CoNeT Mobile Lab 3:
PROFINET on Phoenix Contact Platform
- BASICS -

Introduction

1 What is PROFINET?

2 PROFINET vs. Profibus

3 ISO/OSI Reference Model

4 Ethernet Basics

5 Cables and Connectors

6 Internet Protocol Family

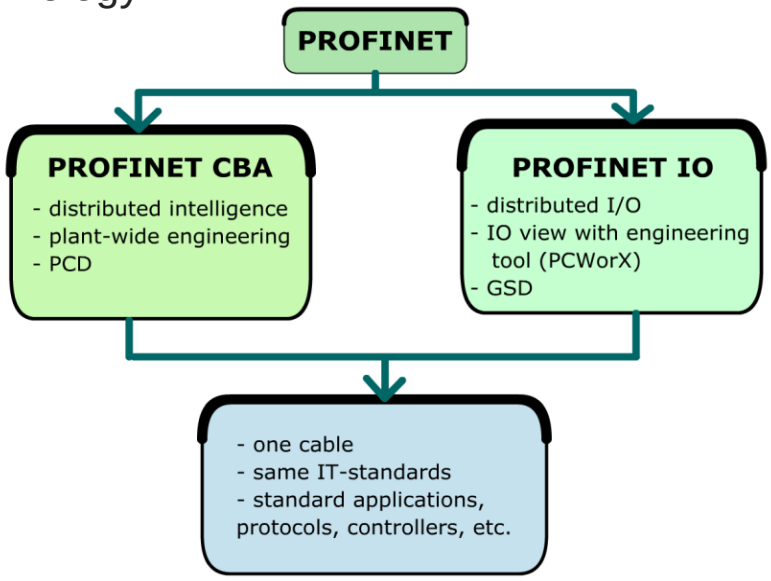
CoNeT - Co-operative Network Training

Education and Culture DG
Lifelong Learning Programme

Fachhochschule Düsseldorf

PROFINET in one statement

PROFINET is the open Industrial Ethernet Standard for Automation of PROFIBUS & PROFINET International and covers all requirements of all branches of Automation Technology.



- You can use PROFINET for your factory and process automations that require response time under 100 milliseconds.
- Other applications, like drive technology applications or clock-synchronized Motion Control, can be served with response time in less than 1 millisecond.
- To run safety applications, you can use PROFIsafe

→ Is based on Industrial Ethernet
→ Uses TCP/IP and IT standards
→ Is automation in real-time
→ Enables seamless integration of fieldbusses

Milestones

Technical milestones to market leadership

2006 TCI – Tool Calling Interface available
2005 PROFIdrive and PROFIsafe for PROFINET available
2004 PROFINET IO based on real-time (RT) and isochronous real-time (IRT)
2003 PROFIsafe appears on the market
2002 PROFINET part of IEC 61158/IEC 61784: 10 profiles available
2001 Presentation of the Ethernet-based PROFINET (CBA)

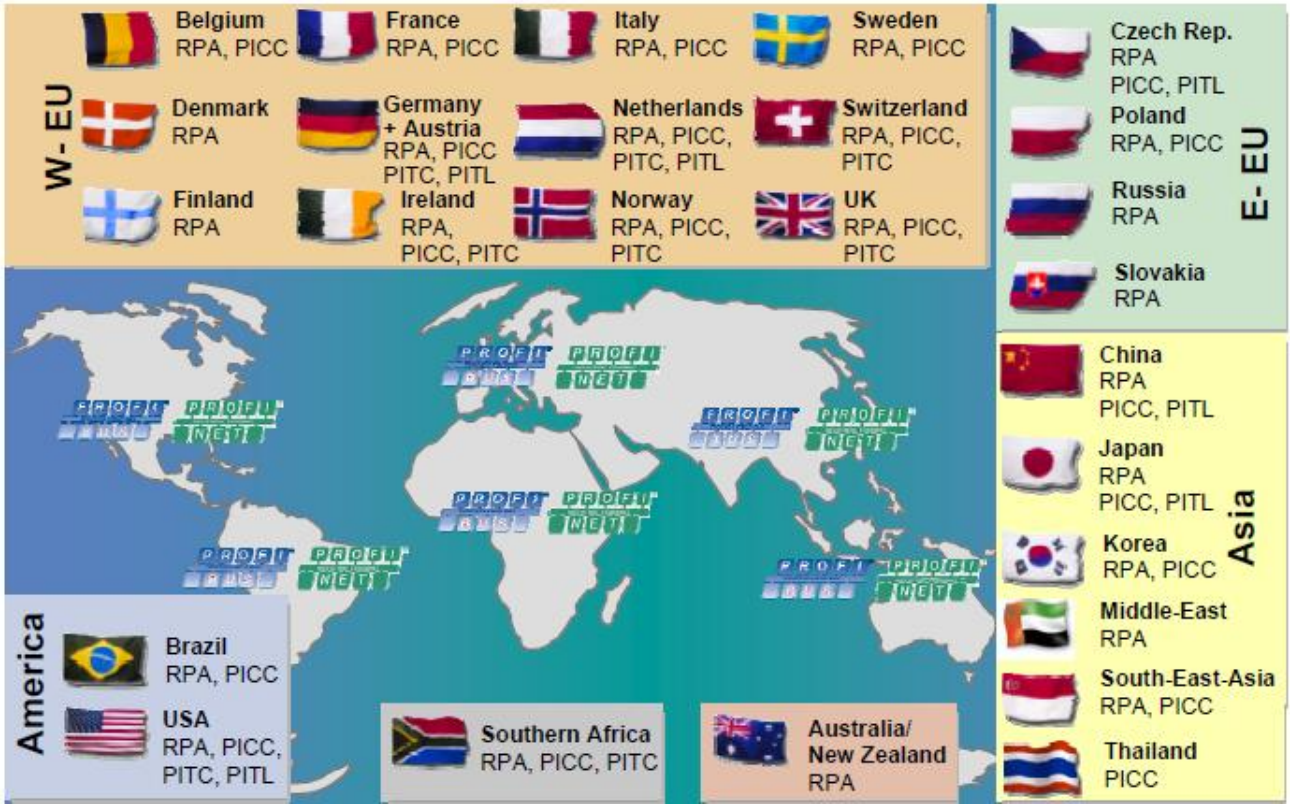
Organisational milestones to market leadership

2007 1 Million PROFINET devices installed
2006 Founding of PI Training Centres
2004 PROFINET Marketing Working Group in Japan and USA
2002 First PROFINET Competence Center and Test Laboratory

With 1.400 members around the world, PROFIBUS & PROFINET International (PI) is the world's largest organisation for industrial communication. The PI Support Center (PISC) in Karlsruhe, Germany, is the international point of contact and the communication center.

PI support

- 25 Regional PI Associations (RPA)
- 36 PI Competence Centers (PICC) in 21 countries
- 15 PI Training Centers (PITC) in 8 countries
- 10 PI Test Laboratories (PITL) for certification tests



