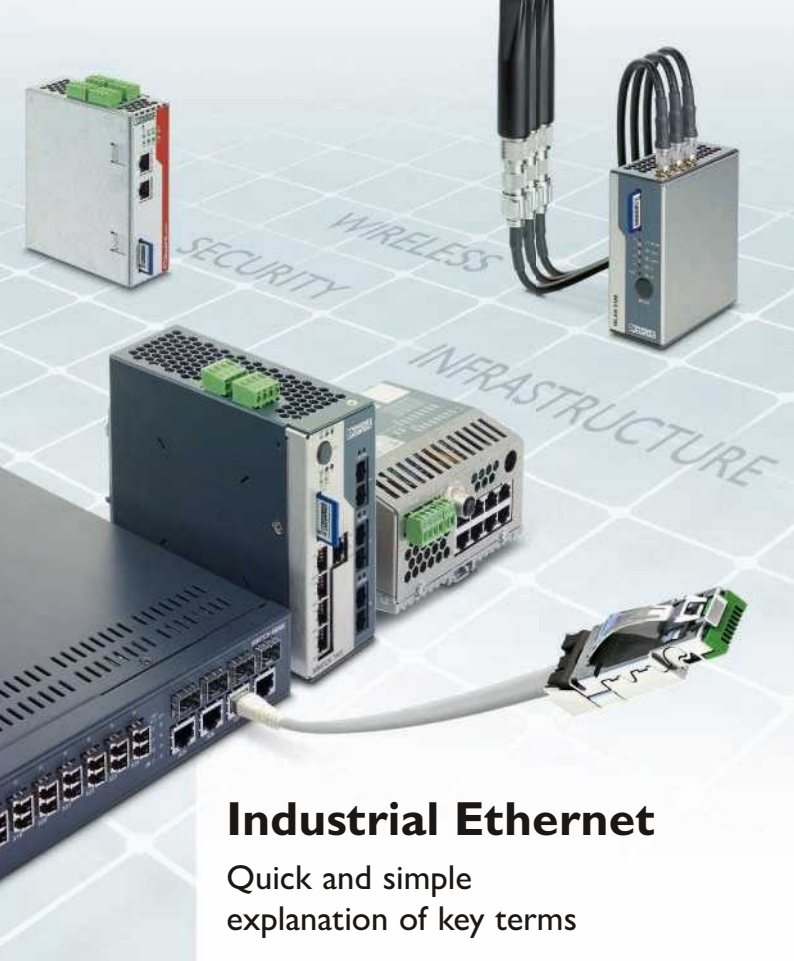

Industrial Ethernet

Quick and simple
explanation of key terms

PHOENIX CONTACT
INSPIRING INNOVATIONS

Industrial Ethernet

The use of industrial Ethernet communication offers many advantages and is becoming more common in the automation of production plants and machinery. Many new technical terms from the IT world are also being used in this context among industrial users.

In this glossary, we have listed and explained the main technical terms from the field of Industrial Ethernet – we make Ethernet easy.

Table of contents

Industrial Ethernet

10Base-T	Standard for data transmission of 10 Mbps Ethernet using unshielded twisted pair cables (Category 3, 4 or 5).
100Base-FX	Standard for data transmission of 100 Mbps Ethernet using fiber optic cables.
100Base-TX	Standard for data transmission of 100 Mbps Ethernet using twisted pair cables (Category 5). Each connection is established via two wire pairs, one wire pair for "transmit data" and the other for "receive data".
100Base-T	Fast Ethernet; 100Base-T has been officially elevated to an IEEE standard as ITU 802.3u. This standard is essentially based on technologies for 10Base-T, the Ethernet version for twisted pair cables. There are several versions of 100Base-T, which differ with respect to the physical layer and therefore the transmission media: 100Base-TX, 100Base-T2, 100Base-T4, and 100Base-FX. With this method, the MAC level and therefore the conventional CSMA/CD access method are retained at a transmission speed of 100 Mbps. As a result, only very short distances can be covered with 100Base-T. In the case of Category 5 twisted pair cables (UTP, STP), the maximum segment expansion is 100 m.
1000Base-LX	Standard for data transmission of 1000 Mbps Ethernet using fiber optic cables at a wavelength of 1300 nm.
1000Base-SX	Standard for data transmission of 1000 Mbps Ethernet using fiber optic cables at a wavelength of 850 nm.

1000Base-T	Standard for data transmission of 1000 Mbps Ethernet using twisted pair cables (Category 5e or 6). Data can be simultaneously transmitted and received on four wire pairs.

A

Access point	The access point is a component which forms the transfer point between a wired and a wireless network. An access point establishes the connection to the wired network for the clients. It is connected to all clients within its wireless range and performs central tasks such as roaming or security functions.
ACD	Address conflict detection (ACD) is a function for detecting IP address errors in the network and therefore avoiding possible network failure.
Ad hoc network	Ad hoc is a wireless network which spontaneously establishes a point-to-point connection between individual devices without an access point.
ADSL	Asymmetric digital subscriber line (ADSL) is a further development of DSL intended to meet the needs of private customers for higher data rates without impairing telephony via the fixed line network.
AES	The Advanced Encryption Standard is an encryption method for WLAN among others. The method is accepted as secure.
AFH	Adaptive Frequency Hopping (AFH) is the automatic adjustment of the list of wireless channels used when these are occupied.
Aging	Aging is a procedure for updating data, especially in address tables. See Aging time

Aging time	A learned MAC address of a device (source address) is deleted from a switch address table if no data telegrams are received from this source address within the aging time. The switch assumes that the device with the source address is no longer in the network.
Alarm/signal contact	An alarm contact is used to generate an alarm in the event of an error in the device, such as a link down or failure of the redundant power supply.
Antivirus scan connector	The antivirus scan connector is an antivirus scan function performed on drives protected by the firewall that are otherwise not externally accessible. All network drives are combined and mirrored to the outside as a single drive in order to allow an external virus scanner to perform a virus scan.
Application layer	The application layer is layer 7 of the ISO/OSI reference model and includes user-specific services for various communication applications, such as file transfer.
ARP	The Address Resolution Protocol (ARP) is used to determine the MAC address of a network device that belongs to an IP address. The assignments determined are managed in the ARP table on the relevant computer.
Auto MDI(X)	The auto MDI(X) function describes the automatic detection and setting of the transmission and receiving power of the connected devices. Each Gigabit device must support this function.
Autocrossing	A device with autocrossing function automatically detects which type of device (DTE or DCE) should be used to establish communication. With this mechanism, there is no need to distinguish between line and crossover connecting cables.

