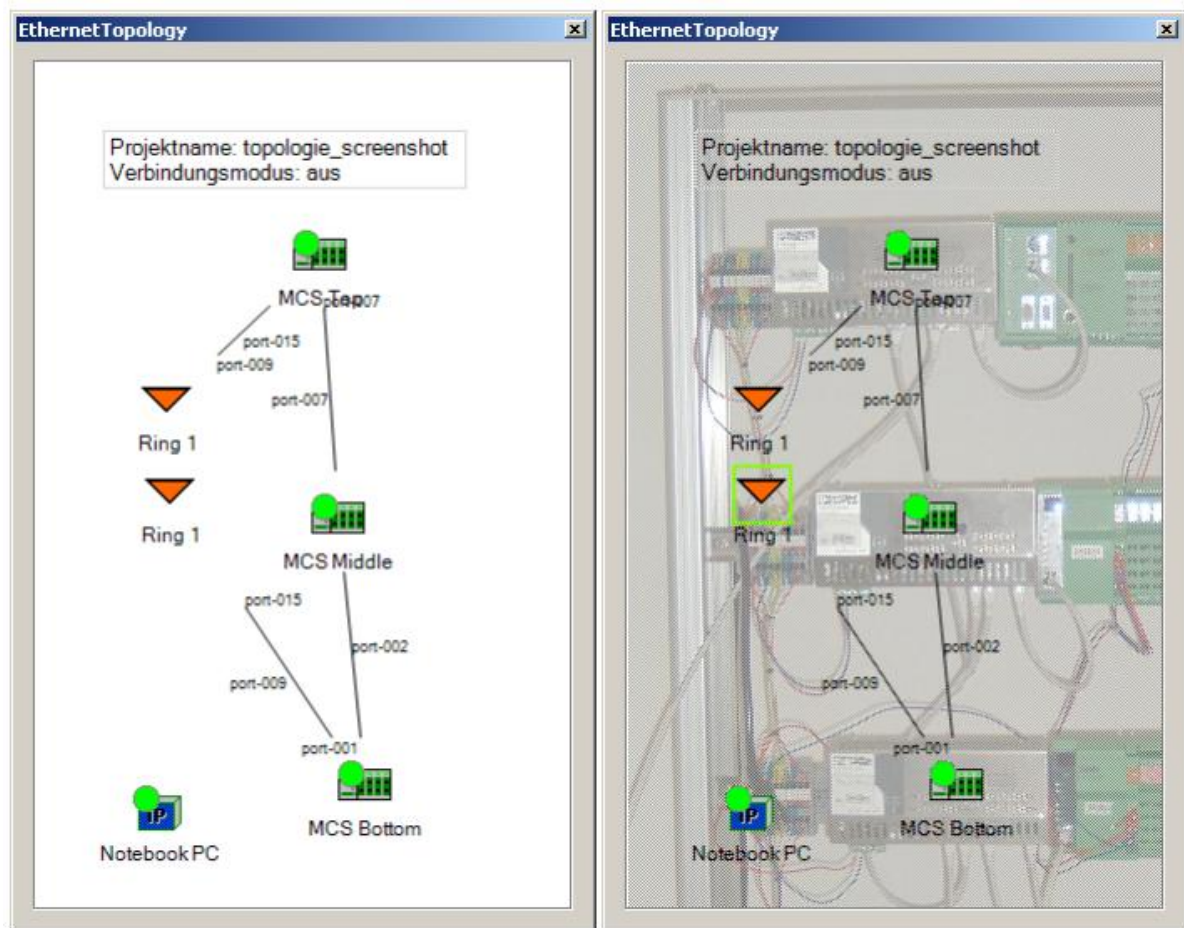


Figura 19: Detecção da topologia. Fonte [11].

### 3.2.2 PROFINET CBA

O conceito que rege o PROFINET *Component Based Automation*, ou simplesmente PROFINET CBA, é o de dividir um sistema inteiro em módulos individuais que são autônomos entre si. Esta versão do protocolo é usada para implementar automação distribuída baseada na divisão do processo inteiro em sub processos e também para comunicação *Controller-Controller*, conforme pode ser visto pela Figura 20. [11]

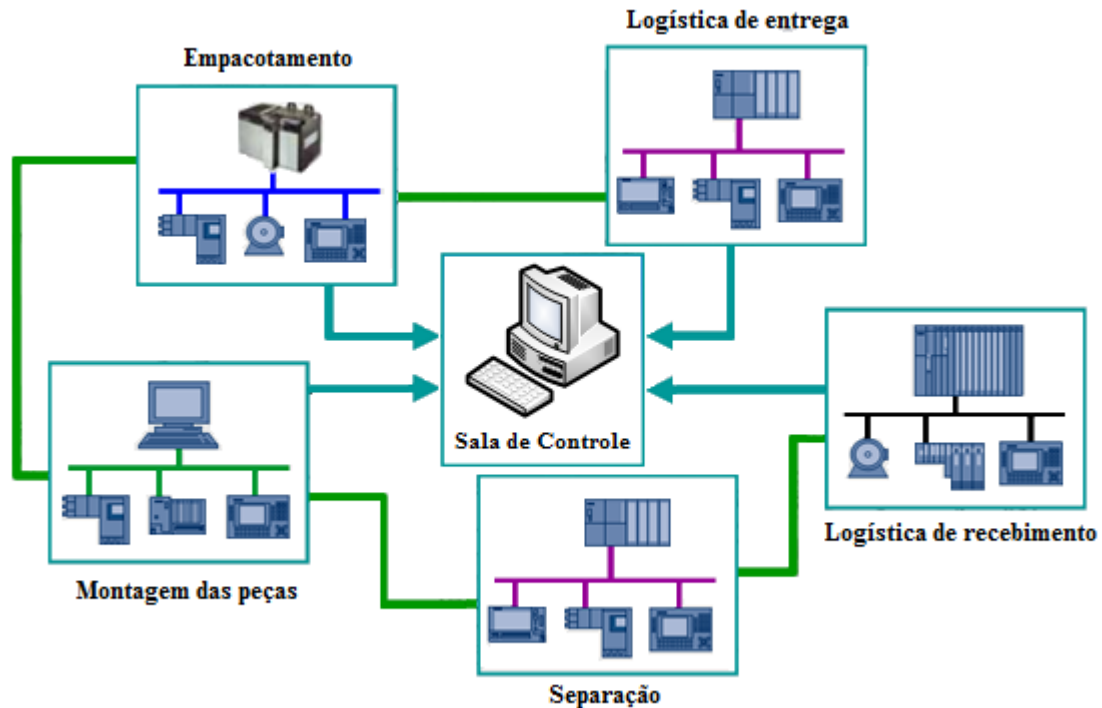


Figura 20: Subdivisão dos processos usando PROFINET CBA. Fonte [14]

PROFINET CBA suporta comunicação cíclica e acíclica com ciclos de transmissão maiores que 10 ms. Estes tempos são apropriados para comunicação entre *IO Controllers*. O protocolo TCP/IP para PROFINET CBA é aceitável para operar um processo com tempos de ciclo na faixa de 100ms.

### 3.3 Componentes da rede

#### 3.3.1 Conectores para ambientes internos

Denominam-se ambientes internos aqueles usados como salas de controle e gabinetes de *switches*.

- Conector RJ 45, de acordo com a IEC 60603-7. [17]



Figura 21: Conector RJ45 para ambientes internos.

Tabela 3: Relação de pinos dos conectores RJ45 para ambientes internos.

Sinal	Função	Cor do fio	Pinagem
RJ 45			
TD+	Transmite dado +	Amarelo	1
TD-	Transmite dado -	Laranja	2
RD+	Recebe dado +	Branco	3
RD-	Recebe -	Azul	6

- Conectores para fibra ótica

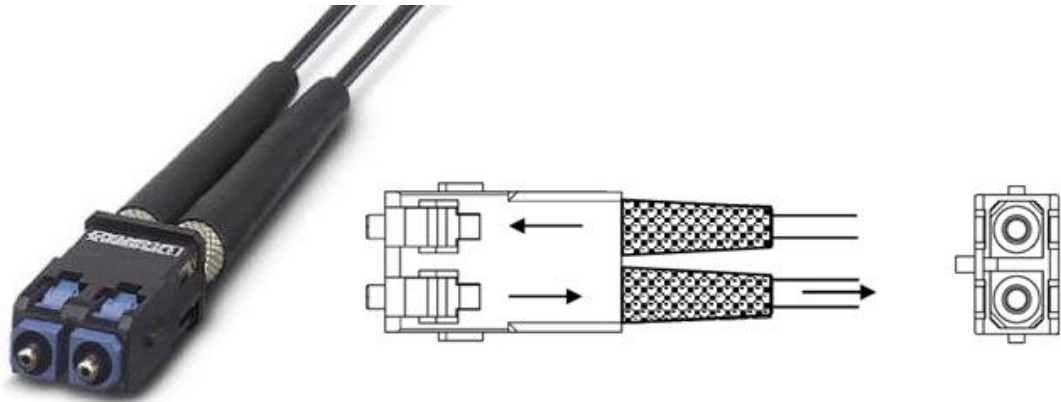


Figura 22: Conector de fibra ótica.

### 3.3.2 Conectores para ambientes externos

Ambientes externos caracterizam-se por apresentarem altas temperaturas, sujeitos à poeira, umidade e vibração.

- **Conectores RJ45 e M 12 com IP67**



Figura 23: Conector RJ45 para ambientes externos.

Tabela 4: Relação de pinos dos conectores M12 para ambientes externos.

Sinal	Função	Cor do fio	Pinagem
<b>M12</b>			
TD+	Transmite dado +	Amarelo	1
TD-	Transmite dado -	Laranja	3
RD+	Recebe dado +	Branco	2
RD-	Recebe -	Azul	4

A pinagem do conector RJ 45 para ambientes externos obedece a Tabela 3.