Worldwide support of PI

1 What is PROFINET

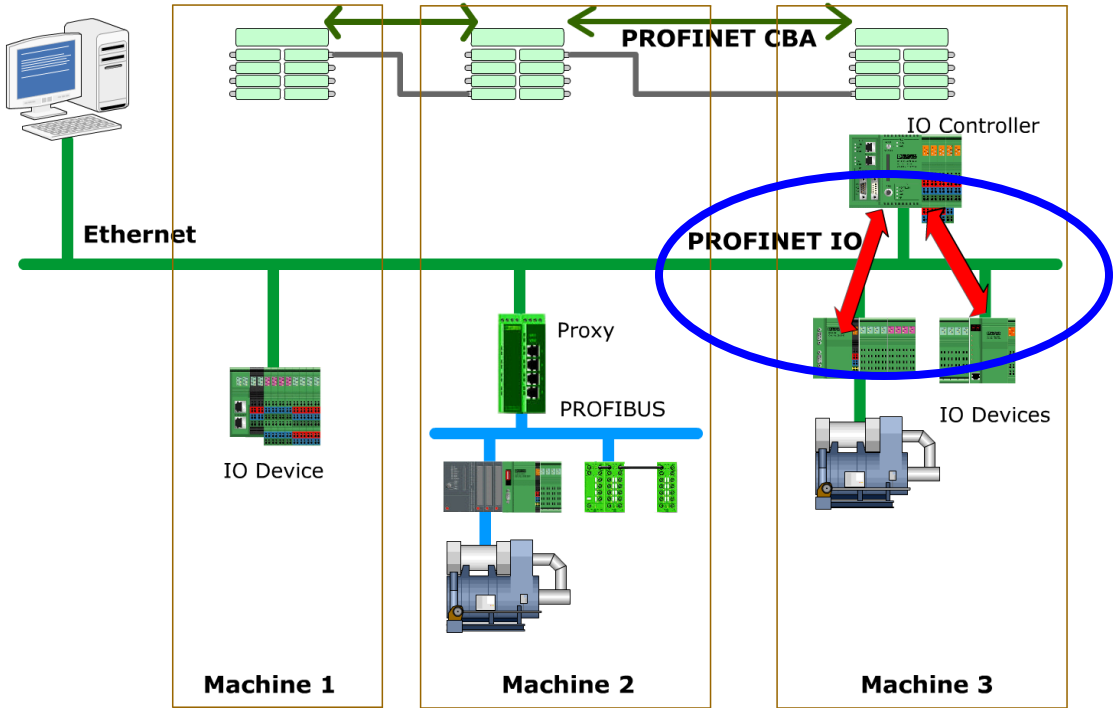
1.1 Function Classes

1.2 Communication and Security

Content of the chapter „What is PROFINET“

PROFINET IO

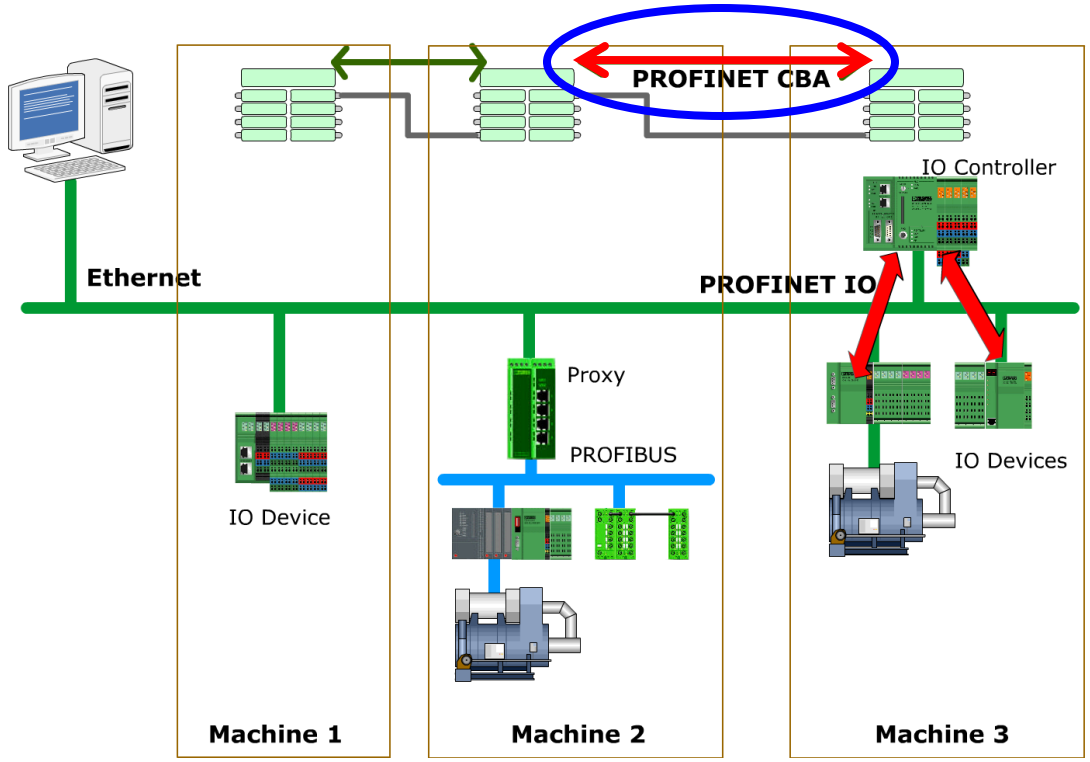
In PROFINET, we can distinguish two function classes that are independent of each other, PROFINET IO and PROFINET CBA (Component Based Automation). PROFINET IO is concerned with the distributed I/O (Input/Output).



- The distributed field devices are connected through the PROFINET IO.
- In PROFINET IO the process data from the field devices is transmitted periodically into the control system – similar to PROFIBUS
- PROFINET IO uses three channels with different time characteristics.

PROFINET CBA

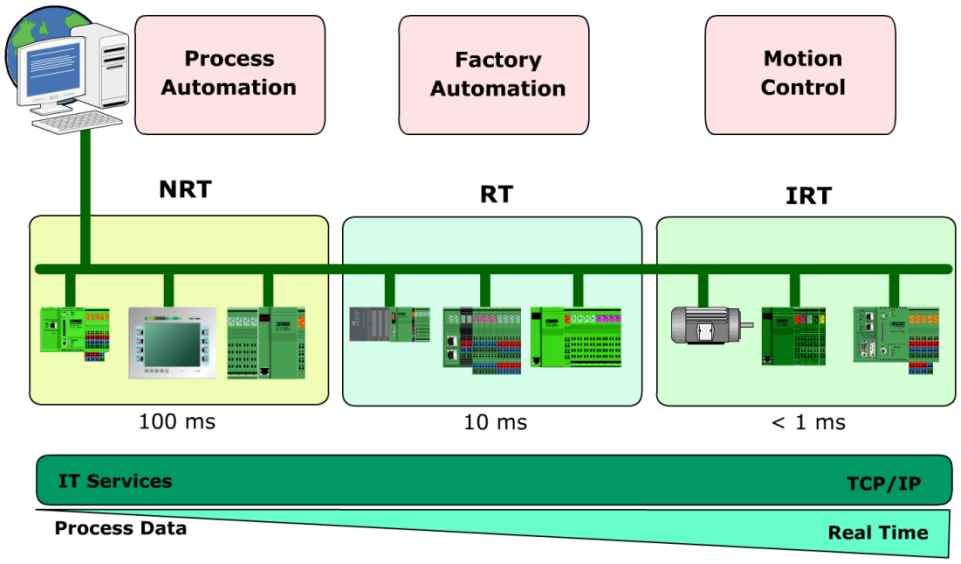
PROFINET CBA is designed for distributed industrial automation applications and is built on the standard DCOM (Distributed Component Object Model) and RPC (Remote Procedure Call) technologies.



- DCOM is an object oriented mechanism that structures how a Client can locate, request and receive data from a Server.
- DCOM was originally developed by Microsoft.
- The DCOM objects, which are modified for the PROFINET CBA, are called technological components.

Communication Concept

PROFINET uses three channels for communication with different performance classes depending on the purpose.



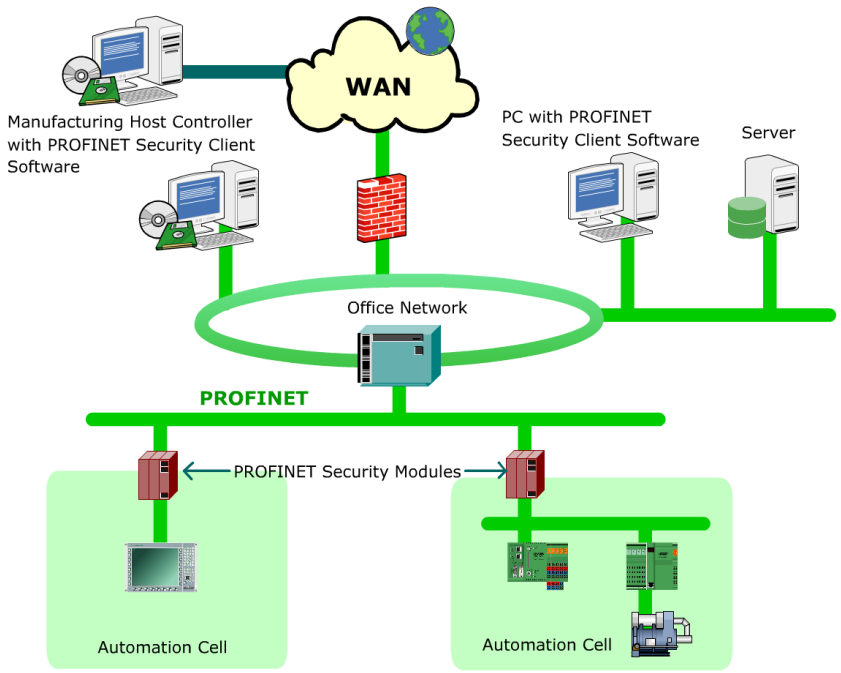
NRT (Non Real Time) for non-time-critical processes with use of standard TCP/IP and UDP/IP when transmitting data packets.

RT (Real Time) for optimized data exchange performance with high-speed data transfer, when standard TCP/IP or UDP/IP cannot satisfy this requirement.

IRT (Isochronous Real Time) for clock-synchronized communication. Drive applications, like Motion Control, need to be satisfied immediately. The IRT can do this with a response time of less than 1 millisecond.

Security Concept

The core of the PROFINET Security Concept focuses on secure networks in separated security zones, so-called cells.

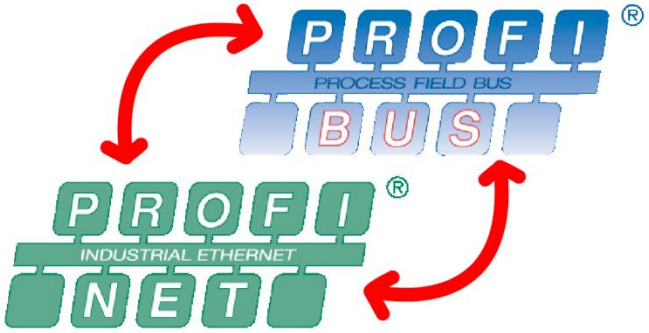


Each cell can be connected to the backbone through an entry point and are protected by using special security network components, such as switches or other security appliances.

These components check the data being transmitted for authorization and integrity. If you want to access the secure automation devices, you can use special security client software.

The data traffic between secure cells or between client software and the cell can also be encrypted using conventional encrypting algorithms.

2 PROFINET vs. PROFIBUS



Content of the chapter „PROFINET vs. PROFIBUS“

Advantages of PROFINET (Time and Network)

- **High-speed operation:** The real time communication channel provides high-speed process data exchange by bypassing the time required to process the TCP/IP stack. The time-critical process data can then be exchanged by using RT or IRT protocols. Both time-critical and time-uncritical data can be set up by one installation on one medium.

- **Simple network structure:** The construction of an Ethernet standard is very simple and easy to implement. Furthermore, this standard is used widely in the office sector, thereby ensuring compatibility.

- **Simple extensible network:** In PROFINET IO for example, you can add the new field devices by using the device library which allows easy extensibility. This kind of approach lets you extend your network by adding or modifying the functions you wish.

- **One line data transfer:** Using Ethernet means that you can use just one cable to transmit all kinds of data. This, in turn, reduces costs. Switches allow you to access your desired devices.