Auto negotiation	In auto negotiation mode, two Ethernet devices automatically negotiate their data transmission speed (10 Mbps, 100 Mbps or 1000 Mbps) and transmission method (half or full duplex).
Auto polarity	Auto polarity is a device function that automatically corrects wiring errors in wire pairs in 10Base-T or 100-Base-TX interfaces and also reverses the polarity of the data signals.
Auto sensing	In auto sensing mode, an Ethernet device automatically sets itself to the data transmission speed (10 Mbps or 100 Mbps) of the device to which it is connected.

B

BFOC	Bayonet Fiber Optic Connector – standardized fiber optic connector for multi-mode and single-mode fibers at 10 Mbps, also referred to as an ST connector. The connector is secured with bayonet locking.
Bluetooth	Bluetooth is an industrial standard from 1990 for the wireless networking of devices over short distances. Bluetooth provides a wireless interface to replace cable connections between devices.
Bluetooth 1.2	Data rates of up to 1 Mbps. Supports Adaptive Frequency Hopping (AFH).
Bluetooth 2.1 + EDR	Data rates of up to 1.2 Mbps. When using Enhanced Data Rate (EDR), Forward Error Correction (FEC) is not supported. Bluetooth 2.1 is backwards compatible.

BootP	The Bootstrap Protocol is directly based on the User Datagram Protocol (UDP) in terms of its application. Communication takes place via a single data packet according to the client/server principle. In addition to the server IP address, the client can also request the IP address of the next router, the IP address of a specific server or the name of the server's boot file. In the manufacturer-specific part, specially defined information can also be transmitted.
BPDU	Bridge Protocol Data Unit (BPDU) refers to signaling packets between switches that are used with Spanning Tree.
Bridge	A bridge is a device used to connect two separate networks. The incoming data packets are filtered using the destination address and are forwarded to the second network or rejected. Bridges connect subnetworks according to the ISO/OSI reference model using protocols on layer 2.
Broadcast	Broadcast refers to a collective call to all devices in the network that is not forwarded via routers and bridges.
Broadcast domain	An area in a network where broadcast telegrams are forwarded. Broadcast domains are separated by routers.
Browser	A browser is a computer program that is used to view Internet pages (text, images) on a monitor.
Bus	A bus or fieldbus is an industrial communication system that connects different devices, sensors, actuators, and drives to a controller. Fieldbus technology was developed in the 1980s to replace the wiring of binary signals and analog signals with digital transmission technology.

C

CAN	A Controller Area Network (CAN) is an asynchronous, serial bus system which was developed in 1983 in order to network control devices in automobiles.
CANopen®	CANopen® is a communication protocol based on CAN that is mainly used in automation technology and for networking within complex devices. CANopen® is widely used in Europe.
CAT5	EIA/TIA specification for Ethernet cables, connectors, and outlet boxes. Suitable for 10 and 100 Mbit networks, transmission via two wire pairs.
CAT5e	Extended CAT5 specification with strict electrical properties. Full duplex mode via four wire pairs. Suitable for 1000 Mbit networks.
CAT6	EIA/TIA specification for Ethernet cables, connectors, and outlet boxes. This results in an increased bandwidth requirement of 10 Gigabits.
CAT7	EIA/TIA specification for Ethernet cables, connectors, and outlet boxes. This results in an increased bandwidth requirement of 10 Gigabits. CAT7 cables have four wire pairs that are shielded from each other within an overall shield. Since the RJ45 connector does not satisfy the requirements according to 802.3an, a new connector has been developed.
CIFS	CIFS Integrity Monitoring (CIM) is a form of antivirus protection – or more accurately an antivirus sensor – suitable for industrial applications which is able to detect whether a Windows-based system (controller, operator interface, PC) has been attacked by malware without the need to load virus patterns. CIFS therefore offers dynamic monitoring of Windows systems.

CIFS integrity checking	When CIFS integrity checking is performed, Windows network drives are regularly checked against a reference status to determine whether certain files (e.g., *.exe, *.dll) have been changed.
CIP	The Common Industrial Protocol (CIP) is the application layer of EtherNet/IP™ which is based on TCP and UDP.
CIP Motion	CIP Motion is an extension of the Common Industrial Protocol which provides the necessary functions for a synchronous machine application.
CIP Safety	CIP Safety is an extension of the Common Industrial Protocol and ensures seamless communication between standard devices and safety components in a network.
CIP Sync	CIP Sync is an extension of the Common Industrial Protocol which is based on PTP 1588 time synchronization. Motion control or axes are thereby synchronized.
CLI	Command line interface (CLI) is a command language from the IT world for the parameterization and configuration of network components.
Client	A client is a hardware or software component that accepts services from a server. The client is always the service requester.
Collision	A collision occurs when two devices simultaneously attempt to send data on the same medium. A collision is resolved according to the CSMA/CD method.

Collision domain	Collision domain describes the section in a network where two devices attempt to send data on the same communication medium at the same time. If that happens, a collision will occur.
COM server	A COM server is a termination device in TCP/IP networks which provides interfaces for serial devices via the network.
Crossover cable	A crossover cable is a cable configuration that connects two devices of the same type (DTE/DTE and DCE/DCE). The pin assignment is different at the cable ends so that transmit cables can be connected to receive cables.
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is a method for accessing wireless channels in IEEE 802.11 networks.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a method for dealing with data collisions in wired networks. A station ready for transmission listens to determine whether the transmission medium is free (Carrier Sense). It then starts transmitting and simultaneously checks if other stations (Multiple Access) are also transmitting data. If two or more stations are transmitting data simultaneously there will be a collision. The stations will then stop transmitting (Collision Detection) and try to transmit again after a random time.
cUL 1604	cUL 1604 is a US safety standard for electrical equipment in potentially explosive environments.

cUL 508	cUL 508 is a US safety standard for industrial control equipment.
Cut-through switching	Cut-through switching refers to the forwarding of incoming data packets from the moment the destination address is detected. The advantage is the short latency, but the disadvantage is that faulty data packets are also forwarded.