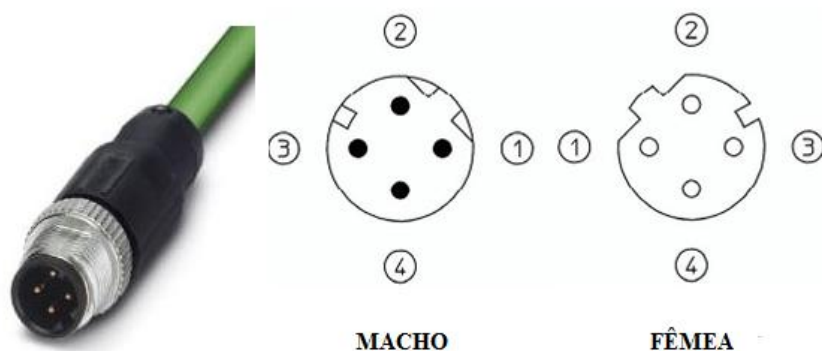


Figura 24: Conector M12 para ambientes externos.

### 3.3.2 Meios de transmissão

Assim como no protocolo Profibus, em PROFINET existem dois meios distintos de transmissão de troca de dados: cabo de cobre e fibra ótica. Conforme será explorado, os dois meios apresentam características próprias que usadas em conjunto possibilitam a construção de uma rede robusta, eficiente e inune a ruídos eletromagnéticos.

Devido a grande quantidade de aplicações diferentes, existem vários tipos de cabos de cobre e de fibra ótica que são individualizados por suas propriedades especiais. Contudo é importante ressaltar que a instalação física é uma das grandes Fontes de erros em automação industrial e cabe ao projetista determinar qual meio de transmissão será mais adequado a cada projeto. Cabe também ao instalador seguir procedimentos simples de instalação, usar ferramentas adequadas e equipamentos de proteção individual para que obtenha que se um trabalho limpo, seguro e com um nível de qualidade. No final deste tópico, encontra-se um conjunto de itens que auxiliam a instalação da rede física e a sua manutenção.

#### 3.3.2.1 Cabos de cobre

São compostos por 4 fios que se diferenciam em tipos conforme a estrutura dos fios e ao material que compõe o envoltório dos mesmos. Apresentam quatro cores codificadas, sendo o primeiro par de fios amarelo e laranja, o segundo branco e azul. As cores de cada par são alocadas diametralmente opostas. Assim como em aplicações usando Ethernet, a máxima distância é limitada a 100 metros quando usando cabos de cobre.

Os cabos são caracterizados em três classes conforme suas aplicações.[21]

- Tipo A: cabos projetados para instalações fixas. Este cabo não é sujeito a nenhum tipo de movimento depois de instalado.
- Tipo B: cabos projetados para instalações flexíveis. Este cabo permite que a haja pequenas movimentações ou vibrações.
- Tipo C: Cabos projetados para aplicações especiais. Permite movimento constante depois de instalado, por exemplo, aplicações como *festoon*. Para este tipo de cabo a distância máxima de 100 metros de cabeamento diminui.

Há ainda um número expressivo de tipos especiais de cabos de cobre produzido para diversas aplicações, conforme segue.

- Cabo PE: designados para instalações onde há umidade constante.
- Cabos de terra.
- Cabos retardantes de chama e não corrosivos (FRNC – *Flame Retardant non corrosive cables*): indicados para instalações onde há um cuidado maior em relação à prevenção e a não proliferação de incêndios.
- Cabos *Trailing*: recomendado para instalação em máquinas com partes móveis.
- Cabos *Festoon*.
- Cabos para navios: são recomendados para instalações em navios.

Serão apresentadas na Tabela 5 somente as características do cabo de cobre tipo A por este ser o mais utilizado na indústria. Todavia, as informações referentes aos cabos tipo B e tipo C podem ser adquiridas em [16].

**Tabela 5: Parâmetros do cabo de cobre tipo A.**

Parâmetro	Limites especificados
Impedância	100 $\Omega$ +- 15 $\Omega$
Taxa de transmissão	100Mbps/s
Max. comprimento do cabo	100m
Número de fios	4
Diâmetro do fio	0.64mm
Cor do envoltório	Verde
Cor dos fios	Branco, azul, amarelo e laranja

### 3.3.2.1 Fibra Ótica

Usada em áreas onde há a presença de interferências eletromagnéticas ou significativa diferença de potencial entre terras. Além disso, a fibra ótica apresenta algumas vantagens em relação ao cabeamento de cobre:

- Pode cobrir uma distância maior que o cabo de cobre.
- Prove isolamento elétrica entre áreas da planta industrial.
- São totalmente inunes às interferências eletromagnéticas.

Há quatro tipos de fibra ótica diferentes:

- Fibra ótica de plástico (POF).
- Fibra de vidro (multi-mode).
- Fibra de vidro (single-mode).
- Fibra de vidro com envoltório de plástico (HCF/PCF).

A Tabela 6 relaciona a fibra ótica com o comprimento máximo.

**Tabela 6: Comprimento máximo da fibra ótica conforme seu tipo.**

Tipo de fibra	Distância do barramento (m)
POF	+ de 50
HCF/PCF	+ de 100
Multi-mode	+ de 2000
Single-mode	+ de 14000

### 3.3.3 A switch

Em um uma aplicação real, o IO-Controller é responsável por inicializar a switch, atribuindo-a um IP, um nome, comparar a configuração presente nela com a desejada e arquivar os alarmes mandados por ela. Em cada evento de troca do dispositivo físico, o *IO-Controller* reconhece automaticamente o novo dispositivo atribuindo-o uma nova parametrização e configuração. A *switch* usada em PROFINET possui buffer para evitar colisões de mensagem conforme descrito anteriormente pelo tópico 2.3. [18]

A *switch* possui dois modos de operação: o default e o modo PROFINET. O último modo deve ser escolhido para que a switch possa fazer parte da rede PROFINET. Para realizar essa operação é possível acessar os serviços de web da *switch* através de um browser e seu IP, como é possível também mudar a configuração via serial.

A Figura 25 mostra o serviço de web da *switch* FL SWITCH MCS 16TX da *Phoenix Contact* onde é escolhido o modo de operação.

Operating Mode	
Mode	<input checked="" type="radio"/> Default <input type="radio"/> Profinet
<p><i>Mode 'Profinet'</i>            Activating the mode 'Profinet' the following settings will be done:</p> <ul style="list-style-type: none"> <li>■ <i>select ip address assignment DCP</i></li> <li>■ <i>enable LLDP</i></li> <li>■ <i>clear the default System Name like 'FL SWITCH SMCS'</i></li> <li>■ <i>save the configuration</i></li> <li>■ <i>execute a reboot</i></li> </ul> <p><i>Changing from the mode 'Profinet' to an other mode the following settings will be done independently of the setting before selecting the mode 'profinet':</i></p> <ul style="list-style-type: none"> <li>■ <i>select ip address assignment BootP</i></li> <li>■ <i>replace an empty System Name by the default System Name like 'FL SWITCH SMCS'</i></li> </ul> <p>The settings become effective after <u>saving</u> the configuration and <u>rebooting</u> the device.</p>	
Enter password	<input type="text"/> <input type="button" value="Apply"/>

Figura 25: Modos de operação da switch via serviço de rede. Fonte [18]

Quando o modo PROFINET é escolhido serviços como o LLDP são habilitados. A cada 5 segundos é transmitida uma mensagem deste tipo. Isto foi verificado no estudo de caso apresentado pelo Capítulo 4.

A switch operando como IO-Device necessita de um arquivo gsd<sup>4</sup> que pode ser encontrado no site do seu fabricante. A Figura 26 mostra os parâmetros que são definidos pelo usuário.

<sup>4</sup> Gsd: vide tópico 3.2.1.5





























	Name	Value
	Vendor	Phoenix Contact
	VendorID	0x00B0
	Designation	FL SWITCH MCS 16TX (Profinet IO)
	DeviceID	0x0013
	Functional description	Managed Compact Switch as a Profinet IO ...
	Device type	Switch
	Device family	FL
	Order number	2832700
	Revision	00/4.70/16TX
	DNS/PROFINET Device Name	fl-switch-mcs-16tx5.Teste.de
	Station Name	fl-switch-mcs
	Device Name	fl-switch-mcs
	Module Equipment ID	
	IP Address	192.168.0.5
	Subnetmask	255.255.255.0
	Default Gateway	
	Realtime class	RT
	Reduction ratio input	512 ms
	Reduction ratio output	512 ms
	Faulty telegrams until connection is aborted	3
	Monitoring Time Inputs (ms)	1536
	Monitoring Time Outputs (ms)	1536
	Operation in case of configuration differen...	no
	Log connection state	yes
	Drive BF	yes
	Node ID	762

Figura 26: Os parâmetros da *switch*. Fonte [18]

### 3.4 Conformance Classes

Para facilitar o projeto da rede, a organização PROFINET dividiu o escopo de funções PROFINET em *Conformance Classes* (CC). O objetivo foi simplificar a operação de sistemas quando PROFINET IO for usada. Todas as *Conformances Classes* incluem por padrão funções básicas como troca de dados cíclicos, acíclicos e alarmes. [11]

Existem três classes que diferem entre si, conforme o tipo dispositivo, tipo de comunicação, meio de transmissão usado.

- **Conformance Class A (CC-A):** Usa a infraestrutura da rede Ethernet presente e integra funções básicas PROFINET. Todos os serviços TI podem ser usados sem restrições. Somente esta classe permite comunicação wireless.
- **Conformance Class B (CC-B):** Em adição à CC-A, esta classe permite a reposição do dispositivo sem a necessidade de ferramenta de engenharia. Um protocolo TCP (UDP) /IP é usado para integrar a segurança dos dados. Os dispositivos de campo desta classe apresentam *switch* integradas de duas portas.
- **Conformance Class C (CC-C):** Complementar à CC-B, esta classe permite uma alta precisão e determinismo na transmissão de dados, incluindo aplicações síncronas. Indicada para aplicações como sincronismo de motores.

A Tabela 7 mostra algumas propriedades das *Conformance Classes*.

