

GLOSSARY

Industrial Ethernet



Industrial Ethernet Glossary

Industrial Ethernet communication Protocols

Ethernet is becoming ubiquitous and cost-effective, with common physical links and increased speed. As such, many industrial communication protocols are moving to Ethernet-based solutions. Ethernet communications with TCP/IP typically are nondeterministic, and reaction time is often around 100 ms. Industrial Ethernet protocols use a modified Media Access Control (MAC) layer to achieve very low latency and deterministic responses. Ethernet also enables a flexible network topology and a flexible number of nodes in the system. Let's look at some of the popular Industrial Ethernet protocols in detail.

EtherCAT, a protocol optimized for process data, uses standard IEEE 802.3 Ethernet Frames. Each slave node processes its datagram and inserts the new data into the frame while each frame is passing through. The process is handled in hardware so each node introduces minimum processing latency, enabling the fastest possible response time. EtherCAT is the MAC layer protocol and is transparent to any higher-level Ethernet protocols such as TCP/IP, UDP, Web server, etc. EtherCAT can connect up to 65,535 nodes in a system, and EtherCAT master can be a standard Ethernet controller, thus simplifying the network configuration. Due to the low latency of each agent node, EtherCAT delivers flexible, low-cost and network-compatible industrial Ethernet solutions.

EtherNet/IP is an application-layer protocol on top of TCP/IP. EtherNet/IP uses standard Ethernet physical, data link, network and transport layers while using Common Industrial Protocol (CIP) over TCP/IP. CIP provides a standard set of messages and services for industrial automation control systems, and it can be used in multiple physical media. For example, CIP over CAN bus is called DeviceNet, CIP over the dedicated network is called ControlNet and CIP over Ethernet is called EtherNet/IP. EtherNet/IP establishes communication from one application node to another through CIP connections over a TCP connection, and multiple CIP connections can be established over one TCP connection.

PROFINET is a widely used industrial Ethernet by major industrial equipment manufacturers such as Siemens and GE. It has three different classes. PROFINET Class A provides access to a PROFIBUS network through a proxy, bridging Ethernet and PROFIBUS with a remote procedure calling ON TCP/IP. Its cycle time is around 100 ms, and it is

mostly used for parameter data and cyclic I/O. The typical application includes infrastructure and building automation. PROFINET Class B, also referred as PROFINET Real-Time (PROFINET RT), introduces a software-based real-time approach and has reduced the cycle time to around 10 ms. Class B is typically used in factory automation and process automation. PROFINET Class C (PROFINET IRT), is Isochronous and real-time, requiring special hardware to reduce the cycle time to less than 1ms to deliver sufficient performance on the real-time industrial Ethernet for motion control operations. PROFINET RT can be used in PLC-type applications, while PROFINET IRT is a good fit for motion applications. Branch and Star are the common topologies used for PROFINET. Careful topology planning is required for PROFINET networks to achieve the required performance of the system.

POWERLINK was originally developed by B&R. Ethernet POWERLINK is implemented on top of IEEE 802.3 and, therefore, allows a free selection of network topology, cross-connect and hotplug. It uses a polling and time slicing mechanism for real-time data exchange. A POWERLINK master or "Managed Node" controls the time synchronization through packet jitter in the range of 10s of nanoseconds. Such a system is suitable for all kinds of automation systems ranging from PLC-to-PLC communication and visualization down to motion and I/O control. Barriers to implementing POWERLINK are quite low due to the availability of open-source stack software. In addition, CANopen is part of the standard which allows for easy system upgrades from previous Fieldbus protocols.

Sercos III is the third generation of the Serial Realtime Communication System (Sercos). It combines on-the-fly packet processing for delivering real-time Ethernet and standard TCP/IP communication to deliver low latency industrial Ethernet. Much like EtherCAT, a Sercos III slave processes the packet by extracting and inserting data to the Ethernet frame on-the-fly to achieve low latency. Sercos III separates input and output data into two frames. With cycle times from 31.25 microseconds, it is as fast as EtherCAT and PROFINET IRT. Sercos III supports ring or line topology. One key advantage to using ring topology is communication redundancy. Even if the ring breaks due to the failure of one slave, all remaining slaves still get the Sercos III frames with input/output data. Sercos III can have 511 slave nodes in one network and is most used in servo drive controls.