D

DALI	Digital Addressable Lighting Interface (DALI) is a control protocol for digital lighting devices in building automation systems. DALI uses a serial, asynchronous data protocol with a transmission speed of 1200 bps. The control cable is electrically isolated, polarity-free, and there is therefore no risk of polarity reversal.
Data link layer	Layer 2 in the OSI model – the layer protocols indicate how the frames are sent via the network. Communication between the switches via the Ethernet protocol takes place on this layer.
dB / dBi / dBm	The decibel is a logarithmic unit which makes it easier to work with large value ranges. dB: comparison of two values dBi: antenna gain compared to an omnidirectional antenna (“isotropic radiator”) dBm: power level compared to 1 mW
DCE	Data communication equipment (DCE) refers to infrastructure components in a communication path, e.g., modem, hub, switch. DCE devices can be connected directly, i.e., with 1:1 cables, to DTE devices. Direct connection of two DTE devices can only be implemented using crossed cables.

DCP	The Device Control Protocol (DCP) is a protocol in the PROFINET environment for reading the names of network devices as well as assigning names and IP addresses.
DeviceNet™	DeviceNet™ is a low-cost industrial network that uses CAN technology. It connects industrial I/O components to the controller or PCs.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an automatic, dynamic, and usually temporary assignment of IP addresses from a defined address area.
Directional characteristics	Angle dependence of an antenna, for example. A distinction is made between panel antennas and omnidirectional antennas.
DLR	The device level ring (DLR) is a redundancy mechanism which ensures that switch-over times of less than 3 ms can be achieved in the event of an error.
DNS	Domain Name System (DNS) refers to a system that assigns host names, Internet addresses in plain text, and IP addresses to one another. For implementation, DNS servers or files designated as "hosts" are used as the data source, for example.
DNV	Det Norske Veritas (DNV) is a Norwegian classification society for shipbuilding.
DSL	Digital subscriber line (DSL) is a physical layer transmission standard. High transmission speeds of up to 500 Mbps via a copper cable.

DTE	Data terminal equipment (DTE) refers to termination devices that are always installed at the start and end of a communication path, e.g., PLC, PC, etc. Direct connection of two DTE devices can only be implemented via crossed cables.
Dynamic DNS	Dynamic DNS continues to assign the same name when the IP address changes.
Dynamic routing	In the case of dynamic routing, dynamic routing protocols find a path between individual networks. RIP and OSPF are dynamic protocols.

E

EDS file	EDS stands for Electronic Data Sheet. The EDS file is a device description which is required in the EtherNet/IP™ environment in order to integrate field devices into a control environment.
EIA	The Electronics Industry Association (EIA) is an American association for the standardization of interfaces and communication applications.
EMC	Electromagnetic compatibility (EMC) specifies the freedom from interference of electrical and electronic devices in their environment.

Ethernet	Network standard developed by Intel, DEC, and Xerox, which has been widely used, especially in LANs, since 1976. The Ethernet standard contains specifications on the network architecture (bus or star topology), hardware (e.g., cabling with coaxial or twisted pair cables), transmission methods, and access methods.
EtherNet/ IP™	The Ethernet Industrial Protocol (EtherNet/IP™) is an Ethernet-based fieldbus and open standard of the ODVA.
Explicit messaging	Explicit messaging is based on the principle of "request/ response".

F

Fast Ethernet	Fast Ethernet is operated using Category 5 copper cables or fiber optics, the data transmission speed is 100 Mbps. Fast Ethernet was standardized in 1995 by IEEE 802.3.
FCC	The Federal Communications Commission (FCC) is a US agency that manages and assigns the frequency spectrum on a regional and national level.
FCC CFR47 Part 15	Standard on noise emission for information technology equipment. Federal Communications Commission Code of Federal Regulations.

FCS	Frame Check Sequence (FCS) refers to a bit field for saving user data in bit-oriented protocols. The sender and receiver use a specified algorithm to create and compare a checksum. This method is used to detect errors during data transmission.
FDCML	Field Device Configuration Markup Language (FDCML) is an XML-based, flexible description language for describing field devices. This language is used to provide information on the manufacturer, device type, configuration, and device parameters.
Firewall	Firewalls are network components which use special protocols to monitor and restrict requested services, the data they contain, and the direction of information flow. Access rights can be defined depending on authentication and identification. Firewalls can also be used to encrypt data.
FO	Fiber optics (FO) is a transmission medium with an inner conductor made from glass or plastic and several coatings as protection against mechanical strain.
FRD	Fast ring detection (FRD) is an extension of the RSTP (Rapid Spanning Tree Protocol) from Phoenix Contact where switch-over times of 100 to 500 ms can be achieved in the ring with up to 56 devices. The protocol can only be used on a 10/100 Mbit basis.
F-SMA	Fiber optic connector for POF and HCS fibers, secured with a union nut, easy connection thanks to fast connection technology.

F/STP	Foiled Shielded Twisted Pair (F/STP) is a twisted pair cable with pair shield as wire mesh and overall shield as foil.
FTP	The File Transfer Protocol (FTP) is a TCP/IP protocol for transferring files. To transfer files via FTP, a connection must be established between the client and an FTP server. To log into this server, an access ID and corresponding password must be entered.
Full duplex	Full duplex is simultaneous, independent two-way transmission in both directions; simultaneous transmitting and receiving.

G

Gain	Improvement in transmission power and sensitivity by concentrating on a radiation pattern. Antennas with a large gain have a small opening angle.
GARP	The Generic Attribute Registration Protocol (GARP) refers to a group of protocols used to exchange parameters between switches on layer 2 of the ISO/OSI reference model. Existing protocols include GMRP and GVRP.
Gateway	A gateway is a technical device that enables transition between different networks (e.g., between Ethernet and INTERBUS). Gateways are protocol converters that convert received data to another protocol.
GBIC	Gigabit interface converter. See SFP

Gbps	Transmission unit – Gigabits per second.
Gigabit Ethernet	Gigabit Ethernet refers to a very fast Ethernet data network that is standardized by IEEE 802.3. It is based on a transmission speed of 1000 Mbps with a variable packet length of 64 to at least 1518 bytes (1522 bytes with VLAN tag).
GL	Germanischer Lloyd (GL) is a German classification society for shipbuilding.
GMRP	GARP Multicast Registration Protocol See GARP
GOOSE	Generic Object Orientated System Event (GOOSE) is an Ethernet protocol which is transmitted via layer 2 and enables event-controlled communication in IEC 61850.
GSD	General Station Description – in order to be able to integrate components into an automation solution, various information regarding the device must be provided in the engineering steps. Within the PROFINET system, the device description is imported into the engineering system in XML format. The GSD high-level language (markup language) GSDML is used for this. In an engineering system, the GSD file is used as the basis for planning the configuration of a PROFINET I/O system.
GSDML	GSD Markup Language – XML-based high-level language for GSD files.
GVRP	The GARP VLAN Registration Protocol (GVRP) is a protocol that switches can use to exchange information with VLANs. If a VLAN is set up on a switch, the switch sends this information to all switches that are connected directly. This enables other switches, e.g., the port that received the information, to also become part of this VLAN.