**Tabela 7: Propriedade das *Conformances Classes*.**

Características	CC-A	CC-B	CC-C
Protocolos com tempo real	<i>RT</i>	<i>RT</i>	<i>RT/IRT</i>
Tipos de dispositivos	<i>IO Controller</i> <i>IO Device</i> <i>IO Supervisor</i>	<i>IO Controller</i> <i>IO Device</i> <i>IO Supervisor</i>	<i>IO Controller</i> <i>IO Device</i> <i>IO Supervisor</i>
Usa a infraestrutura do padrão Ethernet	Sim, nenhuma certificação é necessária. <ul style="list-style-type: none"> <li>• Switches</li> <li>• WLAN</li> <li>• Bluetooth.</li> </ul>	Sim, mas switches também são IO Devices e precisam ser certificadas.	Não, necessita-se de switches com hardware capaz de suportar PROFINET IO-IRT.
Meio de transmissão	Fio de cobre (100Mbps). FO (100Mbps). Wireless <ul style="list-style-type: none"> <li>• WLAN (2.4GHz)</li> <li>• Bluetooth (5GHz)</li> </ul>	Fio de cobre (100Mbps). FO (100Mbps).	Fio de cobre (100Mbps). FO (100Mbps).
Aplicações Síncronas	Não	Não	Sim
Detecção de Topologia	Não	Sim	Sim

### 3.5 Topologias de rede

Quando uma rede de automação industrial, independente do protocolo a ser utilizado, é projetada, deve atender parâmetros necessários para seu correto funcionamento. O projetista deve estar atento aos efeitos da interferência eletromagnética para evitar acoplamento de ruído ao sinal, às distâncias a serem percorridas, aos conceitos de segurança intrínseca e de áreas classificadas, à quantidade de dados na rede, além de muitos outros fatores. Uma das vantagens do protocolo PROFINET é a flexibilidade no projeto das topologias de rede.

A combinação das possíveis topologias facilita ao projetista atender às necessidades do projeto de forma satisfatória.

Neste tópico, serão abordadas as topologias passíveis de serem adotadas. Percebe-se que são exatamente as mesmas utilizadas no protocolo Profibus, diferindo somente nos equipamentos usados. A *switch* exerce a mesma função que a *junction box* no protocolo Profibus, interliga várias estações ao mesmo barramento. No entanto, como uma diferença, a *switch* apresenta inteligência de direcionar as mensagens para seus destinatários.

Existem as seguintes topologias: [16]

- **Topologia Estrela:** É muito comum em redes PROFINET. Indicada para ambientes com limitada extensão geográfica. Caracteriza-se por uma *switch* conectada a vários dispositivos. Se uma estação falha ou é removida, os outros nós PROFINET continuarão a funcionar. Mas, se a *switch* falha, a comunicação com as demais estações será interrompida.
- **Topologia Árvore:** Esta topologia é criada a partir da junção de várias redes com topologia estrela. Uma *switch* central trabalha como distribuidora de sinal para as redes com topologia em estrela. Como as *switches* encaminham os dados baseadas no endereço, as mensagens são destinadas à rede correta e assim, para o aparelho certo. Essa topologia é tipicamente usada em plantas industriais para conectar setores diferentes.
- **Topologia linha ou barramento:** É a mais conhecida topologia em automação industrial. Os dispositivos PROFINET que possuem uma *switch* interna facilitam o uso desta aplicação. Ao contrário das topologias estrela e árvore, se um aparelho falha ou é retirado, os aparelhos localizados após esse dispositivo perdem comunicação com os demais. Isto pode ser contornado pelo uso da

estrutura em anel, O que garante mais robustez à rede.

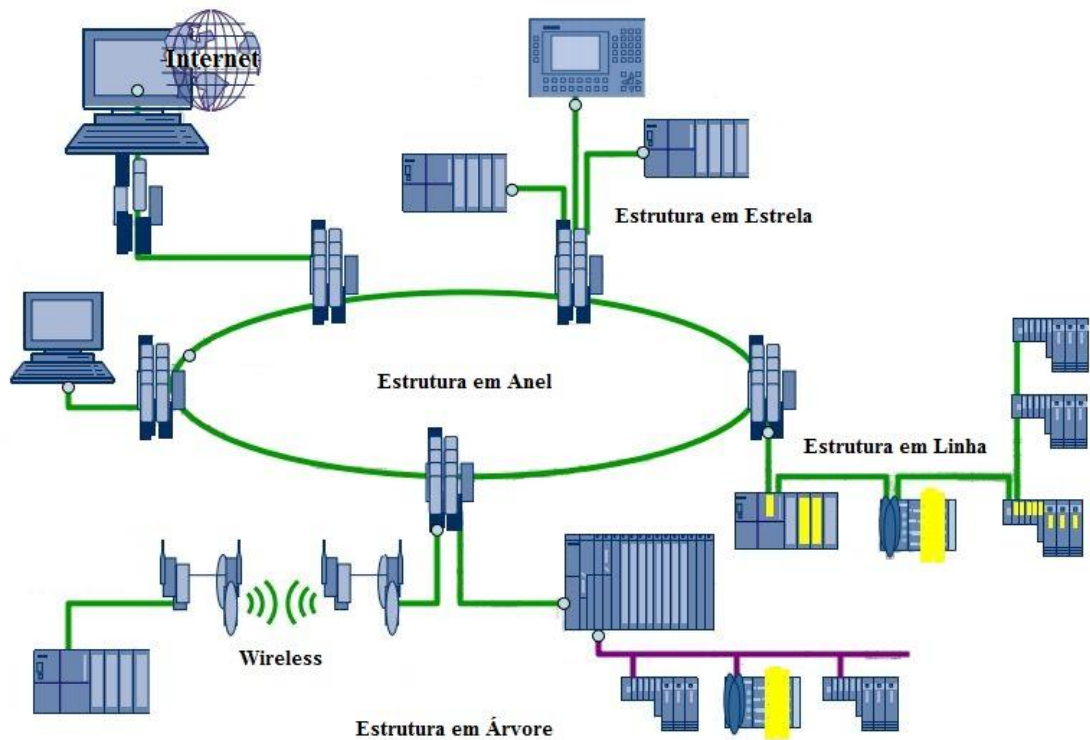


Figura 27: Exemplos de topologias de rede. Fonte: [11]

### 3.6 Wireless

Nas últimas décadas, a complexidade do cabeamento foi reduzida com a implementação dos protocolos de campo nas fábricas. Entretanto, aplicações em áreas agressivas ou em máquinas rotativas ainda necessitam de cuidados especiais. Para esses tipos de instalações, a comunicação *wireless* pode ser altamente satisfatória. O mercado está aumentando gradualmente para esse tipo de tecnologia. A comunicação *wireless* pode ser incorporada em diferentes áreas e com diferentes funções, como por exemplo, conectar segmentos de redes e realizar comunicação com dispositivos de campo. [1]

A PNO especificou o *Bluetooth* (IEEE 802.15.1) e a WLAN (IEEE 802.11) para comunicações em PROFINET. Estes padrões apresentam características diferentes que os distinguem em suas aplicações.

### 3.6.1 PROFINET com comunicação WLAN

WLAN é bem resistente às interferências. Dependendo da qualidade do sinal, taxas de transmissão acima de 54 Mbit/s podem ser obtidas. Para uma frequência de 2,4 GHz são providos três canais WLAN, ao passo que usando uma frequência de 5 GHz são providos 18 canais que podem ser usados simultaneamente.

WLAN (*Wireless Local Area Network*) é um padrão que opera na Camada Física do modelo OSI, o que significa que os frames do PROFINET RT podem ser transmitidos transparentemente.

A taxa máxima de troca de dados varia entre 6Mbit/s e 25 Mbit/s para transmissão half duplex. Apesar dos frames do PROFINET RT serem transmitidos transparentemente, a velocidade de tempo real baseada em cabos (100Mbps) nunca será atingida. Se uma rede WLAN é composta unicamente de um dispositivo, tempos de ciclos curtos de 4ms a 8ms podem ser obtidos com pequenos *jitters*.

Como um meio público é usado para transmitir os dados na comunicação *wireless*, uma ampla gama de interferência pode ocorrer. Entretanto, WLAN transmite na faixa de 2.4 GHz, a transmissão não é deturpada por interferências de campo, que ocorrem a uma faixa de kHz e MHz.

### 3.6.2 Comunicação PROFINET via Bluetooth

Bluetooth é uma tecnologia *wireless* que tem se tornado muito popular na indústria. Segundo [18], mais *chips* Bluetooth são vendidos do que WLAN a cada ano. Isto ocorre predominantemente no uso da tecnologia para aparelhos celulares. O Bluetooth foi padronizado pela IEEE 802.15.1. Além disso, o SIG (*Grupo especial de Interesse Special Interest Group*), uma associação de fabricantes de chips e aparelhos Bluetooth, definiu vários perfis de aplicação, o perfil Bluetooth para transmissão de voz, o perfil para comunicação serial e também o perfil para transmissão Ethernet. [19]

Bluetooth provou ser muito eficaz em ambientes industriais com grande quantidade de concreto reforçado e aço. Ademais, essa tecnologia trabalha com uma largura de banda de 1MHz no espectro de frequência, o que possibilita vários sistemas de operarem em simultaneamente sem efeitos adversos. Embora esse fato leve a uma

limitação na velocidade de transmissão que é de aproximadamente 700 kbps é ainda rápido o suficiente para uma série de aplicações em automação.

A princípio, o método de operação do Bluetooth não necessita de configuração de nenhum parâmetro *wireless* para estabelecer uma comunicação, a ideia é que a tecnologia seja transparente para o usuário final, sem que exija conhecimentos avançados. [19]

Para atingir um alto nível de confiabilidade durante a transmissão de dados, os dispositivos usam *adaptive frequency hopping*. Uma transmissão de dados com *adaptive frequency hopping* ocupa a banda de 2.4GHz inteira, onde há troca de 79 canais 1600 vezes por segundo, de forma que se um canal está sendo usado ou sofre uma perturbação de outro sinal *wireless*, é removido da *hopping sequence*.

Em outras palavras esse esquema é chamado de "salto de frequência". Isso possibilita que o dado seja transmitido e nenhum outro sinal *wireless* seja perturbado. Conforme pode ser observado pela Figura 28, vários sinais *wireless* operam em uma mesma planta.