Time-sensitive networking (TSN) is an Ethernet extension defined by the Institute of Electrical and Electronics Engineers (IEEE) designed to make Ethernet-based networks more deterministic. TSN is a local area network (LAN)-a level solution that can work with non-TSN Ethernet, but timeliness is only guaranteed inside the TSN LAN. You can group TSN standards based on what use case it solves: a common view of time, guaranteed maximum latency, or co-existence with background or other traffic. Like any popular standard, the TSN toolbox of standards is evolving.

Ethernet Terms

Industrial Ethernet can also refer to the use of standard Ethernet protocols with rugged connectors and extended temperature switches in an industrial environment, for automation or process control.

Numbers

4B/5B

A block encoding scheme is used to send Fast Ethernet data. In this signal encoding scheme, 4 bits of data are turned into 5-bit code symbols for transmission over the media system.

4D/PAM5 (aka PAM-5)

The encoding scheme used for 1000BASE-T over four twisted-pair links has high bandwidth utilization. It uses four signalling levels for data and one level for forwarding error correction.

8B/10B

The 8B/10B encoder takes in 8-bit data and 1-bit control as input and converts them into a 10-bit output. The 8B/10B encoder automatically performs a running disparity check for the 10-bit output.

10BASE-T

10 Mbps Ethernet system based on Manchester signal encoding transmitted over Category 3 or better twisted-pair cable.

10BASE-FL

Popular 10 Mbps link fiber optic solution which replaces the older FOIRL implementation utilizing 850 nm fibre optic technology.

100BASE-FX

100 Mbps Fast Ethernet system based on 4B/5B signal encoding transmitted over fibre optic cable utilizing 1300 nm fibre optic technology.

100BASE-FX

100 Mbps Fast Ethernet system based on 4B/5B signal encoding transmitted over fibre optic cable utilizing 1300 nm fibre optic technology.

100BASE-TX

100 Mbps Fast Ethernet system based on 4B/5B signal encoding transmitted over two copper pairs.

100BASE-X

The term used when referring to any Fast Ethernet media system based on 4B/5B block encoding. Includes 100BASE-TX and 100BASE-FX media systems.

1000BASE-T

A standard for 1000 Mbps Ethernet communication over Category 5 UTP.

10GBASE-T

A standard that provides connections with the bandwidth of 10 Gbit/s and a maximum transmission distance up to 100 meters over the unshielded or shielded twisted pair cables.

10GBASE-SR/LR/LRM/ER/ZR

There are two basic types of optical fiber used for 10 Gigabit Ethernet: single-mode (SMF) and multimode (MMF).[20] In SMF light follows a single path through the fiber while in MMF it takes multiple paths resulting in differential mode delay (DMD). SMF is used for long-distance communication and MMF is used for distances of less than 300 m.

802.3 IEEE

The CSMA/CD group is the oldest working group in the 802 project. It defines the norms according to the CSMA/CD access procedures proposed by the DIX-group. This working group focuses on discussing high-speed protocols.

802.1x

802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network

Α

Address Resolution Protocol (ARP)

A TCP/IP protocol for obtaining the physical address (MAC) of a node when the Internet address is known.

Applet

A computer program for creating an active Web document - usually written in Java.

Application Layer (Layer 7 in the OSI model)

This is the highest OSI layer in which networking

application software interfaces with the human operator and uses underlying protocols to establish host-to-host connections. Examples include a Web browser, an email application, Telnet and a building management system application.

Application Programming Interface (API)

The information is followed by programmers to write client-server programs.

Asynchronous Transmission

Transfer of data with start/stop bits and a variable time interval between data units.

AUI

Attachment Unit Interface. The 15-pin signal interface defined in the original Ethernet standard that carries signals between a station and an outboard transceiver.

Authentication

Verification of the identity of the sender of a message - usually with a username and a password.

Auto-Negotiation

An Ethernet standard protocol allows devices at either end of a link to advertise and negotiate modes of operation such as the speed, half-or fullduplex operation and full-duplex flow control.

Auto-MDIX (Auto-Crossover)

A protocol allowing two Ethernet devices to negotiate their use of the Ethernet TX and RX cable pairs so two Ethernet devices can connect whether using a crossover cable or a straight-through cable.

В

Backbone

A network that joins smaller networks together.

Bandwidth

The maximum capacity of a network channel. Usually expressed in bits per second (bps). Ethernet channels have bandwidths of 10, 100, or 1000 Mbps.