H

Half duplex	Half duplex is a method where data is transmitted in both directions, but not simultaneously.
HASH	HASH is a checksum for checking the integrity of a piece of information.
HCS fiber	Hard-clad silica (HCS) (also known as hard-clad silica fiber (HCSF)) is an optical fiber with a silica glass core and cladding made of special plastic.
HCS GI fiber	HCS graded index fiber – HCS fiber with a special internal glass core. In the case of this glass core, transitions between the refractive indices of the glass fibers are continuous, which results in particularly good transmission properties and longer transmission distances.
Header	The start of a data packet is referred to as the header. It contains information on the packet size and transmission method, as well as the sender and recipient address.
Hop	Hop refers to a jump from one network node to another.
HSR	High-availability Seamless Redundancy (HSR) is a redundancy mechanism which results in zero switch-over time and reconfiguration time in a redundancy scenario by doubling the transmitted information in a ring.
HSR Quadbox	The Quadbox is an infrastructure element that couples two HSR rings. Four HSR-capable ring ports are required for this.

HSR Redbox	The “Redundancy Box” connects SAN (Single Attached Nodes) redundantly to the HSR ring, two HSR-capable ring ports are required for this.
HTML	Hypertext Markup Language (HTML) is not a programming language, but a standardized page description language for web pages. In order that HTML documents can be displayed by all popular computers, operating systems, and browsers, they only contain ASCII text. Formatting and commands are placed in angle brackets so that the browser can distinguish them from the actual content. The HTML standard was introduced by the World Wide Web Consortium (W3C) in Geneva, Switzerland.
HTTP	The Hypertext Transfer Protocol (HTTP) is a protocol (transmission standard) that controls the exchange of data between a web server and a web client. HTTP is based on TCP/IP.
HTTPS	The Hypertext Transfer Protocol Secure (HTTPS) is a protocol for data exchange where each packet of information is encrypted.
Hub	A hub is at the center of a star topology. It forwards received data to all ports and uses CSMA/CD to ensure collision-free data transmission. A hub is always used in half duplex mode.

I

ICMP	The Internet Control Message Protocol (ICMP) is a protocol for exchanging information and error messages when transmitting IP data packets. The most commonly known command is the “ping command”.

IE	Industrial Ethernet (IE) places high demands on network availability, network security, and ambient conditions of the Ethernet components in automation technology.
IEC	International Electrotechnical Commission
IEC 61850	The IEC 61850 series of standards on "Communication networks and systems for power utility automation" describes general requirements for the automation of power switchgear. These include the engineering, information models, communication solutions, and conformance tests.
IED	An intelligent electronic device is any electronic device in a power application which is integrated into communication according to IEC 61850 (e.g., protective, control, and measuring devices in switchgear = primary technology).
IEEE	The Institute of Electrical and Electronics Engineers (IEEE) is an American association which develops standards, focusing on information technology.
IGMP	The Internet Group Management Protocol (IGMP) is a protocol for organizing multicast groups in a network.
IGMP snooping	Internet Group Management Protocol snooping (IGMP snooping) is a function where switches on layer 2 check the IGMP packets, create multicast groups, and forward incoming multicast data packets according to group which they belong to.
Implicit messaging	Implicit messaging is used for the cyclic transmission of I/O data.
INTERBUS	INTERBUS is a fieldbus system for widespread use in a company; for example, the sensor/actuator level as well as the automation level and PC monitoring are covered by this bus. INTERBUS was developed by Phoenix Contact.

IP	The Internet Protocol enables the connection of devices that are located in different networks. It operates on layer 3 of the ISO/OSI reference model.
IP address	An IP address is a unique device address in Ethernet. It is a numerical code made up of four numbers between 0 and 255 (32 bits) separated by dots (dotted decimal notation). The IP address is assigned by the network administrator and consists of two parts: the network address and the host address.
IP masquerading	See NAT
IP spoofing	IP spoofing is where IP packets are sent from a fake IP address in a network.
IPsec	Internet Protocol Security (IPsec) is a standard which uses encryption to ensure the authenticity of the sender and maintain the integrity and confidentiality of the data when sending IP telegrams. The components of IPsec are the Authentication Header, the Encapsulating Security Payload, the Security Association, and the Internet Key Exchange.
IPv4	Internet Protocol Version 4 – IPv4 has an address area of 4 bytes.
IPv6	Internet Protocol Version 6 – IPv6 is an ongoing development of Version 4 (IPv4) and offers significantly enhanced addressing options and improved security aspects.

IRT	Isochronous realtime (IRT) PROFINET is used in conformance class C. Thanks to bandwidth reservation, part of the available transmission bandwidth of 100 Mbps is reserved exclusively for realtime tasks. A method similar to time-division multiplexing is used here. The bandwidth is split into fixed cycle times for various types of PROFINET communication.
ISDN	Integrated Services Digital Network (ISDN) is a standard for communication in a digital communication network.
ISM band	Industrial, scientific, and medical bands (ISM bands) are frequency bands for using applications in these areas. For example, there are ISM bands in the frequency range 433, 868, 2400 MHz. The 5 GHz band is not an ISM band, WLAN applications have secondary status here. This is taken into account by the DFS mechanism according to IEEE 802.11h.
ISO	International Organization for Standardization – umbrella organization for national standards bodies.
ISO/OSI reference model	Reference model for open system interconnection – seven-layer model for the network architecture for data communication. Each layer defines services and makes them available to higher layers.
ISP	Internet service provider – the ISP provides the connection to the Internet and therefore enables IP packets to be exchanged. Colloquially referred to as provider.