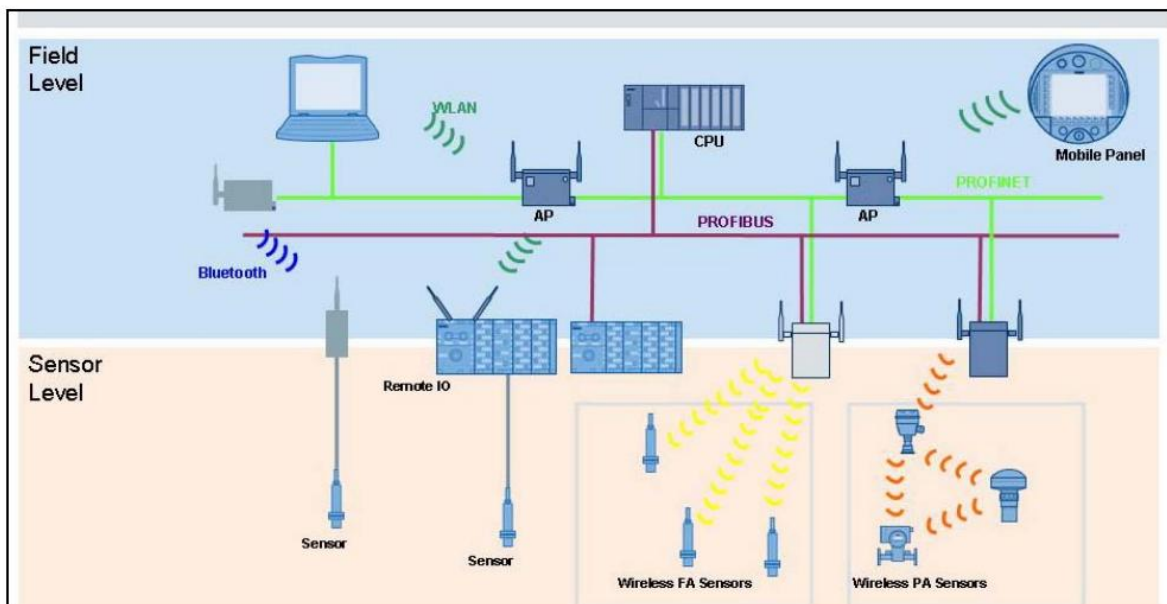


Figura 28: Vários sinais wireless presentes em uma planta industrial. Fonte [19]

### 3.7 Segurança

Durante os últimos anos, sistemas de automação eram compostos por computadores individuais e isolados. Atualmente, sistemas de automação estão sendo integrados através de *sítes* e redes corporativas. Esta arquitetura integrada prove muitos benefícios. Há uma maior visibilidade do chão de fábrica possibilitando melhoria na tomada de decisões e análises. Usar uma única interface reduz custos de diagnósticos e além do mais, permitem acesso remoto aos processos de produção. [19]

Ademais, comunicação integrada verticalmente entre todos os níveis de automação, em particular a interconexão entre redes de automação e redes de escritório baseadas no padrão Ethernet agregaram valor aos sistemas de controle e manufaturamento. Entretanto, a facilidade para a troca de dados aumentou, por sua vez, a vulnerabilidade das plantas às ações maliciosas que podem ocasionar danos aos processos. Estas ações são conhecidas há anos nas redes corporativas, mas não no mundo da automação. [19]

O crescente uso de sistemas baseados em padrões (como por exemplo, baseados em *Windows*) assim como redes baseadas em Ethernet e TCP/IP em automação tornaram esses sistemas também vulneráveis a ataques de vírus, *worms* e cavalos de tróia. Vale lembrar que todas essas novas vulnerabilidades às quais as novas arquiteturas e o uso de *softwares* conhecidos estão sujeitos, deve-se ao fato de que sistemas de automação foram projetados para tem desempenho, não segurança. Como consequência, pessoas não autorizadas podem, potencialmente podem acessar bases de dados, remotas. Os invasores podem até ser empregados realizando tarefas inapropriadas ou mesmo agindo de má fé por saberem das vulnerabilidades do sistema. Dentre os danos que invasores podem acarretar, pode se citar o acesso às informações confidenciais, perda de integridade e confiabilidade de dados do processo, danos nos equipamentos e danos aos funcionários. [19]

O protocolo PROFINET adotou um padrão de segurança baseado em cinco pontos:

- **Arquitetura da rede:** este conceito é baseado na idéia de que uma planta industrial possa ser dividida em zonas de segurança (também denominadas células). Células diferentes podem ser interconectadas por um barramento principal, onde cada célula deva ter somente um ponto de acesso a este

barramento. Pode-se ainda realizar uma conexão deste barramento principal ao escritório.

- **Confiança:** Dentro de cada zona de segurança, a comunicação é baseada na confiança. Todos os dispositivos podem comunicar-se entre si livremente, o que significa que todos os componentes de uma zona de segurança podem comunicar-se com componentes de outra zona. Componentes não pertencentes às zonas de segurança que estejam isolados, conectados ao barramento principal e redes de escritórios podem ter permissão para se comunicarem com as zonas de segurança. Interconectando mutuamente todas as zonas de segurança será expandido o conceito de uma rede fechada. Uma rede é denominada aberta se, um dispositivo de fora da rede pudesse se comunicar com dispositivos de dentro de uma zona de segurança.
- **Perímetro de defesa:** Cada zona segura deve ser protegida por algum tipo de *firewall* localizado no ponto de acesso ao barramento principal. Este *firewall* deve permitir comunicação entre seus dispositivos e componentes de outras zonas seguras ou redes de escritório. Como é fácil copiar e forjar IP ou MAC, o controle de acesso não deve ser baseado apenas em filtragem de endereços, mas também em protocolos criptografados.
- **Confiabilidade e integridade:** A comunicação entre *firewalls* que protegem zonas de segurança ou entre um firewall e um dispositivo pertencente a uma zona tem que ser protegida contra perdas de confiabilidade e integridade. Ambas devem ser providas, baseadas na padronização de protocolos de segurança de rede.
- **Integração transparente a firewalls:** O *firewall* de uma zona de segurança deve ser implementado de forma transparente.

Para concluir os tópicos referentes à teoria do protocolo PROFINET, é recomendado que se faça um *checklist* visual que evita os erros mais comuns de acordo com [20].

Tabela 8: Checklist visual da rede.

Sim Não		Aspecto a ser verificado
1.		O tipo de cabo é adequado?
2.		O comprimento máximo do cabo (100m para cabos de cobre) foi obedecido?



- 
- |     |  |
|-----|--|
| 3.  | O conector usado está de acordo com o plano (RJ45, M12,...)?                         |
| 4.  | O cabo PROFINET está danificado?   |
| 5.  | Quinas de calhas metálicas estão sem rebarbas ou superfícies cortantes?              |
| 6.  | Precauções contra danos mecânicos foram tomadas?                                     |
| 7.  | A malha de blindagem está conectada aos painéis e estes estão devidamente aterrados? |
| 8.  | A topologia foi observada?   |
| 9.  | Existe uma porta Ethernet para conexões de analisadores?                             |
| 10. | A Fonte de alimentação está de acordo com as especificações do projeto?              |
| 11. | A malha de blindagem do cabo PROFINET está conectada ao terra?                       |
| 12. | Equipotencialidade de terra garantida de acordo com as normas?                       |
-



## **CAPÍTULO 4**

### **O estudo de caso**

Este capítulo foi originalmente pensado como forma de verificar, na prática, tudo o que foi observado na teoria. Ademais, destinou-se um tópico para comparar o protocolo PROFINET com o Profibus. Tomou-se o cuidado de descrever detalhadamente todos os experimentos e análises realizadas, buscando sempre a melhor forma para expor os resultados.

#### **4.1 Introdução**

Um dos grandes desafios para a conclusão deste trabalho foi a ausência de equipamentos PROFINET no Laboratório de Automação Industrial (LAI) da Universidade de São Paulo – São Carlos. Até o presente momento da conclusão deste trabalho, o LAI já adquiriu alguns deles, todavia não atendendo aos objetivos deste trabalho. Por ser a primeira abordagem do protocolo PROFINET no LAI, priorizou-se os tópicos mais importantes, com receio de omitir informações relevantes.

Surgiu então, a necessidade de buscar uma solução na indústria para a conclusão da parte prática deste trabalho. Gentilmente, o Dr. José Guilherme Sabe abriu as portas da Equitron Automação, empresa localizada no município de São Carlos, a visitas para aquisição de dados. Além disso, o engenheiro Guilherme Fernandes, de forma brilhante, soube entender as necessidades do trabalho e adequa-las à realidade da empresa.

A partir daí, o trabalho ganhou outra dimensão. Utilizando a linha de produção da Equitron, pôde-se estudar uma aplicação do protocolo e vê-lo em funcionamento. Mais do que esperado, a linha de produção possibilitou comparar os

protocolos Profibus e PROFINET em condições reais iguais. Esta análise foi enriquecedora tanto para o trabalho quanto para o conhecimento pessoal do autor.

Por razões éticas, optou-se por não revelar os detalhes industriais presentes nos equipamentos e nas malhas de controle dos mesmos. Ademais, esta parte não é relevante para as análises e estudos realizados a seguir, foco principal do trabalho não foi comprometido.

## 4.2 A arquitetura

O estudo ao longo deste capítulo será baseado nas topologias mostradas pela Figura 29 e pela Figura 30, deste modo, há necessidade de descrevê-las sucintamente dentro dos limites estabelecidos pelo bom senso.

Denominou-se rede Profibus a rede composta por um mestre e um escravo, ambos da fabricante Siemens. O mestre é uma CPU IM151-8 PN/DP (order number 6ES7 151-8AB01-0AB0 / V3.2) e o escravo é um inversor de frequência SINAMICS S110 CU305 V4.3 ( order number 6SL3 040-0JA00-0xxx).