Advantages of PROFINET (Others)

- **Seamless integration with fieldbus systems:** For those who already have a fieldbus system, e.g. PROFIBUS/INTERBUS/CAN, installed in their factory, PROFINET offers the so-called Proxy that connects PROFINET and other fieldbus systems. The investment made in already installed fieldbuses is thus protected.

- **Individual settings:** The field devices can be set individually, e.g., you can set up different field devices with different cycle times on the same network. This lets you have cyclic data at different times depending on your requirements.

- **Cost-effective technology:** In comparison with other network systems e.g. ATM or Frame Relay, the set up cost and performance of Ethernet is much more cost-effective than these others. Moreover, Ethernet will give each user the same speed regardless of where the application is actually hosted.

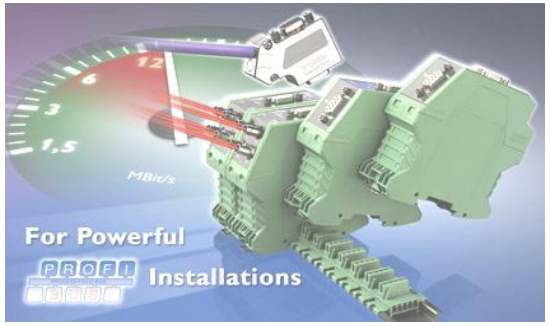
- **IT Software:** For accessing process data or for diagnostic purpose, you can use the conventional software of the IT world, such as web browsers, like Internet Explorer, Firefox, Opera, etc., or office applications, like Microsoft Office.

Comparison I

FEATURES	PROFIBUS DP	PROFINET IO
	Master Class 1	IO Controller
	Master Class 2	IO Supervisor
	Slave	IO Device
Wired transmission technology	PROFIBUS over copper or fiber-optic cable	Industrial Ethernet over copper or fiber-optic cable
Wireless transmission technology	Infrared transmission is possible	Industrial WLAN (Wireless Local Area Network) is possible
Data exchange	On request	Once the IO device is parameterized, it can work by itself. Data can be exchanged cyclically or acyclically (on request)
Data transfer rate	Max. 12 Mbit/s	100 Mbit/s with full duplex
Data channels	One exactly defined data channel between Master and Slave	Several data channels between Controller/Supervisor and Device

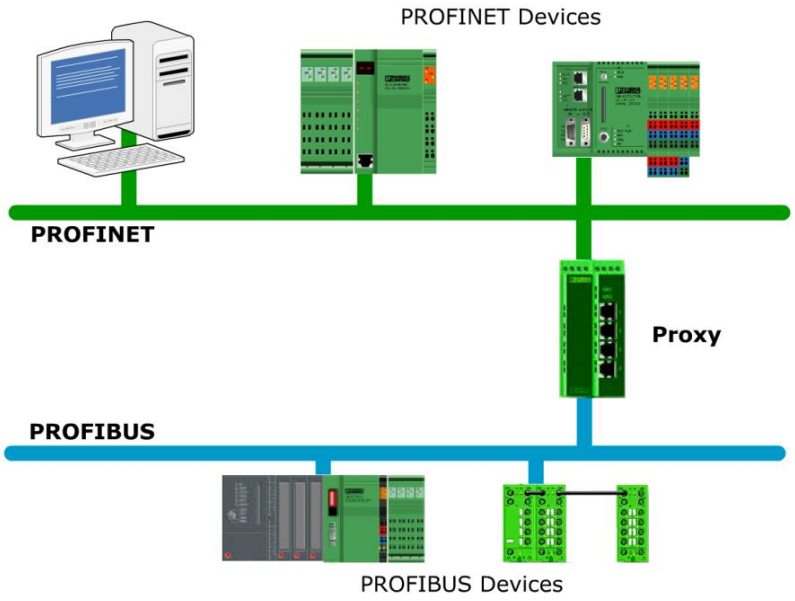
Comparison II

FEATURES	PROFIBUS DP	PROFINET IO
Number of the devices	126 devices maximum	Arbitrary, depends on network
IT services	Not possible	Can be integrated
Device description	Keyword based	XML based with schema definition
Data priority	Same priority	Different priorities can be set
Access of a field device	Read only from several users	Read and write from several users possible
Topology	Standard: star and tree Possible: bus and ring	Standard: line Possible: tree and ring



Integration with PROFIBUS

PROFINET uses a so-called proxy in order to integrate an existing fieldbus system, such as PROFIBUS, INTERBUS, ASI, etc., to the PROFINET system. With this architecture, you will have a hybrid system consisting of fieldbus and Ethernet-based subsystems.



The main reasons for developing the new technology are to reduce the cost and improve the existing technique. PROFINET accomplishes this in every way.

It uses standard technology which is simple to implement and cost-effective, and the new concept to handle industrial automation is easier than before.

A seamlessly continuous technological transition from a fieldbus system to PROFINET is therefore possible.

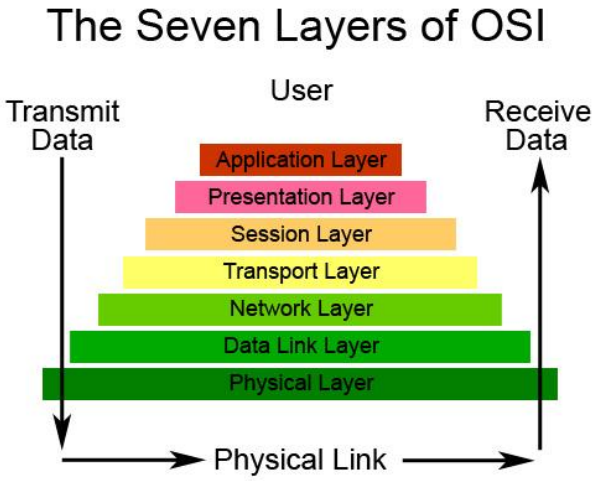
ISO/OSI Reference Model

3.1 7-Layer Model

3.1.1 Overview

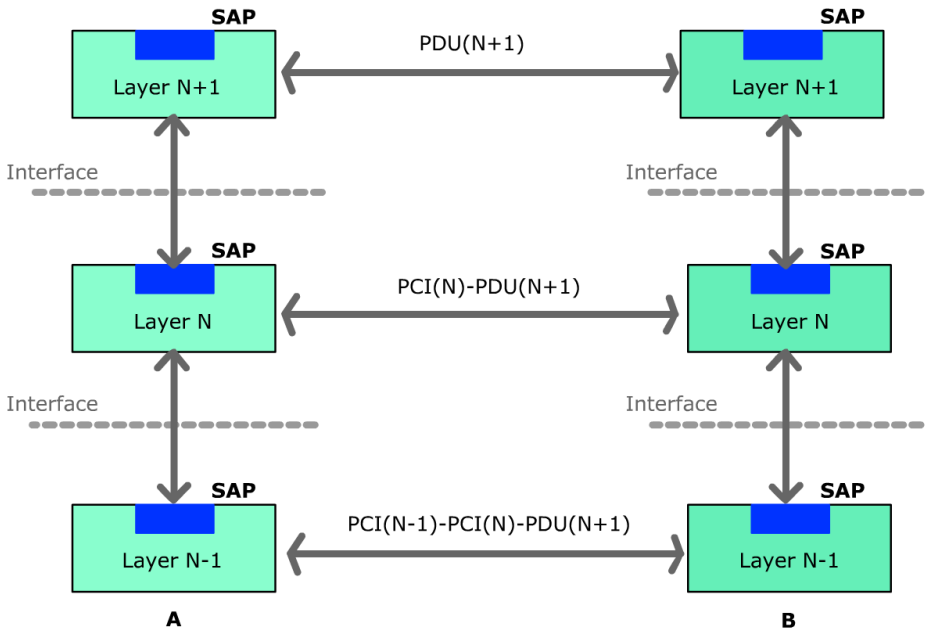
3.1.2 PROFINET in the reference model

3.2 Communication Path



Layer Communication

The ISO/OSI reference model (International Standardization Organization and Open System Interconnection) is the layer model which one can refer to as a reference for data communication.