J

Jabber	A jabber is a telegram with invalid CRC and/or a length of more than 1518 bytes that is sent to the network by a station. It is usually caused by a faulty network card or driver.
Jitter	Jitter refers to signal deformations and skew in the received signal compared to the sent signal.
Jumbo frames	Jumbo frames are Ethernet frames that are greater than 1518 bytes. The maximum size for standard frames is specified in standard IEEE 802.3. In the case of some special applications, such as image transfer and data backup, jumbo frames can be useful as the protocol overhead can thereby be minimized. Oversized data packets according to IEEE 802.3 are ignored or deleted by hardware which does not support jumbo frames.

K

kbps	Kilobits per second
KEMA	Test institute in the Netherlands: Keuring Van Elektrotechnische Materialen – inspection of electrical equipment in Arnhem.

L

L2TP	The Layer 2 Tunneling Protocol (L2TP) is used to create a VPN tunnel on layer 2. See IPsec

LACP	The Link Aggregation Control Protocol (LACP) is a protocol for dynamically bundling various physical networks, certified according to IEEE 802.3ad.
LAN	A Local Area Network (LAN) is a network of computers, which share applications, data, printers, and other services. Their physical expansion is limited to a local area such as a building and/or a group of buildings.
Large Tree Support	Large Tree Support is an extension of RSTP from Phoenix Contact. This extension allows ring structures with up to 57 switches to be created.
Latency	Delay time between a device receiving data and forwarding it again after processing.
Layer 3 switch	A multifunctional device that is a combination of a router and a switch. Each port of this type of switch is located in a separate subnetwork.
Link aggregation	Function where the switch ports are combined to form a virtual port. This increases data throughput significantly and provides redundancy, certified according to IEEE 802.3ad.
Link status	The device sends regular link status pulses to the ports of connected partner devices to monitor the validity of the connection to these partner devices. On Phoenix Contact devices, a valid connection is indicated by a green LED.
LLDP	The Link Layer Discovery Protocol (LLDP) is a function for automatically detecting neighboring devices. The devices in the network exchange LLDP packets and save them in neighbor tables.

M

MAC	Media access control (MAC) is a general term for the type and method of access to transmission media.
MAC address	Globally unique ID for a network component that cannot be modified and consists of six bytes and a manufacturer ID.
MAC address table	Address table of a switch where it stores the port to which a packet must be sent. In the address table, a MAC address is assigned to the port via which the respective device can be reached. The table is updated regularly.
Malware	Malware is an unsolicited program that is usually installed secretly or without the user's knowledge. These programs perform harmful functions on the system.
MAN	A Metropolitan Area Network (MAN) is where several LANs are connected, usually via fiber optics. Physical expansion of up to 100 km.
Mbps	Megabits per second
MDI	A Media Dependent Interface (MDI) is an Ethernet connection which can be connected directly to other infrastructure components, without the need for special crossover cables. These connections are often referred to as “uplinks”.
MDI-X	Media Dependent Interface Crossover (MDI-X) is an Ethernet connection which can be connected directly to termination devices such as PCs or controllers.

MIB	A Management Information Base (MIB) is a database containing the objects and variables of monitored network components which are required for network management via SNMP.
MIMO	Multiple Input Multiple Output (MIMO) refers to transmitting and receiving at several antennas simultaneously. Together with WLAN standard 802.11n, this enables the data rate to be increased by creating parallel data streams (e.g., spatial multiplexing). MIMO technology benefits from a reflective environment. Three antennas are often used in practice.
Mirroring	See Port mirroring
Modulation type/ chipping sequence	Different digital modulation types and chipping sequences are used in different WLAN standards for wireless data transmission (e.g., PSK, QAM, CCK, DSSS, OFDM). Basically, the more complex the procedure is, the higher the data rate that can be transmitted and the lower the robustness of the transmission.
MRP	The Media Redundancy Protocol (MRP) is a redundancy protocol that is part of PROFINET standard IEC 61158, which ensures switch-over times of 200 ms in a ring topology.
MTBF	Mean Time Between Failure (MTBF) is the average time a system operates without an error occurring.
Multi-mode module	Also: SX module. Optical transceiver used in conjunction with multi-mode fibers and for transmission over medium distances.

Multicast	Multicast refers to transmitting data packets from a sender to a defined group of recipients. This logically created group receives a group address from the area reserved for multicasts.
Multicast address	Telegrams with a multicast address can be received by several devices which are ready to receive for this address.

N

N connection	Stable connection standard for antennas (antenna cables).
NAT	Network Address Translation (NAT) is also referred to as IP masquerading. The NAT router establishes the connection between the Internet (external) and entire networks (internal). Only the NAT router and its IP address are visible externally, all connections from within the system to the Internet and vice versa are made via the NAT router, which manipulates the relevant entries in the data telegrams. NAT routers can be used to provide a certain degree of protection for the internal network.
Network layer	Layer 3 in the OSI model – addressing takes place on this layer, i.e., finding a path through the network. The network layer takes care of messages transmitted from the sender to the recipient while they are on their way from one node to the next.
Network management	Network management is carried out by the administrator using software. The network can be configured, optimized, and monitored. In the event of an error, the cause can be determined.

NIC	A network interface card (NIC) is an adapter card which is integrated in a PC and provides the necessary software/ hardware for communication via a network.
NTP	The Network Time Protocol (NTP) is used for time synchronization in computer systems. Its successor is SNTP.

O

ODVA	The Open Device Vendor Association (ODVA) is an association that promotes the worldwide use of DeviceNet™ and EtherNet/IP™ network technologies and standards in industrial automation.
OID	Object ID – in conjunction with SNMP, the OID is information from the MIB.
OLE	Object Linking and Embedding (OLE) is a central architecture in Windows.
Omni-directional	An antenna which radiates horizontally over 360°. As the gain increases, the vertical emission angle decreases, i.e., the antenna is insensitive above and below this zone.
OPC	OLE for Process Control is the most widely used standard-based data connectivity method in the world. It enables communication between devices and applications from different manufacturers.
OSPF	Open Shortest Path First (OSPF) is a dynamic routing protocol which selects the most inexpensive route in a network to forward data to a device in another subnetwork. The successor to RIP.