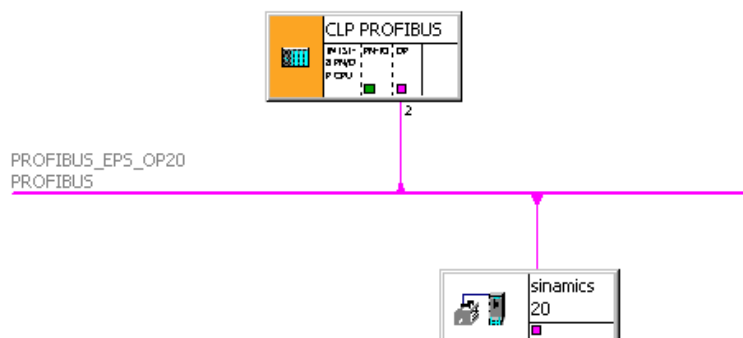


Figura 29: Rede Profibus.

Da mesma maneira, denominou-se rede PROFINET a rede composta por um IO-Controller e um IO- Device, também ambos da fabricante Siemens. O IO-Controller é uma CPU IM151-8 PN/DP (order number 6ES7 151-8AB01-0AB0 / V3.2) e o IO-Device é um inversor de frequência SINAMICS S120-CBE20-V4.4 ( order number (6SL3 040-10A0x-0AA0 / V4.4).

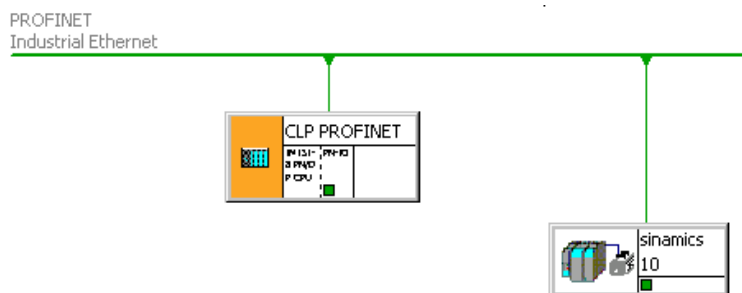


Figura 30: Rede PROFINET.

A linha de produção é composta por máquinas distintas. Cada uma contém uma pequena rede que atende às necessidades daquela máquina e, em uma visão geral, todas as máquinas eram interconectadas por cabos Ethernet e RS485, de forma que as sub-redes eram interconectadas também, formando uma rede única global Profibus e uma PROFINET. Na fase de aquisição de dados, a sub-rede foi isolada da rede global descrita de forma a obter as topologias mostradas pelas Figura 29 e Figura 30

### 4.3 As análises

Para monitorar a troca de dados da rede PROFINET, contou-se com o auxílio do *software Wireshark* versão 1.3.6-SVN-33047. Com base nessa aquisição de dados foram feitas as análises pertinentes. Ao todo, a rede foi monitorada por 600 minutos. A princípio este tempo parece insuficiente, mas vale lembrar que os protocolos trabalham na escala de milissegundos, tornando-se assim, suficiente o espaço amostral.

Iniciando as análises, a partir da Figura 31 foi possível verificar que o meio físico Ethernet é compartilhado por uma gama de protocolos e não exclusivo ao protocolo PROFINET.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq , Seq=30513, Delay=
2	0.028547	192.168.164.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
3	0.186390	192.168.164.1	192.168.164.255	NBNS	Name query NB ARMMF.ADOBE.COM<00>
4	1.200118	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq , Seq=30514, Delay=
5	1.301128	SiemensA_f4:5f:ad	LLDP_Multicast	LLDP	Chassis Id = eps.plcop030 Port Id = port-002 T
6	1.962181	192.168.164.1	192.168.164.255	NBNS	Name query NB ARMMF.ADOBE.COM<00>
7	2.400159	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq , Seq=30515, Delay=
8	2.713624	192.168.164.1	192.168.164.255	NBNS	Name query NB ARMMF.ADOBE.COM<00>
9	3.025668	192.168.164.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
10	3.477977	192.168.164.1	192.168.164.255	NBNS	Name query NB ARMMF.ADOBE.COM<00>
11	3.600200	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq , Seq=30516, Delay=
12	4.800261	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq , Seq=30517, Delay=
13	5.374844	192.168.164.1	192.168.164.255	NBNS	Name query NB ARMMF.ADOBE.COM<00>
14	6.000392	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq , Seq=30518, Delay=
15	6.036574	192.168.164.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
16	6.130049	192.168.164.1	192.168.164.255	NBNS	Name query NB ARMMF.ADOBE.COM<00>
17	6.301417	SiemensA_f4:5f:ad	LLDP_Multicast	LLDP	Chassis Id = eps.plcop030 Port Id = port-002 T
18	6.546029	fe80::59ea:1a08:ca ff02::1:3		LLMNR	Standard query A wpad
19	6.546507	192.168.164.1	224.0.0.252	LLMNR	Standard query A wpad
20	6.597990	fe80::59ea:1a08:ca ff02::1		ICMPv6	Router advertisement
21	6.644835	fe80::59ea:1a08:ca ff02::1:3		LLMNR	Standard query A wpad

Figura 31: Aquisição dos dados com o software Wireshark.

O próprio software indica que o protocolo PTCP (*Precision Time Control Protocol*) é referente ao PROFINET.

Considerando Figura 34, observa-se que o PN-PTCP representa um total de 27,5% de todos os frames enviados, totalizando 542 *frames*. Com auxílio da Figura 35, pode-se quantificar o número de bytes enviados. Chega-se ao valor de 16,15% de todos os bytes enviados, ou 32520 bytes. Calculando, chega-se em 60 bytes por *frame* conforme indicado pela Figura 32.

11	3.600200	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq , Seq=30516, Dela
12	4.800261	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq , Seq=30517, Dela
13	5.374844	192.168.164.1	192.168.164.255	NBNS	Name query NB ARMMF.ADOBE.COM<00>
14	6.000392	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq , Seq=30518, Dela
15	6.036574	192.168.164.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
16	6.130049	192.168.164.1	192.168.164.255	NBNS	Name query NB ARMMF.ADOBE.COM<00>
17	6.301417	SiemensA_f4:5f:ad	LLDP_Multicast	LLDP	chassis Id = eps.plcop030 Port Id :
18	6.546029	fe80::59ea:1a08:ca ff02::1:3		LLMNR	Standard query A wpad
19	6.546507	192.168.164.1	224.0.0.252	LLMNR	Standard query A wpad
20	6.597990	fe80::59ea:1a08:ca ff02::1		ICMPv6	Router advertisement
21	6.644835	fe80::59ea:1a08:ca ff02::1:3		LLMNR	Standard query A wpad

Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)					
Ethernet II, Src: SiemensA_f4:5f:ad (00:0e:8c:f4:5f:ad), Dst: LLDP_Multicast (01:80:c2:00:00:0e)					
Destination: LLDP_Multicast (01:80:c2:00:00:0e)					
Source: SiemensA_f4:5f:ad (00:0e:8c:f4:5f:ad)					
Type: PROFINET (0x8892)					

Figura 32: Quantidade de bytes por frame do protocolo PROFINET- PTCP.

Observa-se uma variação da quantidade de bytes por frames quando o protocolo LLDP é analisado. Cada frame é composto por 127 bytes no campo de dados. LLDP é um protocolo de camada 2, independente do fabricante usado para

apurar a identidade e a funcionalidade e receber informações da mesma camada física de outros dispositivos. Em outras palavras, é através do LLDP que os dispositivos PROFINET criam a topologia de rede e trocam informações entre si.

16	0.130049	192.168.104.1	192.168.104.255	NBNS	Name query NB AKMMF.ADOBE.COM<00>
17	6.301417	SiemensA_f4:5f:ad	LLDP_Multicast	LLDP	Chassis Id = eps.plcop030 Port Id =
18	6.546029	fe80::59ea:1a08:ca ff02::1:3		LLMNR	Standard query A wpad
19	6.546507	192.168.164.1	224.0.0.252	LLMNR	Standard query A wpad
20	6.597990	fe80::59ea:1a08:ca ff02::1		ICMPv6	Router advertisement
21	6.644835	fe80::59ea:1a08:ca ff02::1:3		LLMNR	Standard query A wpad

Frame 17: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits)	
Ethernet II, Src: SiemensA_f4:5f:ad (00:0e:8c:f4:5f:ad), Dst: LLDP_Multicast (01:80:c2:00:00:0e)	
Destination: LLDP_Multicast (01:80:c2:00:00:0e)	
Source: SiemensA_f4:5f:ad (00:0e:8c:f4:5f:ad)	
Type: 802.1 Link Layer Discovery Protocol (LLDP) (0x88cc)	
Link Layer Discovery Protocol	

**Figura 33: Quantidade de bytes por frame do protocolo LLDP.**

Utilizando os recursos de estatísticas do *Wireshark*, foi possível também quantificar a participação dos outros protocolos presentes no meio físico. É visível a predominância do UDP (*User Data Protocol*) com 53,58%, seguidos de protocolos menos expressivos como NetBIOS, *Hypertext Transfer Protocol*.

A quantidade de frames enviados por cada protocolo, assim como a quantidade de bytes são mostrados pelas Figura 34 e Figura 35 respectivamente.

Nota-se aqui uma grande diferença do padrão PROFINET para o padrão Profibus. Neste, o uso do meio de transmissão, seja ele o RS485 ou o *Manchester Bus Powered* (MBP) é feito por um só protocolo, ao passo que o padrão Ethernet compartilha o meio de transmissão Ethernet com uma série de deles.