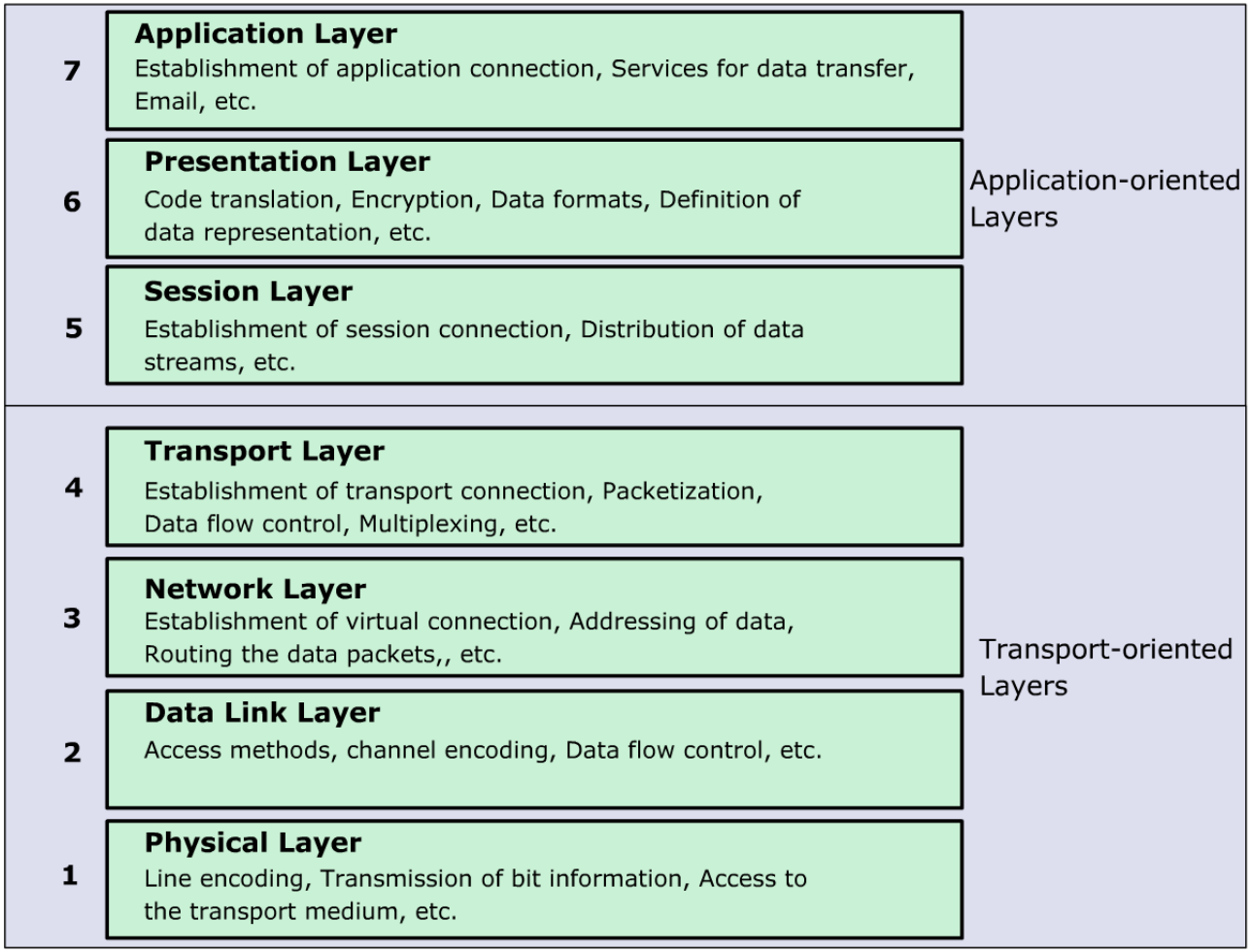
PDU – Protocol Data Unit
PCI – Protocol Control Information

According to the ISO/OSI reference model, communication operations can be divided into seven layers.

Every layer has a specified assignment, which can be passed to the next upper or lower layer, according to the task, as a service.

Communication between two layers is carried out by using the specific interface **SAP** (Service Access Point) and protocols **PDU** and **PCI**.

Characteristics of the 7 Layers



PROFINET in Layer 1 and 2

ISO/OSI Layer	Integration on PROFINET
Layer 1: Physical Layer On this layer, the single bits will be transmitted over the cable. The electrical and mechanical properties of the transmitting medium are controlled for the purpose of making sure that all of the bits arrive at the receiver completely. Electrical properties are, for example, how much volt is “1” and how long is a bit. Mechanical properties are, for example, cable types, pin assignment for the connectors, or direction of the transmission (uni- or bidirectional).	PROFINET uses the Fast Ethernet with 100 Mbit/s according to the IEEE 802.3. The Fast Ethernet works in the full-duplex mode (bidirectional). Cable types are: - **10BaseTX:** 10 Mbit/s in copper cable (Twisted Pair). - **10BaseFX:** 10 Mbit/s in fiber optic cable. - **100BaseTX:** 100 Mbit/s in copper cable (TP). - **100BaseFX:** 100 Mbit/s in fiber optic cable.
Layer 2: Data Link Layer This layer delivers the error-free data transmission between two users to layer 3. The incoming data are split up into frames. The receiver can check whether the transmission was correct or not. This layer manages the collision-free access of the transmission medium. The MAC (Medium Access Control) is defined for the purpose of unique identification of the device. This MAC address will be given by the device manufacturer.	The **PROFIBUS (PROFIBUS/PROFINET International) (PI)** offers the device manufacturers the manufacturer identifier part of the MAC address. This part is also called OUI (Organizationally Unique Identifier). The device manufacturers can purchase this part from the PNO and then add their own consecutive numbering part.

PROFINET in Layer 3 and 4

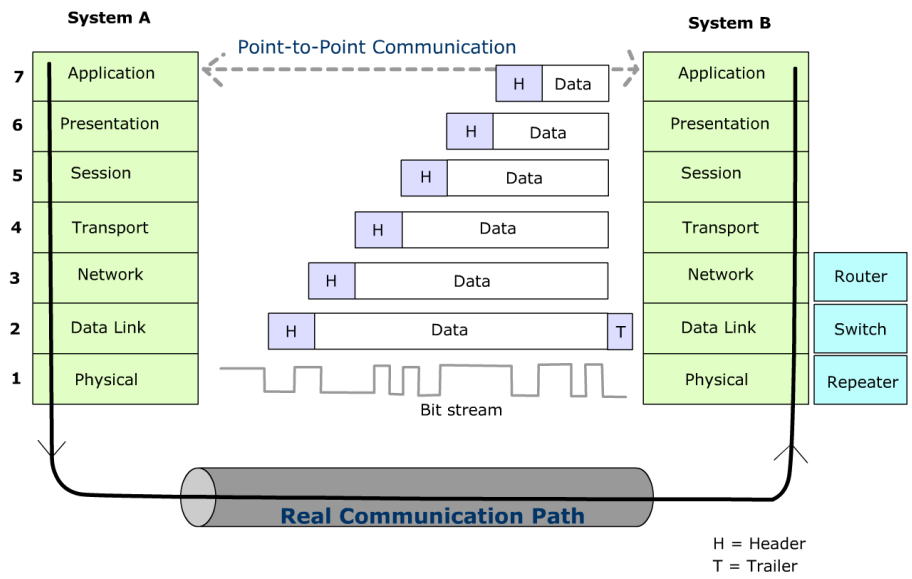
ISO/OSI Layer	Integration on PROFINET
Layer 3: Network Layer This layer enables communication between users over long distances and different network types. The Network Layer transmits the data packets by using their IP address (Internet Protocol). A suitable routing is selected. The packets are temporarily saved on subnodes. These subnodes look at the current routing table and find the most suitable route. They then forward the packets along the route selected.	It is necessary to give the PROFINET devices the network addresses by a suitable engineering tool. Within one network, an IP address must be unique. We can access the appropriate PROFINET device by using its IP address. The packets can be transmitted to this device correctly.
Layer 4: Transport Layer This layer has the task of ensuring the communication connection. The data packets may be broken down into small pieces (fragmentation) and assembled again on the receiver's side (defragmentation). If there are possible errors, they will be corrected here. The most famous protocol for data flow control is TCP (Transmission Control Protocol). TCP is connection-oriented, i.e., the connection must be established by using a preliminary protocol before the data can be sent. Another protocol is UDP (User Datagram Protocol). UDP is connectionless, i.e., the connection will not be observed.	PROFINET CBA uses the TCP protocol. In PROFINET IO, UDP is implemented for the process data exchange. PROFINET applications use ports 34962 to 34964 for communication.

PROFINET in Layer 5, 6 and 7

ISO/OSI Layer	Integration on PROFINET
Layer 5: Session Layer In this layer, services like dialog control for supervision of data flow direction or recovery points will be actualized. If a connection is interrupted, it can be recovered at the last point, without repeating from the beginning.	No usage.
Layer 6: Presentation Layer The data will be translated into the common format on this layer. On the sender's side, the data will be coded and compressed. On the receiver's side, the data will be then decoded and decompressed. Then they will be transmitted to the respective application.	No usage.
Layer 7: Application Layer The specific interfaces will be defined on this layer. These interfaces enable communication between applications. Communication between different protocols will be actualized by using the so-called gateways or proxies.	The following scenario is conceivable: A fieldbus system PROFIBUS is installed. You want to have PROFINET and then integrate PROFIBUS devices to the PROFINET. Thanks to the defined interface in layer 7 and the use of a proxy, you can actualize this relatively easily. Data exchange between PROFIBUS and PROFINET devices is therefore possible seamlessly.

Communication Path

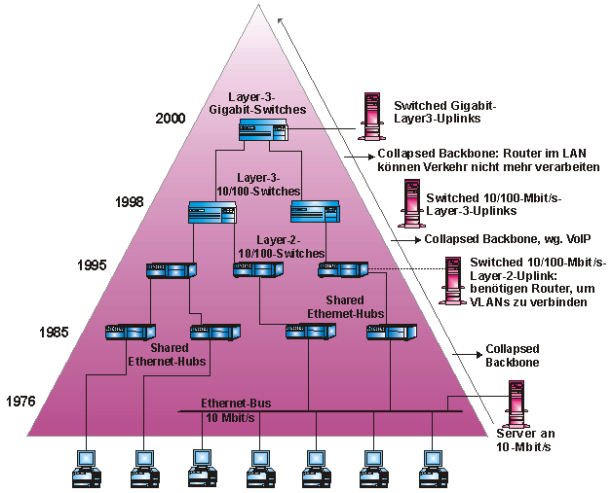
In the diagram below, communication between two systems (A and B) occurs in a horizontal direction. Single bits are transmitted from system **A** to **B** over a physical medium in layer 1. However, communication within system **A** (here, the sender), happens in a vertical direction.



- The data packets on layer 7 will have a layer 7-header added are then passed to layer 6.
- On layer 6, the data packets will have a layer 6-header added. They are then passed to layer 5, and so on.
- When they reach layer 1, the data packets are transmitted.