P

PAN	A Personal Area Network (PAN) is a network that can be immediately established/broken down by small devices such as PDAs or mobile phones. PANs can be established using wired transmission technologies such as USB and FireWire or wirelessly via Bluetooth, for example. The range is normally only a few meters and used for communication between devices.
Performance	In IT, this refers to the time response and the performance of programs (software) and devices (hardware).
Physical layer	The physical layer is layer 1 of the ISO/OSI reference model and defines the mechanical, electrical, and functional parameters of the physical interface: transmission speed, character length, voltage level, transmission medium, etc.
Ping	A ping (Packet Internet Groper) is a small data packet that is used to measure the reliability of a network connection and the response time of a server. A client contacts a server at its ping port. As soon as the server responds, the client calculates the elapsed time in milliseconds. The function also determines whether pings are lost. To achieve realistic results, pings with different byte sizes should be sent.
PLC	A programmable logic controller (PLC) is an electronic module for use in automation technology and for control tasks in industrial environments.
PoE / PoE+	Power over Ethernet enables Ethernet devices to be supplied with power via an Ethernet copper connection. PoE is specified in standard IEEE 802.3af with a maximum power output of 15.4 W. There is also the newer standard IEEE 802.3at – known as PoE+ or PoE plus prior to standardization – which supports a maximum power output of 25.5 W.

POF	Polymer optical fiber See Polymer fiber
Polarization	Oscillation plane of a wave. In the case of wireless transmission, the polarization of both antennas must match in order to achieve the maximum range.
Polymer fiber	Optical fiber made from 100% plastic, easy assembly with F-SMA fast connection technology, diameter of 980/1000 µm.
Port	Interface or also Ethernet slot for data transfer to infrastructure components or termination devices.
Port forwarding	Port forwarding refers to the forwarding of data to another computer system that arrived in the computer system via a specific port.
Port mirroring	Function where data transmitted from a port is copied (mirrored) to another port, e.g., for diagnostic purposes.
Port security	Function which prevents unauthorized access to the network. With this function it possible to specify MAC addresses that are permitted to access the network. All other addresses are denied access.
Port trunking	See Link aggregation
Powerlink	Powerlink is a protocol extension to the Ethernet standard according to IEEE 802.3 for transmitting realtime data in the microsecond range. Its main purpose is to transmit process data in automation technology.

PPP	The Point-to-Point Protocol (PPP) is the successor to the SLIP protocol. PPP enables data transmission via permanent and dial-up connections in analog and digital fixed-line and mobile phone networks. It is used when a PC is connected to the Internet via phone lines.
PPPoE	Point-to-Point Protocol over Ethernet
Presentation layer	The presentation layer is layer 6 of the ISO/OSI reference model and defines procedures for conversion and format adjustment. It ensures correct interpretation of the data.
Prioritization	Predefined criteria are used to transmit certain data packets faster than others.
PROFIBUS	PROFIBUS is a open fieldbus standardized according to EN 50170.
PROFINET	Ethernet communication model from field level to control level.
PROFINET I/O	A PROFINET I/O system consists of the following devices: • I/O controller: a controller which controls the automation task • I/O device: a field device that is controlled by an I/O controller • Software that is used to parameterize and diagnose the individual I/O devices
PROFINET diagnostics	There are special diagnostic options in PROFINET, e.g., topology detection or fiber optic diagnostics.

PRP	The Parallel Redundancy Protocol (PRP) is a redundancy mechanism which enables network redundancy with zero switch-over time in the event of an error.
PSE	Power sourcing equipment (PSE) refers to devices (e.g., switches) which provide power according to draft standard IEEE 802.3af. This standard defines power supply via an Ethernet twisted pair cable.
PSU (PS)	Power supply unit, power supply
PTCP	PROFINET Precision Transparent Clock Protocol The PTCP protocol is used for time synchronization in PROFINET IRT applications. The connected ports of two components cyclically exchange time information with one another by means of multicast messages. The forwarding of PTCP packets to another network by unsuitable components must be prevented as the multicast packets spread in the network and can cause unforeseeable network loads.
PTP	The Precise Time Protocol (PTP) is a protocol for synchronizing the clock settings of several devices in a network. As defined in IEEE 1588, accuracy in the nanosecond range can be achieved by a hardware version and accuracy of a few microseconds can be achieved by a software version.
PTP – boundary clock	These clocks transport time information to other networks. They are time receivers in one network and the time source in the other network.

PTP – ordinary clock	These clocks are integrated into termination devices and are either the time source or the time receiver.
PTP – transparent clock	This type of clock receives PTP time information, calculates the signal runtime, and forwards the corrected time (time information – signal runtime). It is mostly used in infrastructure components such as switches (available as of PTP v2).

Q

QoS	Quality of Service (QoS) is a collective term for quality classes for network services. It takes speed, bandwidth, delay, security, and priority into consideration.

R

RADIUS	The Remote Authentication Dial-In User Service (RADIUS) is used to protect authentication in wireless networks.
Redundancy	Increased data availability in a network due to various redundancy mechanisms.
Repeater	WLAN operating mode for extending the wireless range. The device logs into an existing access point as a client and as the access point creates a new wireless cell.
RFC	Request for Comments (RFC) is a standardization document from the Internet research and development group, e.g., for the definition of protocols or services.

RIP	The Routing Information Protocol (RIP) is a protocol for the automatic creation of routing tables in a network. Each routing table is sent to the next router in the network and completed.
RJ45	The RJ45 plug-in connection was originally developed in 1980 by AT&T for 3 MHz and was accepted as a standard in cabling standards EN 50173-1 and FSO 11801.
RMON	Remote monitoring (RMON) is a subset of SNMP MIB II and enables the monitoring and management of network devices using ten different information groups.
Roaming	Roaming is a function where a wireless device automatically detects a foreign wireless network as the home network.
Router	Routers are connecting elements which act on layer 3 of the ISO/OSI reference model between different networks. The destination IP address is used to determine which network the packet should be forwarded to.
Routing	Process of determining the optimum path through networks for data transfer.
Routing table	The routing table contains the path information for devices. It provides the basis for determining the optimum path for the relevant packet.
RPI	The requested packet interval (RPI) is the time interval in an EtherNet/IP™ network at which a device requests its packets.