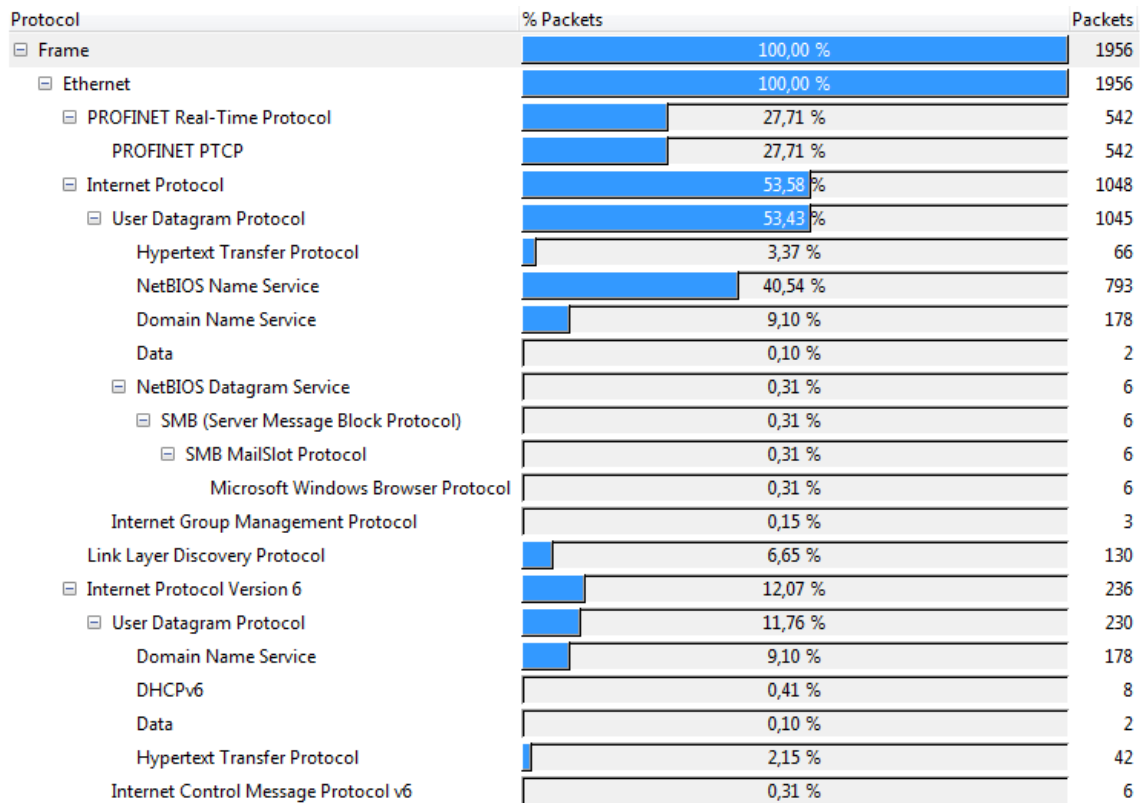


Figura 34: Quantidade de frames enviados por cada protocolo.

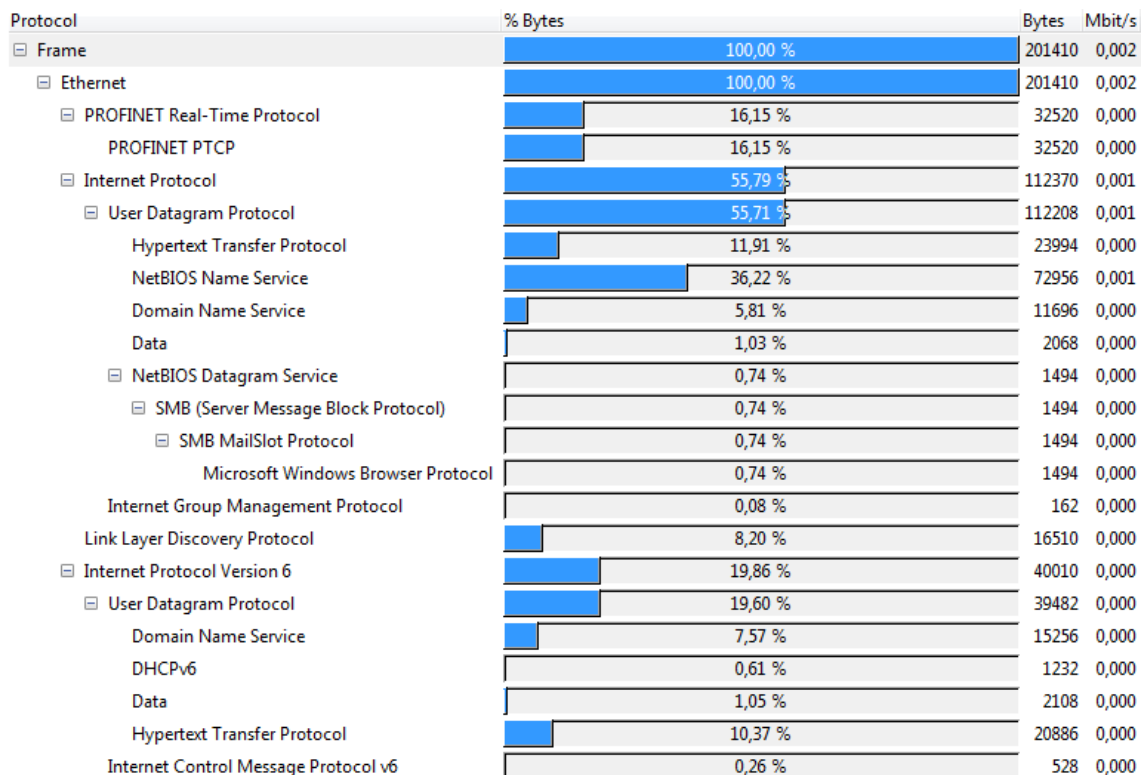


Figura 35: Quantidade de bytes enviados por cada protocolo.



## 4.4 Comparação dos protocolos

### 4.4.1 Jitter

Quando se trabalha com sistemas de comunicação, espera-se que as mensagens cheguem em intervalos de tempo determinados. Mas, na situação real não é isso que acontece, as mensagens podem chegar atrasadas ou adiantadas.

Essas variações de tempo é o que foi denominado *jitter*. Neste trabalho, o conceito de jitter é utilizado para quantificar a variação de tempo dos pacotes em uma rede. O termo correto a se utilizar nesse caso seria *Packet Delay Variation*. A Figura 36 representa as três possíveis condições de *jitter*:

- Atrasado: quando o pacote de dados de referência inicia-se antes do pacote real.
- Avançado: quando o pacote de dados de referência inicia-se depois do pacote real.
- Situação ideal: quando o pacote de dados de referência inicia-se ao mesmo tempo que o pacote real.

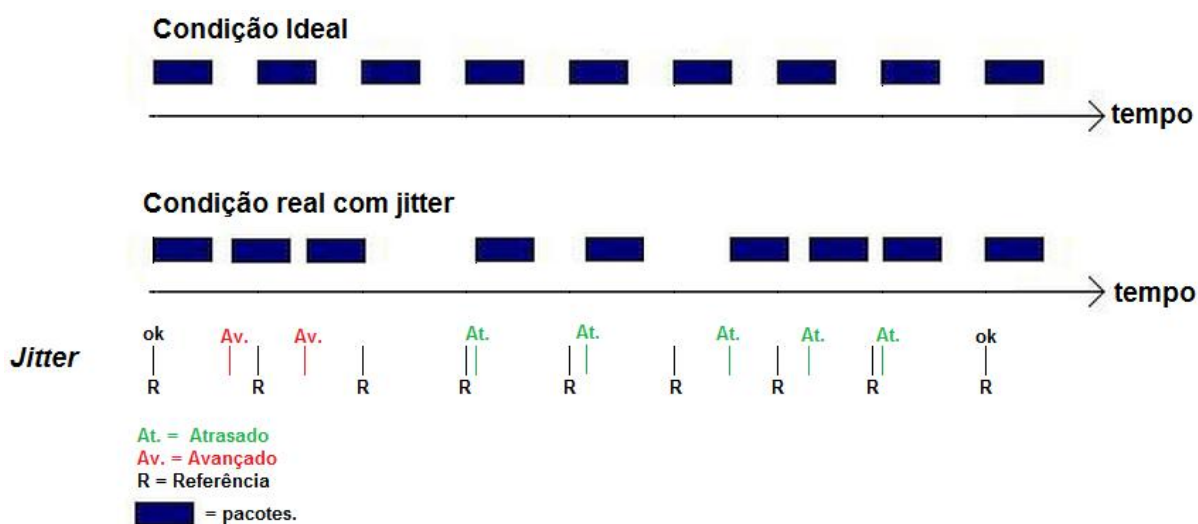


Figura 36: Situações de *Jitter*.

Optou-se pelo estudo deste conceito devido sua importância na indústria. Um atraso excessivo pode causar instabilidade e em situações mais graves até acidentes.

#### 4.4.2 A comparação

Os estudos que seguem agora são regidos pelo conceito apresentado. As duas redes analisadas serão comparadas em relação aos seus respectivos *jitters*.

Com auxílio do analisador de rede *Protocol Analyzer* da fabricante *Softing*, foi monitorada a troca de comunicação da rede Profibus e, como já citado, com o *software Wireshark* foi possível monitorar a troca de dados da rede com o outro protocolo. A rede Profibus também foi monitorada por 600 minutos.

Houve a necessidade de uma preparação das amostras coletadas antes que fosse possível aferir alguma informação. Durante esta fase de estudo dos *frames*, notou-se que o inversor de frequência na rede PROFINET informava seus dados sem a necessidade do *IO-Controller* requisitá-las, fato que verifica o sistema Provider Consumer do protocolo e não logo o sistema mestre escravo do protocolo Profibus. É conveniente citar que o IO-Device manda sua mensagem no modo *LLDP\_Multicast* ou para o *MAC address* 01:80:c2:00:00:0e, conforme pode ser visto na Figura 37, para destiná-la à todos os dispositivos pertencentes à rede. No protocolo PROFIBUS, a mensagem é destinada para endereços específicos.