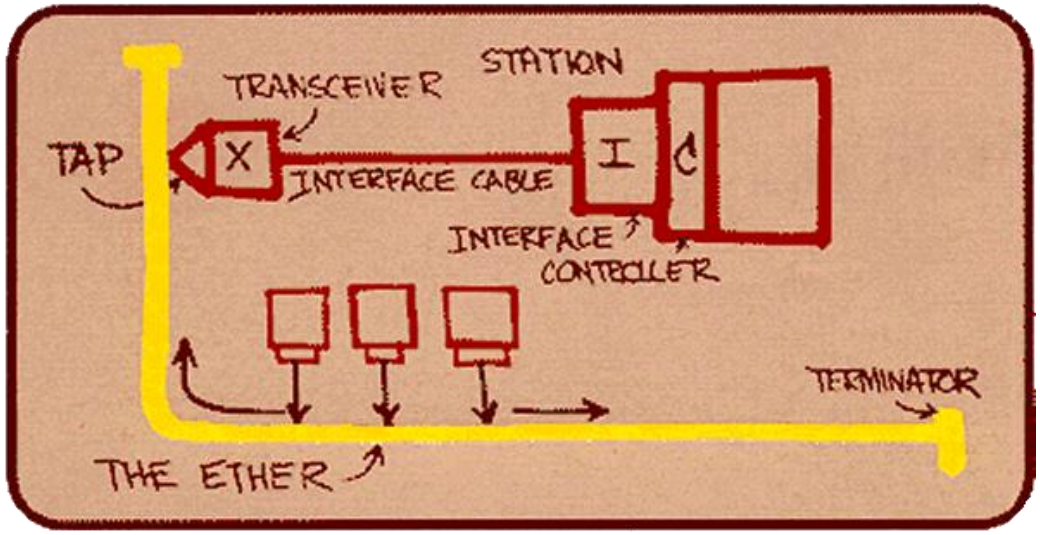
Only the essential layers will participate in the communication process. If there is no use of the specified layer, the header of that layer will not be added.

4 Ethernet Basics



Short History

Ethernet is a kind of computer network that is a part of the most commonly installed local networks in the world. The most well known examples are **LAN** (Local Area Network) and **WLAN** (Wireless Local Area Network).

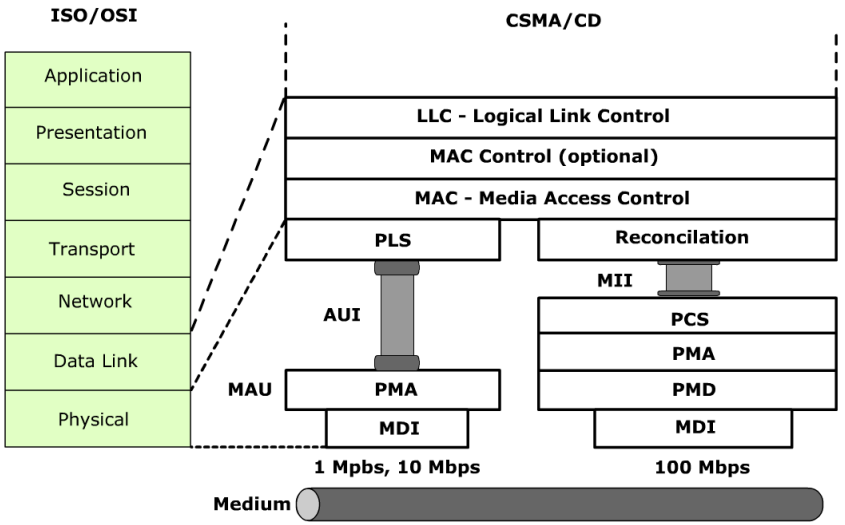


The history of the Ethernet began at the beginning of the seventies. The US Company **XEROX** introduced the innovative concept of the Ethernet.

On February 1980, the working group 802 of the American **IEEE** (Institute of Electrical and Electronics Engineers) officially defined the first standard for LAN communication.

Ethernet Layer 1 and 2

The Ethernet standard is made up of the following components:



AUI - Attachment Unit Interface
MDI - Medium Dependent Interface
MII - Medium Independent Interface
MAU - Medium Attachment Unit

PLS - Physical Layer Signaling
PMA - Physical Medium Attachment
PMD - Physical Medium Dependent
PCS - Physical Coding Sublayer

MAC (Media Access Control)

PLS (Physical Layer Signaling)

AUI (Attachment Unit Interface)

MAU (Medium Attachment Unit)

PMA (Physical Medium Attachment)

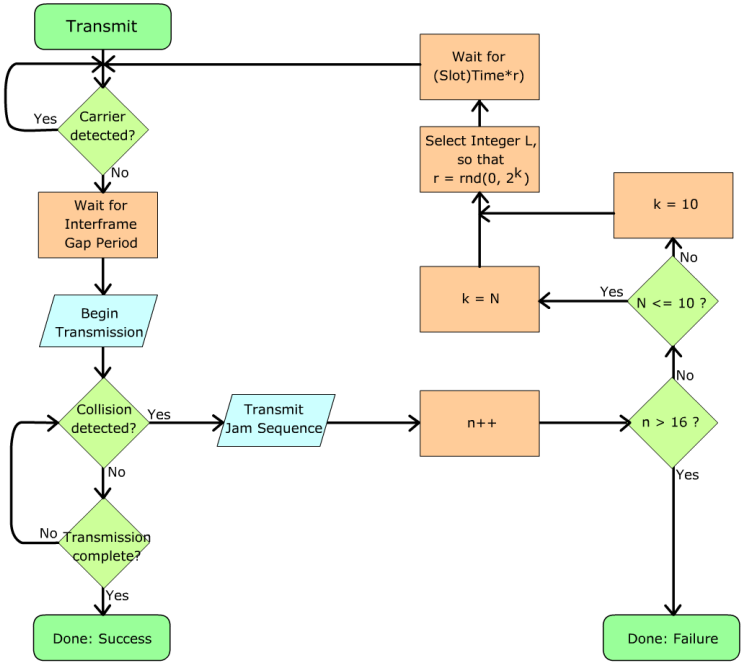
MDI (Medium Dependent Interface)

Ethernet uses **CSMA/CD** network access methods to control access to the network. The devices attached to the network cable listen to the transmission medium and begin to transmit data as soon as the medium is available. If the medium is in use, the devices wait before transmitting.

CSMA/CD

The access method **CSMA/CD** consists of three components:

- **CS** (Carrier Sense): The devices check whether the medium is available.
- **MA** (Multiple Access): MA indicates that many devices can connect to or share the same network. If the medium is available, each device can begin to transmit the data.



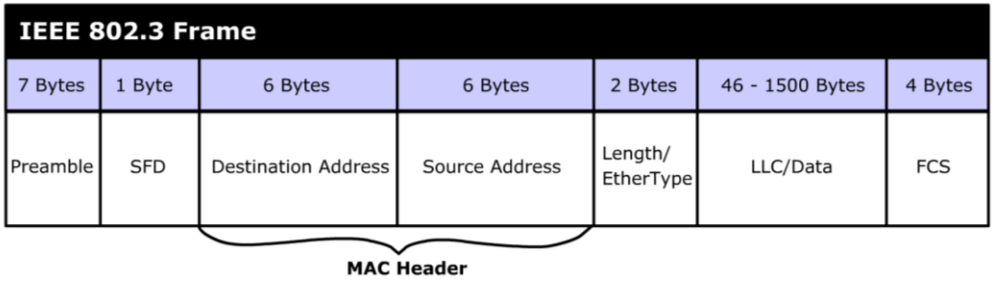
- **CD** (Collision Detection):

  If more than one device starts to transmit data at the same time, this causes a data collision. If a collision occurs, the devices abort their transmission attempts, wait for a random time and then retransmit the data.

  This approach is called truncated binary exponential backoff

Frame Structure

A standard IEEE 802.3 Ethernet frame consists of following components:

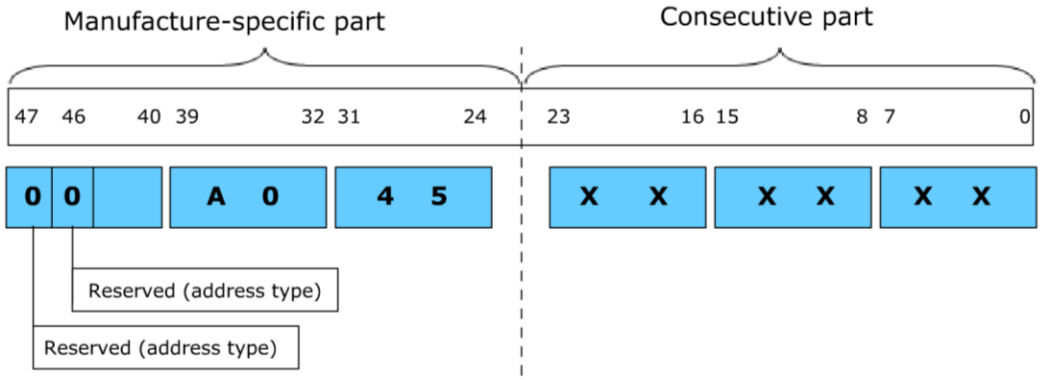


- Preamble: The preamble consists of 7 bytes of alternating 1 and 0.
- Start Frame Delimiter (SFD): The SFD consists of 10101011.
- Destination Address: The Destination Address consists of the **MAC** address of the receiver.
- Source Address: The source address consists of the **MAC** address of the sender.
- Length/EtherType: This field consists of the length or the EtherType of the following data field
- Data: The data filed consists of the user data that can be 48 to 1500 bytes.
- Frame Check Sequence (FCS): This field consists of the checksum of the transmitting data,

MAC Address

The **MAC** (Media Access Control) address is the hardware address of the devices that participate in the network.