RS-232 interface	The RS-232 interface is defined in American standard EIA-232 and in international standard CCITT V.24. This serial interface carries out data exchange between two devices in full duplex mode (point-to-point connection). The maximum transmission speed is 115.2 kbps and the maximum transmission distance is 15 m. See DCE, DTE
RS-485 interface	The RS-485 interface is defined in American standard EIA-485. This serial interface provides the option of establishing multipoint connections with up to 32 devices. The transmission speed is 12 Mbps maximum and the transmission distance is 1200 m maximum. There are RS-485 interfaces in 2-wire and 4-wire technology. For 2-wire technology, data can be transmitted in half duplex mode; for 4-wire technology, data can be transmitted in full duplex mode.
RSTP	The Rapid Spanning Tree Protocol (RSTP) is a redundancy mechanism according to IEEE 802.1D-2004 which supports any topology.
RTU	Remote terminal unit (RTU) refers to devices that are used for remote control in power generation and power transmission systems as well as process technology systems. They perform control, measurement or regulation functions and are in contact with the control center and control level.

S

SAS	A substation automation system (SAS) handles the automation of energy systems (e.g., switchgear, substations). It is used for communication between intelligent electronic devices (IEDs) as well as communication with and within the control level.

SAV / SV	Sampled analog values or sampled values for short is an Ethernet protocol which is transmitted via layer 2 and transmits special analog sample values in IEC 61850 communication.
SCADA	Supervisory Control and Data Acquisition (SCADA) refers to systems for controlling and visualizing processes.
SCL	System Configuration Language – XML-based, object-oriented description language according to IEC 61850.
SCRJ	Interface module for use on the Modular Managed Switch with diagnostic function and connection options for polymer fibers or HCS fibers.
SD card	An SD card (Secure Digital memory card) is a digital storage medium which works according to the principle of Flash storage.
Server	A server is a hardware or software component which makes services available to a client. The server is always the service provider.
Session layer	Layer 5 in the OSI model – this layer ensures the control structure of the session between two applications via the network, such as opening and closing a session.
SFP module	Small form factor pluggable module – an SFP module is an optical interface for the flexible use of various fiberglass modules. The standardized interfaces for Gigabit applications can be replaced during operation.
SFP SX module	Optical transceiver. Wavelength: 850 nm; transmission distance: 550 m for 50/125 µm fiberglass, 300 m for 62.5/125 µm fiberglass.

SFP LX module	Optical transceiver. Wavelength: 1310 nm; transmission distance: 30 km for 9/125 µm fiberglass, 250 m for 62.5/125 µm fiberglass.
SFP LX LH module	Longhaul module – optical transceiver used in conjunction with single-mode fibers and for transmission over very long distances. Wavelength: 1550 nm; transmission distance: 80 km for 9/125 µm fiberglass.
Single-mode module	Also: LX module. Optical transceiver used in conjunction with single-mode fibers and for transmission over long distances.
SMA / RSMA	Compact, screwable connection standard for antennas (antenna cables); SMA and RSMA can only be connected via an adapter.
Smart mode	For easy configuration, Smart Managed Switches from Phoenix Contact provide a mode in which it is possible to change the operating state without using additional tools or user interfaces such as CLI, web-based management or SNMP.
SMTP	The Simple Mail Transfer Protocol (SMTP) is a protocol which is used to transmit e-mails – mainly to supply and forward e-mails in computer networks.

SNMP	The Simple Network Management Protocol (SNMP) is manufacturer-independent standard for Ethernet management. SNMP consists of three parts: the protocol itself, the Structure of Management Information (SMI), and the Management Information Base (MIB). The protocol transfers the data, which is defined and collected by the SMI and MIB.
SNMP trap	SNMP traps are alarms or event messages which are transmitted with maximum priority to various addresses, if required, and can then be displayed by the management station in plain text.
SNTP	The Simple Network Time Protocol (SNTP) is a protocol for time synchronization with an accuracy of 1 to 50 ms.
SOHO	Network solutions and Internet access technologies for small offices or home offices.
Spanning Tree algorithm	Spanning Tree is a method for suppressing loops in (redundantly) connected networks. The physically redundant network structures are determined and a loop-free structure is created by disconnecting specific ports. This measure reduces active connection paths in a freely meshed structure. The resulting tree structure has two essential properties: all networked points (ports) are connected by means of just one path. The algorithm is implemented in the relevant devices, and each switch uses defined quality criteria to calculate the path to the root switch. Possible quality criteria include distance, capacity, costs, load, etc.

SSH	Secure Shell (SSH) is a program or network protocol for establishing an encrypted network connection to remote devices.
S/STP	Screened Shielded Twisted Pair – twisted pair cable with pair shield as wire mesh and overall shield as foil.
Static routing	In the case of static routing, the paths are entered manually.
ST connector	Registered trademark of AT&T See B-FOC connector
Store-and-forward switching	Switching technology where the entire data packet is read and checked for errors before it is forwarded.
Storm control	Broadcast, multicast, and unicast bandwidth limits.
STP	Shielded Twisted Pair (STP) is a twisted pair cable with shielding.
Subnet mask	The subnet mask specifies which part of the IP address is used as the subnet address. Example: in a Class A network (subnet mask 255.0.0.0), the first field of the IP address is the subnetwork. The IP address is 207.142.2.1, which means the subnet address is 207.0.0.0 and the device address is 142.2.1.
Switch	Switches connect areas of the network which operate at different speeds, for example, or keep areas with very high traffic separate from other areas of the network. The switch can determine the area of the network to which data packets are addressed and only forwards them to another segment if required. This increases the total useful bandwidth of the network.

T

TAG field	An optional field in the Ethernet telegram which contains information on the priority of user data and assignment to a VLAN.
TCP	The Transmission Control Protocol (TCP) uses IP and ensures that data is correct and data packets are transmitted in the right order.
TCP/IP stack	Part of an operating system or driver which provides all the drivers and functions required to support the IP protocol.
Telnet	Terminal over Network – Telnet is a standard protocol which is used to establish an interactive connection to other devices via Ethernet. Telnet uses TCP/IP as its transmission and data link protocol.
TFTP	The Trivial File Transfer Protocol (TFTP) is a protocol that is suitable for transmitting complete files and uses a minimum of commands such as “read” or “write”. TFTP is mainly used for configuring networks or loading operating systems.
TIA/EIA	Telecommunications Industry Association/Electronic Industries Association – American associations for standardization in the private sector.
TKIP	Security protocol for encryption, e.g., for WLANs. The security level is adequate, but is not as high as AES.
TP	See Twisted pair
Transmission speed	The transmission speed refers to the number of bits transmitted per unit of time. In the case of Ethernet, the following transmission speeds currently apply: 10, 100, 1000, and 10,000 Mbps.