Time	Source	Destination	Protocol	Length	Info
14 6.000392	SiemensA_f4:5f:ad	LLDP_Multicast	PN-PTCP	DelayReq	, Seq=30518, Dela
15 6.036574	192.168.164.1	239.255.255.250	SSDP	M-SEARCH *	HTTP/1.1
16 6.130049	192.168.164.1	192.168.164.255	NBNS	Name query NB	ARMMF.ADOBE.COM<00>
17 6.301417	SiemensA_f4:5f:ad	LLDP_Multicast	LLDP	Chassis Id =	eps.plcop030 Port Id
18 6.546029	fe80::59ea:1a08:ca ff02::1:3		LLMNR	Standard query A	wpad
19 6.546507	192.168.164.1	224.0.0.252	LLMNR	Standard query A	wpad
20 6.597990	fe80::59ea:1a08:ca ff02::1		ICMPv6	Router advertisement	
21 6.644835	fe80::59ea:1a08:ca ff02::1:3		LLMNR	Standard query A	wpad

+	Frame 14: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
+	Ethernet II, Src: SiemensA_f4:5f:ad (00:0e:8c:f4:5f:ad), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
+	PROFINET acyclic Real-Time, Delay, ID:0xff40, Len: 44
+	PROFINET PTCP, DelayReq: Sequence=30518, Delay=0ns

Figura 37: Mensagem de multicast da rede PROFINET.

Prosseguindo com os procedimentos, calculou-se o tempo entre dos eventos consecutivos do mesmo tipo.

A

Tabela 9 mostra os primeiros valores encontrados para os protocolos abordados para demonstrar o raciocínio adotado para calcular o *jitter*.

Tabela 9: Tempo entre dois eventos sucessivos iguais dos respectivos protocolos.

Tempo Profibus ( $\mu$ s)	Tempo PROFINET LLDP ( $\mu$ s)	Tempo PROFINET PTCP ( $\mu$ s)
17.750	5.000.289	1.200.118
17.750	5.000.339	1.200.041
17.752	5.000.306	1.200.041
17.749	5.000.321	1.200.061
17.751	5.000.317	1.200.131

Por requisitos do projeto, a taxa de comunicação adotada no protocolo Profibus foi de 1,5Mbps e o tempo de ciclo da rede Profibus é de 17.750  $\mu$ s. Foi estabelecido que o IO-Device enviaria a cada 1.200.000  $\mu$ s uma mensagem PN-PTCP e a cada 5.000.000  $\mu$ s segundos uma mensagem LLDP (*tempo default*).

Com base nesses valores, foi verificada a variação em torno dos valores de referência para os protocolos, os primeiros resultados são apresentados pela Tabela 10, somente para ilustrar o raciocínio adotado, todavia esta tabela é composta por centenas de pontos.

Tabela 10: Variação do tempo em torno dos valores de referencia.

Tempo Profibus ( $\mu$ s)	Tempo LLDP ( $\mu$ s)	Tempo PROFINET PTCP ( $\mu$ s)
0	289	118
0	339	41
2	306	41
1	321	61
1	317	131

Com os valores das variações e obedecendo aos princípios matemáticos, foi plotado com auxílio do *software Matlab* os histogramas representados pela Figura 33, Figura 34 e Figura 35.

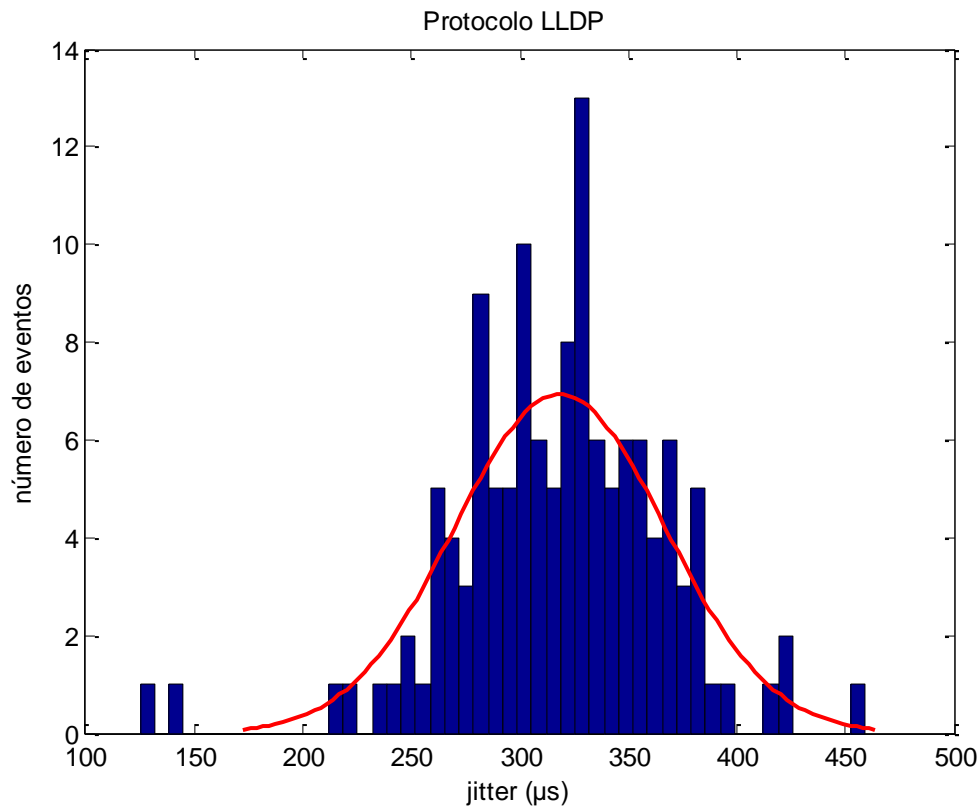


Figura 38: Histograma do jitter nas mensagens LLDP

Optou-se por analisar o *jitter* das mensagens LLDP por estas fazerem parte da rotina de funções dos dispositivos PROFINET, especialmente as *switches*. Foi verificado um *jitter* médio de 322 $\mu s$ , todavia, na literatura não foi encontrado um valor normativo para essa mensagem que possibilitasse uma comparação.

Acredita-se que um *jitter* médio de 322 $\mu s$  seja aceitável para esse tipo de mensagem, visto que o seu papel dela é trocar informações de funcionalidade e criar a topologia entre os dispositivos pertencentes a uma mesma rede. Não há necessidade de um sincronismo rigoroso para tal aplicação.

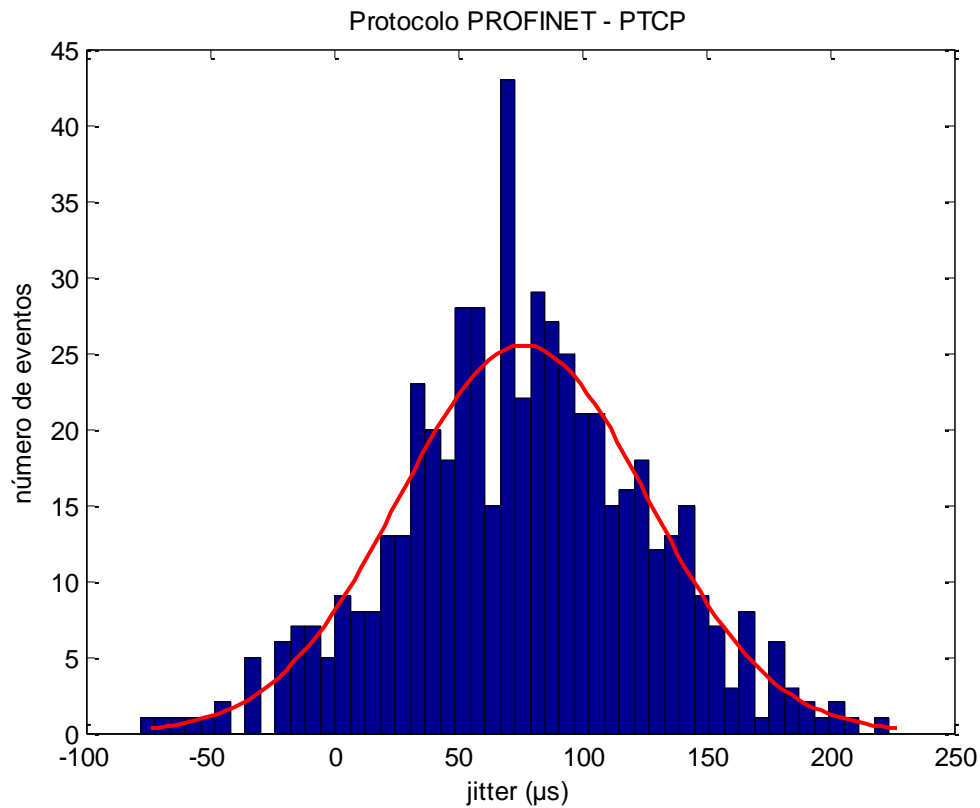


Figura 39: Histograma do jitter visto nas mensagens PROFINET PTCP.

O histograma representado pela Figura 39 expressa os valores de *jitter* em função de eventos. Observou-se um *jitter* médio de 76µs. Para aplicações de PROFINET IRT com tempos de ciclo em torno ou menores de 1ms e *jitter* tipicamente menor que 1µs os *jitter* apresentados seriam considerados extremamente elevados. Todavia, na aplicação estudada somente havia comunicação em tempo real (real time), o que torna os valores encontrados fortemente aceitos.

Já o histograma mostrado pela Figura 41 representa o *jitter* encontrado na rede Profibus. Observou-se um *jitter* médio de 1µs o que confere confiabilidade elevada a esse padrão de comunicação industrial.

É oportuno citar neste momento a quantidade de bytes enviados por cada *frame* Profibus. Com auxílio da Figura 40, chega-se ao valor de 18 bytes no campo de dados, todavia, para que a comparação seja realizada, é necessário somar o SD, o LE, o LEr, o SDr, o DA, o AS, o FC, o FCS e, por fim, o ED, totalizando 27bytes enviados em cada *frame*.

2 -> 4	DP	Request	DATA EXCHANGE	04 3F 80 00 00 00 00 00 40 09 00 01 53 D8 00 00 23 28 40
2 -> 4	DP	Request	DATA EXCHANGE	04 3F 80 00 00 00 00 00 40 09 00 01 53 D8 00 00 23 28 40
2 <- 4	DP	Response	DATA EXCHANGE	2F 37 80 00 00 04 04 00 39 CF 00 01 53 D8 00 00 00 00
2 -> 32	FDL	Request	FDL STATUS	
2 -> 2	FDL	Request	TOKEN	

Figura 40: Bytes transmitidos pelo Profibus.