A MAC address consists of two parts, each 3 bytes long, the manufacturer-specific one and the consecutive numbering one.

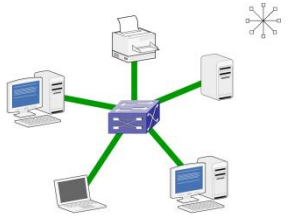


The example shows a MAC address **00.A0.45.XX.XX.XX** where 00.A0.45 is a manufacturer-specific part representing the company Phoenix Contact.

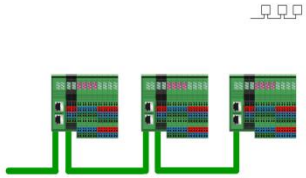
The manufacturer-specific part of a MAC address can be obtained from the IEEE for an administration fee and is called the **OUI** (Organizationally Unique Identifier). The consecutive part can be obtained from the manufacturer. Each manufacturer can register up to 16,777,214 devices.

Network Topologies

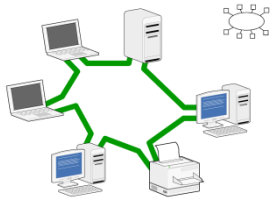
- Star: In a star topology a switch is involved. The devices of the network are connected to a central signal distributor individually. The star is used in areas with high device density and short distances



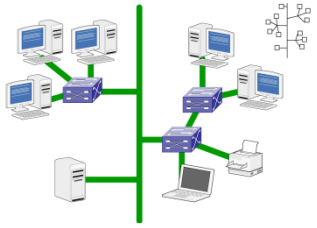
- Line: All of the network devices are connected in series as a bus. For the connection between network devices there is a link device (switch). Line topology is used preferentially to connect distant systems.



- Ring: If you connect the two ends of a line topology, you will have a ring topology. Ring topologies are redundant, i.e., this kind of topology increases the failure safety of the network.



- Tree: If you connect several star topologies together, you will have a tree topology. In the tree, there is a possibility of combining fiber optic and copper cables together. This topology is used when a complex system is divided into several system segments and they need to be interconnected.

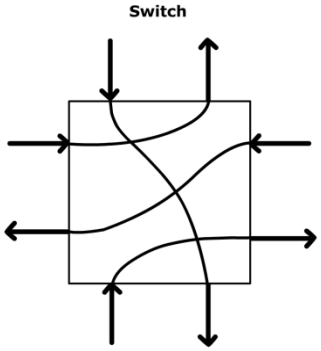


Switch

In PROFINET, industrial Ethernet switches are used to create a simple gateway between network devices. A network in which every device is assigned exactly to one port of a switch is called Switched Ethernet.

Two operating modes of switches:

- Cut-Through Switches: Forward a data packet immediately after receiving the 6 bytes long destination address. The delay time of the switch is between 5 to 60 µs.
- Store-and-Forward Switches: examine every data packet. The delay time of a data packet depends on its frame length.



Properties of switches:

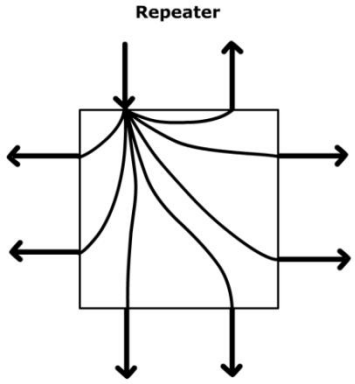
- Blocking or Wire speed (non-blocking): If a switch can serve all services at the same time, then it is non-blocking.
- Managed or Unmanaged: If a switch just uses the address table for transmitting the data packets, we call it "unmanaged".

Hub or Repeater

An Ethernet hub is a device that is used to connect two or more networks or devices together. The multiple twisted pair and fiber optic Ethernet devices can also be connected together. This lets them act as a single segment. Hubs work at layer 1 (the physical layer) of the ISO/OSI reference model.

Characteristics of hubs:

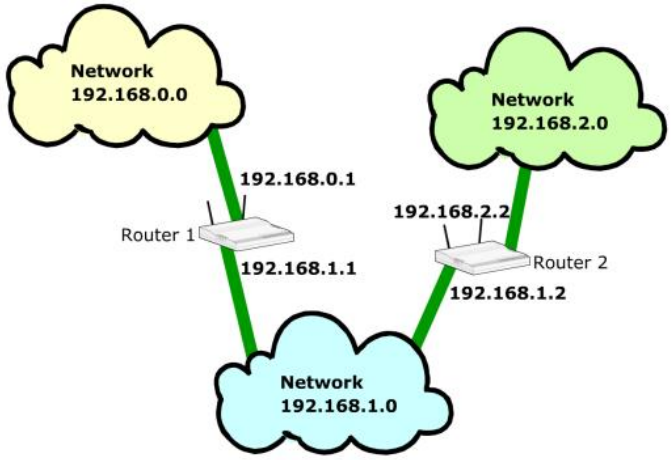
- With hubs, you can pass just one data packet at a time with a speed up to 10/100 Mbps for a dual-speed hub.
- The hubs do not know which station is connected to which port.
- Hubs cannot learn this information.



Ethernet hubs work as repeater for the network, too. Meaning that the signal will be amplified and regenerated for a long distance. They are also responsible for forwarding a jam signal to all ports if they detect a collision.

Router, Signal Coding, VLAN

A router is a computer-networking device that is used to interconnect two or more separate subnets together.



A router will look at the IP address of the data packet and determine, with the help of a subnetwork, whether it is within the same network or not. If not, it will forward the data packet to the appropriate network.

Routers can increase the security of the network. An automation network can be protected by strict and individually adapted access rules.

Signal coding: The signal coding for Ethernet depends on the transfer rate of that Ethernet. In the 10 Mbps Ethernet Standard from IEEE 802.3, the Manchester Coding is used. In Fast Ethernet, the FDDI technique is used.

VLAN: A **VLAN** (Virtual Local Area Network) is a method of creating a closed and secure network.

5 Cables and Connectors

5.1 Cables

5.2 Connectors

5.3 Wireless Systems

Network Installation

The network components for use in industrial automation must be designed to withstand the extreme conditions in the production area.

Office Area	Automation Area
Fixed basic installation in a building	Largely system-related cabling
Laid under raised floor	System-related cable routing
Variable device connection at workplace	Connection points are seldom changed
Pre-fabricated device connection cable	Field-preparable device connection
Tree network topology	Quit often: line and ring network topology
Large data packets (e.g. images)	Small data packets (e.g. process data)
Medium network availability	Very high network availability
Moderate temperature (0 to +50 °C)	Extreme temperature (-20 to +70 °C)
No moisture	Moisture possible
Minimal vibrations	Vibrating machines
Low EMC	High EMC
Low mechanical danger	High mechanical danger
Low chemical danger	High chemical danger, e.g. oil or aggressive atmospheres

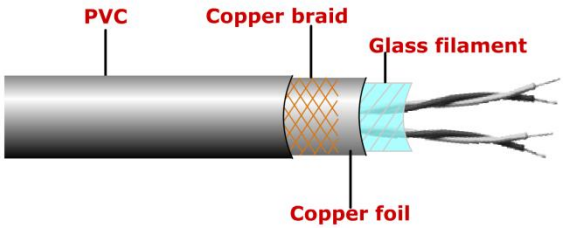
Extreme conditions include, e.g., dust, Electromagnetic Compatibility (EMC), temperature, moisture, vibration, etc.

The installation of a network in an industrial area distinguishes between inside (IP20) and outside (IP65/67) the control cabinet.

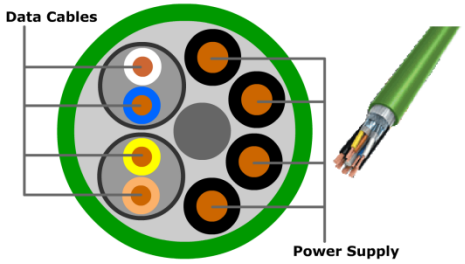
The definitions and descriptions of the industry-standard for Fast Ethernet can be found in the PROFINET Installation Guidelines" from PNO that are based on IEC 11801.

Twisted Pair Cables

Twisted pair cables (from copper): Nowadays, a balanced cable is used. It is also called a symmetrical cable.



Symmetrical because the potential difference to the reference ground is 0 V in an ideal case. To transmit a signal, two wires are twisted together as a signal pair.

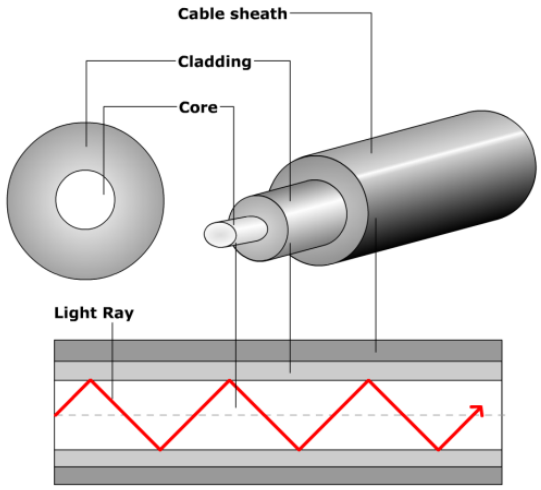


For a full duplex, you need four wires. Therefore, an industrial network cable has at least four wires (quad cable).

In practice, 100BASE-TX cable is used for Fast Ethernet with 4 wires. The cable is defined as **STP** (Shielded Twisted Pair) meaning that two shielded copper wires are twisted into a pair. The cables fulfill the requirements of **CAT5** with cable class D of IEC 11801. CAT5 is for data transmission up to 100 MHz

Fiber Optic Cables

Fiber optic cables: A glass fiber optic cable is comprised of a core and a shield. The core is a highly sterile, extremely thin silica or quartz glass thread which is shielded by glass with low optical density.