Transport layer	Layer 4 in the OSI model – this layer makes sure that the data is transmitted reliably in the network. It provides a logical connection between both end systems of the network, thereby ensuring error-free transport.
Trap targets	Trap targets are the targets which evaluate traps (alarm or event messages).
Trunking	See Link aggregation
Tunneling	Tunneling is also known as encapsulation and describes the encapsulation of data into a data packet of another protocol of the same OSI layer.
Twisted pair	Data cable in which pairs of data wires are twisted together. Twisting the forward and return lines greatly reduces the crosstalk ratio. A distinction is made between STP (Shielded Twisted Pair) and UTP (Unshielded Twisted Pair).
TX	TX is the abbreviation for transmitter and is used to identify the transmit port on a device.

U

UDP	The User Datagram Protocol (UDP) is a wireless protocol which is based on IP but does not use any security measures. UDP supports higher speeds for data transmission.
UNICAST	UNICAST refers to a message for a specific recipient in the network.
UPS	Uninterruptible power supply

USB	Universal Serial Bus (USB) is a serial interface for connecting external devices such as hard disks, keyboards, mice or USB sticks to a computer.
UTP	Unshielded Twisted Pair (UTP) is an unshielded twisted pair cable.

V

VLAN	A Virtual Local Area Network (VLAN) is a virtual network for the creation of separate logical networks which can be connected together physically.
VPN	A Virtual Private Network (VPN) connects several separate networks together via a public network, e.g., the Internet. Cryptographic protocols are used to ensure confidentiality and authenticity.
VRRP	Virtual Router Redundancy Protocol – a protocol which, for reasons of redundancy, combines several routers to create a virtual router.

W

WAN	A Wide Area Network (WAN) is a network of computers, without spatial restrictions and can be distributed nationally or internationally.
WEP	Wired Equivalent Privacy – encryption method based on RC4 for Wireless LAN (note: WEP is completely compromised).

WEP 64-bit	Wired Equivalent Privacy – encryption method based on RC4 for Wireless LAN (note: WEP is completely compromised). The key length is 64 bits.
WEP 128-bit	Wired Equivalent Privacy – encryption method based on RC4 for Wireless LAN (note: WEP is completely compromised). The key length is 128 bits.
Wi-Fi	The Wi-Fi Alliance is an association of companies with the objective of improving interoperability between various devices with wireless interfaces. In many countries, Wi-Fi is used as a synonym for WLAN.
Wireshark	Analysis tool (freeware) for networks which allows network traffic to be recorded and evaluated.
WLAN	A Wireless Local Area Network (WLAN) is a wireless network which operates without cables/lines according to IEEE standards.
WPA	Wi-Fi Protected Access (WPA) is an authentication method with dynamic key exchange. WPA1 is based on RSA RC4 and WPA2 is based on AES.
WPA2	Wi-Fi Protected Access 2 (WPA2) is the implementation of a security standard for wireless networks according to WLAN standards IEEE 802.11a, b, g, and n, and it is based on the Advanced Encryption Standard (AES). It is the successor to WPA, which itself is based on Wired Equivalent Privacy (WEP) now no longer considered secure. WPA2 implements the fundamental functions of the new IEEE 802.11i security standard.
WPAN	A Wireless Personal Area Network (WPAN) is a special type of PAN which uses communication via short wireless paths to avoid short-range cabling.

X

XML	Extensible Markup Language (XML) is a meta language for displaying hierarchically structured data in the form of text files. XML is preferably used for data exchange between different IT systems.

IEEE standards

The IEEE 802 standards from the Institute of Electrical Engineers serve as the basis for non-proprietary standardization in network technology. The most important network standards for Ethernet are listed below.

IEEE 802.1 – LAN	
802.1D	Spanning Tree Protocol
802.1p	Traffic Class Expediting and Dynamic Multicast Filtering (published in 802.1D-1998)
802.1q	Virtual Bridge LANs
802.1s	Multiple Spanning Tree Protocol
802.1w	Rapid Spanning Tree Protocol
802.1X	Port Based Network Access Control
802.1AB	Link Layer Discovery Protocol

IEEE 802.3 – CSMA/CD	
802.3a	10Base2
802.3i	10Base-T
802.3j	10Base-F
802.3u	Fast Ethernet
802.3x	Full Duplex and Flow Control
802.3z	Gigabit Ethernet over glass fiber
802.3ab	Gigabit over UTP
802.3ad	Link aggregation

802.3ae	10 Gigabit Ethernet
802.3an	10GBase-T
802.3af	Power over Ethernet

IEEE 802.11 – Wireless LAN

802.11a	Extension: up to 54 Mbps data rate, 5 GHz band, OFDM
802.11b	Extension: up to 11 Mbps data rate, 2.4 GHz ISM band, DSSS/CCK
802.11g	Extension: up to 54 Mbps data rate, 2.4 GHz ISM band, OFDM, DSSS
802.11h	Adjustment for transmission power (TCP) and frequency management (DFS) to meet the requirements of the 5 GHz band.
802.11n	Enables an increase of the data rate up to 300 Mbps when using channel bundling up to 600 Mbps (in the 2.4 GHz or 5 GHz band).
802.11i	The standard offers secure data encryption when using WPA2 with "pre-shared keys". AES (Advanced Encryption Standard) for additional data encryption is also part of the standard.
802.11d	International (country-to-country) roaming. Adjustment to the regulatory conditions of various countries.
802.11e	Support for QoS
802.11f	Inter Access Point Protocols for supporting interoperability between base stations.

IEEE 802.15 – Wireless PAN

IEEE 802.15.1	Bluetooth

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: + 49 5235 3-00
Fax: + 49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

ION01-14.000.L3
MNR 32003752/2014-05-27/03

INSPIRING INNOVATIONS