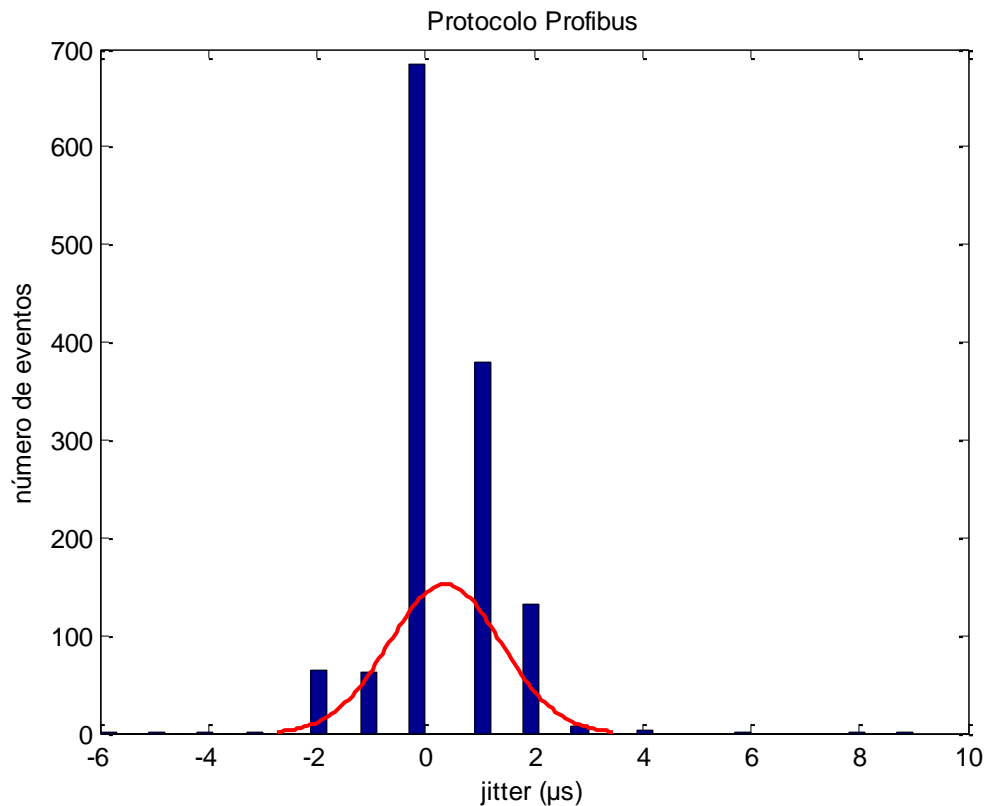


Figura 41: Histograma do jitter nas mensagens Profibus.

Comparando os resultados, não se pode intitular qual dos dois protocolos (Profibus e PROFINET) é o melhor. Tem-se, por sua vez, que considerar que apesar do protocolo PROFINET ter apresentado um *jitter* médio de 76µs, este protocolo opera com uma taxa de comunicação de 100Mbps/s e os frames contém 60 bytes, conforme pode ser visto na Figura 32. Ao passo que a rede Profibus apresentou um *jitter* médio de 1µs, mas a taxa de comunicação utilizada na aplicação é de 1,5Mbps/s e os frames contém 27 bytes, menos da metade dos bytes do padrão PROFINET.

Uma alternativa para comparar os dois protocolos diretamente foi analisar o *jitter* em função da porcentagem do tempo de ciclo. O primeiro padrão abordado foi o Profibus. Este apresenta um tempo de ciclo de 17.750 µs e um *jitter* médio de 1 µs. Este *jitter* representa 0.0056% do tempo de ciclo.

Realizando os cálculos com o padrão PROFINET, verifica-se que o *jitter* médio de 76  $\mu$ s representa 0.0063% do tempo de ciclo de 1.200.000  $\mu$ s.

Se a porcentagem for abordada separadamente, sem contexto nenhum, verifica-se que o protocolo Profibus apresenta resultado mais satisfatório, mas, como já citado anteriormente a velocidade e a quantidade de bytes do último protocolo são superiores, em outras palavras, a quantidade de bytes transmitidos na rede é maior. Conclui-se que ambos os protocolos são alternativas viáveis para o ambiente industrial, cada uma destacando-se em relação às suas particularidades.





## CAPÍTULO 5

### CONCLUSÃO

O uso de redes Ethernet para automação industrial tem apresentado um rápido crescimento devido aos seus benefícios e vantagens providas da adoção de um meio comum de comunicação a todos os níveis. A falta de determinismo e aspectos como robustez de cabos e conectores sofreram significativos avanços, fato que conferiu grande confiabilidade ao uso do padrão. Há anos, indústrias perceberam o potencial da Ethernet e financiaram o desenvolvimento de protocolos baseados nessa tecnologia.

Este trabalho apresentou as peculiaridades do protocolo PROFINET. Tal escolha deu-se pelo grande potencial de crescimento apresentado pelo mesmo e pelo intuito de agregar conhecimentos para o LAI. Foram discutidos os princípios que regem o protocolo e observou-se que o padrão de comunicação PROFINET apresenta um grau de complexidade elevado se comparado aos demais protocolos.

Com o estudo de caso, foi possível comparar o funcionamento do protocolo estudado e do protocolo Profibus. Nessa análise, foram verificados vários aspectos como número de bytes transmitidos, compartilhamento do meio físico por vários protocolos o que foge à regra do protocolo Profibus. Também foi observado o comportamento *Provider Consumer* do padrão PROFINET (este comparado com o sistema mestre escravo do Profibus) e, por fim, ambos os protocolos foram analisados em relação ao seu *jitter*.

A comparação entre os protocolos teve a finalidade de evidenciar as particularidades de ambos. A velocidade maior e a elevada quantidade de dados do padrão PROFINET possibilitam ao profissional experiente recursos expressivos de gerenciamento de ativos, todavia é fato que os dispositivos demandam uma capacidade de processamento maior.

. Fazendo-se uma analogia, cada protocolo abrange uma área específica da pirâmide de automação, para transmitir um bit não é interessante usar uma estrutura de protocolo que trabalhe com Mbit, e o inverso se aplica.

Neste contexto, é mais vantajoso fazer uso do protocolo Asi que trabalha na base de bits, do que o protocolo PROFINET que se baseia em Mbits. Haja vista que o

desenvolvimento de equipamentos, ferramentas e *hardwares* demandam um investimento financeiro diretamente proporcional ao grau de complexidade do protocolo. Não importa que se use um protocolo simples para transmitir um bit, mas sim que ele faça isso com eficiência.

Conclui-se este trabalho com a opinião que não é possível afirmar que o PROFINET é um protocolo melhor que o Profibus no contexto apresentado, mas é possível afirmar que o protocolo PROFINET é um padrão que abre maiores possibilidades para a comunicação e que cada protocolo é melhor para o tipo de função para a qual que foi projetado.

Como sugestão de trabalho futuro, seria interessante estudar a camada física e a de enlace do protocolo PROFINET. A primeira por ser responsável por relacionado à transmissão dos bits, o que envolve *jitter*, e a última por ser responsável ao tratamento do erro do protocolo, se o bit foi transmitido corretamente ou não.

## Referências Bibliográficas

1. **Silva, Ivan Nunes da.** Redes de Computadores - Notas de aula.
2. **Harald Kleines, Sebastian Detert, Matthias Drochner, Frank Suxdorf.** Performance Aspects of Profinet IO. *IEEE Transactions on nuclear Science*. Fevereiro 2008, Vols. Vol. 55, no.1.
3. **Phoenix Contact.** UM EN PROFINET SYS - User Manual - PROFINET basics.
4. **Contact, Phoenix.** User Manual - FL SWITCH MM HS UM.
5. **Jimmy Kjellsson, Anne Elisabeth Vallestad, Richard Steigmann, Dacfe Dzong.** Integration of a Wireless I/O Interface for Profibus and Profinet for Factory Automation. *IEEE Transactions of Industrial Electronics*. October 2009., Vols. Vol. 56, no. 10.
6. **Zdenek Hanzálek, Pavel Burget, Premysl Sucha.** Profinet IO IRT Message Scheduling with Temporal Constraints. *IEEE Transactions on Industrial Informatics*. Agosto 2010, Vols. Vol 6, no. 3.
7. **Brandão, Dennis.** Notas de aula - SEL 0406.
8. **Zimmermann, Hubert.** OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*. 1980, Vols. Vol. Com. 28, no. 4.
9. **Manuele Bertoluzzo, Giuseppe Buja, Stefano Vitturi.** Ethernet Networks for Factory Automation. *IEEE*. 2002.
10. **Prytz, Gunnar.** A performance analysis of Ethercat and Profinet IRT. *IEEE*. 2008.
11. **Torres, Gabriel.** *Redes de Computadores*. s.l. : Axcel Books.
12. **International, Profibus.** *PROFINET Design Guideline, Version 1.04*. 2010.
13. **Siemens.** *PROFINET System Course*. São Paulo : s.n., 2009.
14. —. *Versatile, Open and Integrated. PROFINET in Manufacturing Industry*. s.l. : Ideas 2, 2005.
15. **A. Poschmann, P. Neumann.** Architecture and Model of PROFINET IO. *IEEE*. 2004.
16. **Siemens.** The benefits of PROFINET.
17. **Profibus Internacional.** PROFINET Security Guideline. march 2005, Vol. 1.0.
18. **Profibus International.** PROFINET Cabling and Interconnection Technology - Guideline. Vols. Version 2.00, March 2007 order no: 2252.

19. —. Instalation Guideline PROFINET Part 2: Network Components. February 2004, Vols. Version 1.01, Order Number: 2252 p2.
20. **P. Ferrari, A. Flammini, D. Marioli, A.Taroni.** Experimental evaluation of PROFINET performance . *IEEE*. . 2004.
21. **International, PI.** PROFINET Commissioning Guideline Protocols and Checklist.
22. **Contact, Phoenix.** UM EN FL BT EPA - User Manual.
23. **PROCENTEC.** Certified PROFINET Engineer. 2011, Vol. 4.2.0.