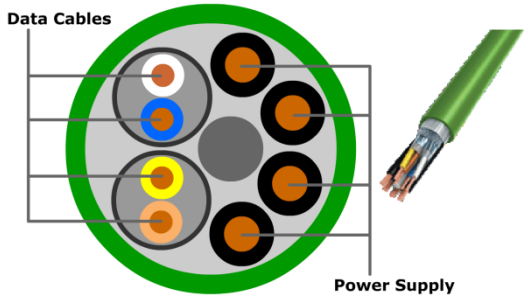
The light pulses are reflected totally and forwarded along the core. In order for data to be sent, the data signals are converted into light pulses by using LEDs or laser diodes.

There are two modes of fiber optic cables, single mode and multimode. PROFINET can be operated with both of them.

Fast Ethernet 100BASE-FX uses two fiber optic cables. The optical interfaces conform to the specifications of ISO/IEC 9314-3 (multimode) and ISO/IEC 9314-4 (single mode). For multimode, the maximum segment length is two kilometers, and for single mode, 14 kilometers.

Hybrid Cables

Hybrid Cable: In the production area, different devices with different cable systems need to be supplied. A hybrid cabling structure is therefore very useful, apart from the process data. The voltage is 24 V. Hybrid cables contain wires (optical or copper-based) for both data signal and transmission of energy.



- For optical cables, two optical wires for data transmission and four copper wires for energy transmission are used.
- For copper-based cables, four copper wires for data transmission and four copper wires for energy transmission are used.

Connectors for copper-based cables

There are two connector types for copper-based cables used in PROFINET:
→ RJ45 and M12.

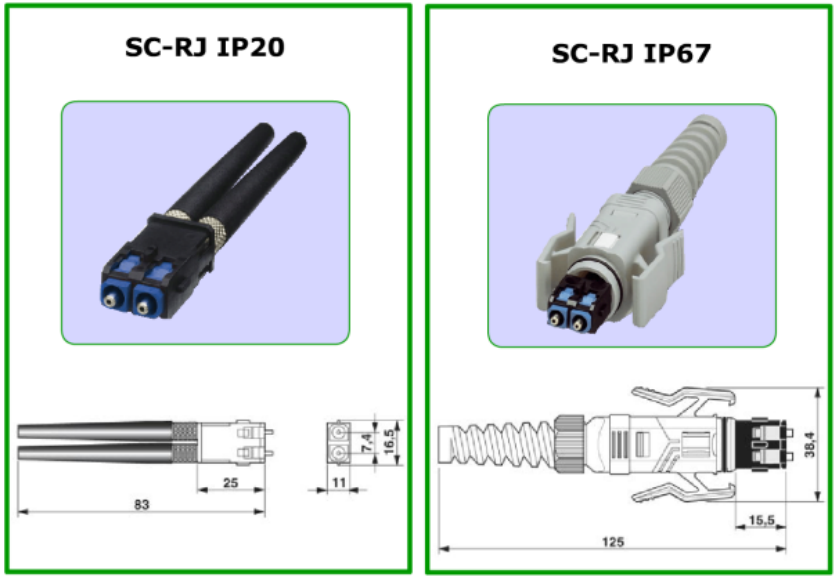
For installation inside a control cabinet, we can use the RJ45 connector with IP20 variant that is compliant with the connectors used in office areas.

For installation outside a control cabinet we use the RJ45 connector with IP65 or IP67 variant, or M12. The hybrid connectors are RJ45 connectors with IP67 variant. The entire plug is fully touch-protected.

Signal	Name	Wire color (quad cable)	Wire color (EN 50173 T568B)	Contact Assignment	
				RJ45	M12
TD+	Transmission Data +	Yellow	Orange/White	1	1
TD-	Transmission Data -	Orange	Orange	2	3
RD+	Receive Data +	White	Green/White	3	2
RD-	Receive Data -	Blue	Green	6	4

Connectors for Fiber Optic Cables

For connecting fiber optic cables in PROFINET, SC-RJ connector technology is used. Key features of the SC-RJ technology are small dimensions, high packing density and high reproducible connection quality



For installation inside a control cabinet, the SC-RJ connector with IP20 variant is used. Outside a control cabinet the IP65/IP67 variant is used.

The SC meets EN recommendations (EN 50377-6). This connector is suitable for both multimode and single mode fibers. In the near future, the M12 connectors will be used, too.

Wireless PROFINET

Wireless systems are becoming increasingly common. The biggest advantages are savings in cabling costs. Due to their mobility and flexibility, you can install devices where the use of electric cables is limitated.

PROFINET field devices can operate with different radio technologies for different application areas, with specific parameters regarding transfer rates, range, number of nodes, and so on.

Thus, the profiles are specified for each technology. They specify how to integrate into PROFINET, which topologies and performance values can be achieved, and the conditions for security requirements.

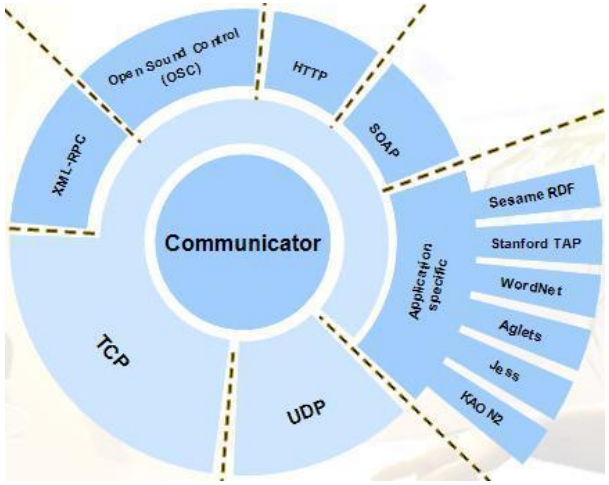
PROFINET supports **WLAN** (Wireless Local Area Network) standard IEEE 802.11b/g, **Bluetooth** standard IEEE 802.15.1 and **ZigBee** standard IEEE 802.15.4. All of these use the 2.4 GHz frequency band in the ISM (Industrial, Scientific, and Medical Band) frequency range that can be used free of charge and without license.

6 Internet Protocol Family

6.1 Internet Protocol

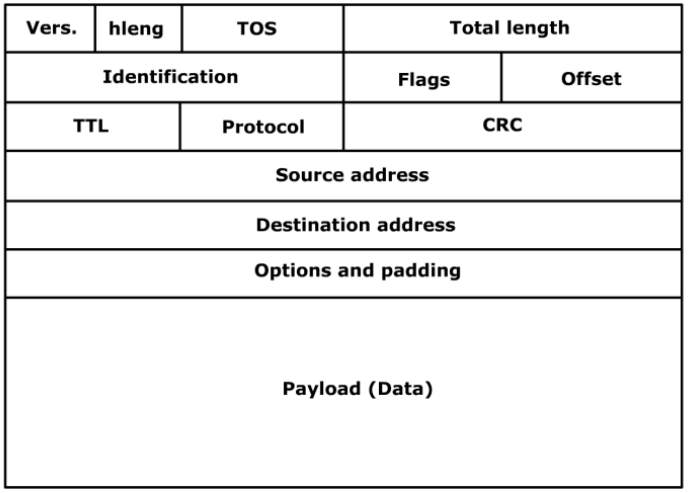
6.2 Transmission Protocols

6.3 Other useful protocols



IPv4 Internet Protocol

The Internet Protocol (IP) is probably the most used protocol in the IT world. The current version of this protocol is 4 (IPv4). IP provides a connectionless transport service transmitting and receiving datagrams.



A datagram consists of a header and a data portion (payload).

The term datagram or packet is used to describe a chunk of IP data.

Each IP datagram contains a specific set of fields in a specific order so that the reader knows how to decode and read the stream of data received.

Internet Protocol version 6 (IPv6) will become more common in the near future because it allows more network addresses to be assigned.

Classes of IP addresses

IPv4 uses a 32-bit IP address for addressing the field devices, and is denoted with decimal figures. An IP address consists of two parts, Host ID and Network ID.

	First bits	Network ID	Host ID	Address	Networks	Host
Class A	0	7 bits	24 bits	0.0.0.0 - 127.255.255.255	126	16777216
Class B	10	14 bits	16 bits	128.0.0.0 - 191.255.255.255	16384	65536
Class C	110	21 bits	8 bits	192.0.0.0 - 223.255.255.255	2097152	256
Class D	1110	28 bits, multicast identifier		224.0.0.0 - 239.255.255.255		
Class E	11110	27 bits, reserved		240.0.0.0 - 247.255.255.255		

IP addresses can be divided into five classes (A, B, C, D, and E), but only A, B and C are used in practice. The first bits represent the network class followed by the network address and the user address

IP Address/Network	Address	Subnet Mask	Addresses in the network	Broadcast
192.168.0.1	192.168.0.1	255.255.255.0	192.168.0.1 to 192.168.0.254	192.168.0.255

Example of an IP address class C

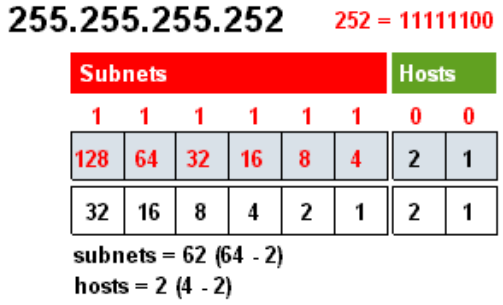
Subnet Mask

The subnet mask indicates how many network devices can connect to this IP address. In binary form, the ones in the subnet mask indicate the subnet number part and the zeros indicate the host part.

Example with IP address class C, 192.168.1.1 and subnet mask 255.255.255.0

	Network	Host
Decimal	255.255.255.	0.
Binary	11111111.11111111.11111111.	00000000

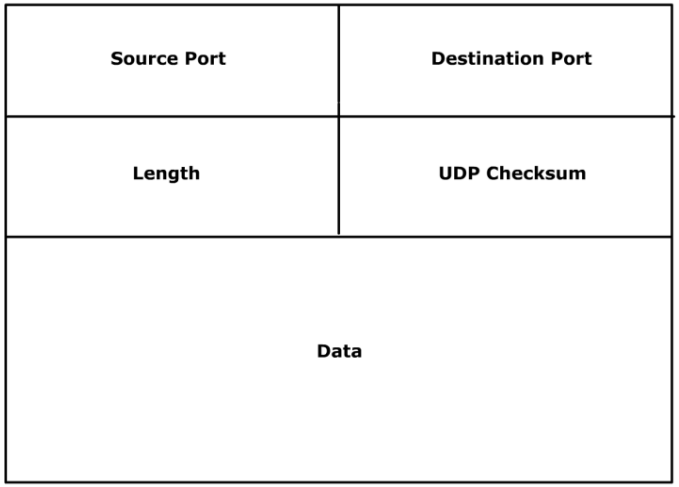
From the example, you can connect 256 network devices to this network, and they will have IP addresses from 192.168.1.0 to 192.168.1.255. But the first (192.168.1.0) and last (192.168.1.255) addresses are reserved for special assignments.



Within an IP network, you can use the subnet mask to extend your network addresses e.g. for 255.255.255.0 as a subnet mask.

User Datagram Protocol

The **UDP** (User Datagram Protocol) is used to provide a connectionless and unreliable data transport service. UDP will not inform the sender whether the data packet was received or lost. Using the UDP, we can have problems with data integrity because the data packet can be dropped, mis-sequenced or doubled.

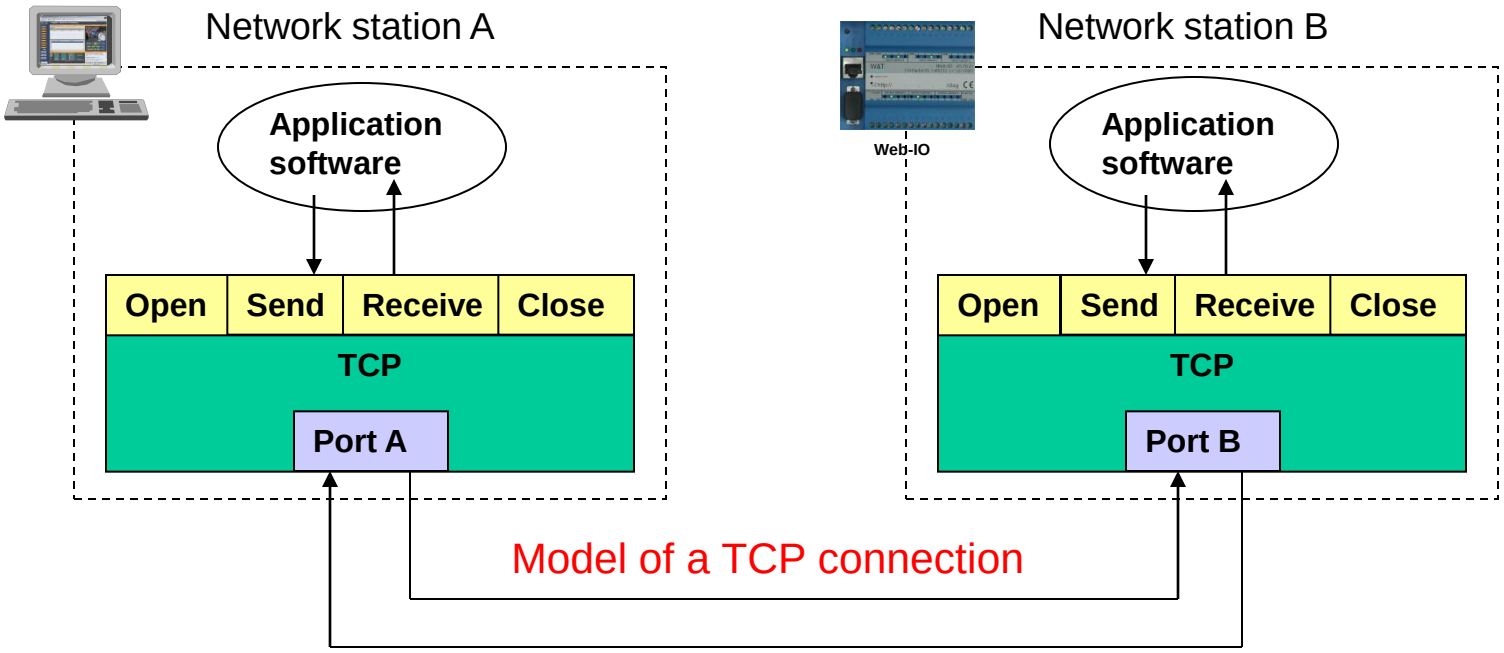


UDP has a short and simple header, only 8 bytes long. UDP introduces the concept of port numbers, which are used by the application layer that resides above UDP.

UDP allows faster data exchange because there is no acknowledgment to the sender. Therefore, in PROFINET IO this protocol is used for acyclic data exchange and system startup.

Transmission Control Protocol

The **TCP** (Transmission Control Protocol) is used to provide a connection-based and reliable data packet transporting service for processes. One can be sure that the data packet is delivered correctly. Besides reliable connections, TCP provides flow control to ensure stations are not flooded with data. The header of TCP is larger than that of UDP.



Port Number Assignment

Port number is introduced in combination with a transport protocol, such as UDP or TCP. This property of port number makes it possible that one station can support several different applications simultaneously.

Three ways to classify port numbers

- Assigned: The **IANA** (Internet Assigned Numbers Authority) defined the assigned port numbers in the range of zero to 1023 for various applications that are considered part of the TCP/IP protocol suite. These port numbers are well-known, meaning that they are used by common applications. These applications include **TELNET**, **FTP**, **SMTP**, **WWW**, **POP3**, etc.

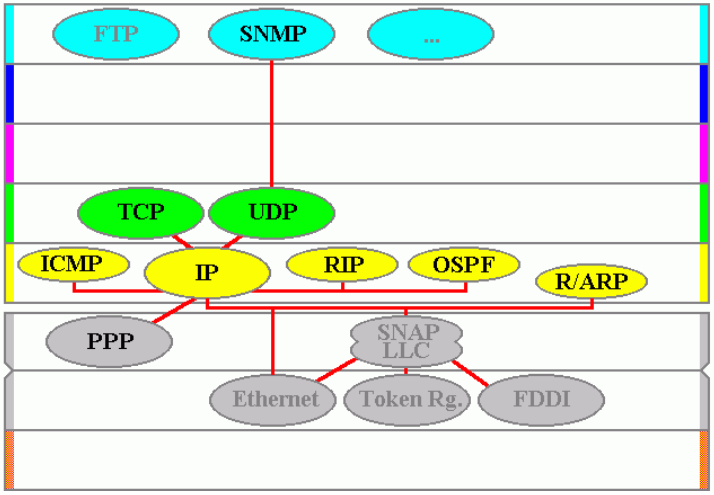
  Example of an IP address with well-known port: 192.168.0.1:**80** (HTTP protocol).

- Registered: The port numbers in the range of 1024 to 49151 can be registered by firms or organizations for proprietary purposes.

- Dynamic: The port numbers in the range of 49152 to 65535 are considered either private or dynamic, and can be used by anyone.

Address Resolution Protocol and others

The **ARP** (Address Resolution Protocol) and the **RARP** (Reverse Address Resolution Protocol) are very important for the network access layer. With these protocols, one can resolve the logic addresses to the physical addresses and vice versa. ARP is used to resolve the Ethernet address from an IP address in order to construct an Ethernet packet around an IP data packet. This must happen in order to send any data across the network.



- **ICMP:** Internet Control Message Protocol is used to forward error information.
- **DHCP:** Dynamic Host Configuration Protocol is used for assignment of the IP addresses and related parameters.
- **DNS:** Domain Name Service is used in order to manage the logic names.
- **SNMP:** Simple Network Management Protocol is used in order to monitor the network.

Summary

PROFINET is an industrial communication system based on the industrial Ethernet standard. It builds on the well-known and highly popular PROFIBUS system. The main advantages of PROFINET against PROFIBUS are high-speed data transfer, which is up to 100 Mbps, and the possibility of obtaining process data from field devices.

PROFINET IO is designed for a data exchange system between controllers and field devices. PROFINET CBA is designed for a distributed automation system. Both concepts are based on using the industrial Ethernet standard.

To understand PROFINET, we took a look at the basics of Ethernet standard. We discussed the ISO/OSI reference model, the installation technique and the network protocols .

References

Popp, M.; Weber, K.: The rapid way to PROFINET. - PROFIBUS Nutzerorganisation e.V., Karlsruhe, Germany, 2004

Popp, M.: Das PROFINET IO Buch. - Hütig GmbH & Co. KG, Heidelberg, Germany, 2005

Bormann, A.; Hilgenkamp, I.: Industrial Networks. - Phoenix Contact GmbH & Co. KG, Blomberg, Germany, 2006

PROFIBUS Nutzerorganisation e.V.: PROFINET Technology and Application System Description. - http://www.profibus.com/pall/meta/downloads/article/00456/

Siemens AG: PROFINET System Description Siemens. - http://support.automation.siemens.com/WW/view/en/25571355