Baud

A unit of signalling speed represents the number of discrete signal events per second and, depending upon the encoding, can differ from the bit rate.

Best-Effort Delivery

In IP, a transmission mechanism that does not guarantee message delivery.

Bit

A binary digit. The smallest unit of data, either a zero or a one.

Bit Rate

The amount of bits that can be sent per second. Usually described in units of kbps or Mbps and frequently referred to as the data rate.

Block Encoding

A system in which data bits are encoded as code bits to ensure synchronization and detection of errors used in Fast Ethernet and Gigabit Ethernet.

Blocking

The condition in which a switching network is working at its full capacity and cannot accept more input.

Blocking Port

In STP and RSTP, a switch port that does not forward frames.

Bridge

A device with filtering and forwarding capabilities that connects two or more networks at the Data link Layer.

Broadcast

A transmission is initiated by one station and sent to all stations on the network.

Browser

An application that displays a Web document - typically with the aid of other Internet services.

Bus

A shared connection for multiple devices over a cable or backplane.

Byte

A unit of digital information - usually 8 bits. Originally, the bits needed to encode a text character. Historically, it was hardware dependent with no standard size. The term octet (8 bits) arose due to the ambiguity of the size of a byte.

С

Cable Modem

A device integrating switch and modem functions to deliver broadband Internet via coaxial cable to a local network.

Cache

Small, fast memory for holding data that is being processed.

Category 5

Twisted-pair cable with characteristics suitable for all twisted-pair Ethernet media systems - including 10BASE-T, 100BASE-TX and 1000BASE-T. Category 5 and Category 5e cable are preferred cable types for structured cabling systems.

Category 5e

An enhanced version of Category 5 cable, developed to improve certain cable characteristics important to Gigabit Ethernet operation. It is recommended that all new structured cabling systems be based on Category 5e cable; however, this cable may not be the best for use in industrial installations because of noise susceptibility.

Channel

A communications pathway.

Checksum

An error detection value is derived from the sum of a bitstream.

Circuit Switching

Using a dedicated path to establish an electrical connection between stations.

Cladding

The glass or plastic surrounding the core of an optical fiber.

Client

A computer or application that obtains services from another machine, is called the server.

Client Process

A local program process that requests service from a remote application.

Client-Server Model

The communication model in which a client program requests service from a server.

Collision

The result of having two or more simultaneous transmissions on a common signal channel such as half-duplex Ethernet or shared Ethernet.

Collision Domain

The set of all stations is connected to a network where faithful detection of a collision can occur. A collision domain terminates at a switch port.

Core

The glass (or, rarely, plastic) centre of an optical fiber.

CRC

Cyclic Redundancy Check. An error-checking technique used to ensure the fidelity of received data.

Crossover Cable

Twisted-pair patch cable wired so as to route the transmit signals from one piece of equipment to the receive port of another piece of equipment, and vice versa. This allows communication between two peer devices. The opposite of a crossover cable is the straight-through cable.

Crosstalk

Line noise is caused by signals from another nearby (usually parallel) line.

Cut-Through Switching

An ethernet switch that uses cut-through switching can make a forwarding decision as soon as it gets the first couple of bytes of the incoming frame. The switch does not have to wait for the rest of the frame to start switching the frame to the outgoing port.

CSMA/CD

Carrier Sense Multiple Access/Collision Detect. The medium access control (MAC) Protocol is used in Ethernet.

D

Datagram

In packet switching, a basic data unit in which delivery is not guaranteed. It contains a *header* (source and destination addresses and a type field) and *data*. See User Datagram Protocol (UDP).

Data Link Layer (Layer 2 of the OSI model)

Communicates between the Network and Physical layers using data groups called *frames*. Aka just the *Link Layer*, it is divided into sublayers for Media Access Control (MAC) and Logical Link Control (LLC)

DCE (Data Communications Equipment)

Any equipment that relays data between Data Terminal Equipment (DTE). DCEs are not considered end devices or stations.

DDoS

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.

DHCP

See Dynamic Host Configuration Protocol.

DiffServ (Differentiated Services)

A layer-three QoS method is described in RFCs 2474 and 2475. It uses the 8-bit *ToS* field in an IP frame.

Digital Data

Data is represented by discrete values or conditions.

Digital Subscriber Line (DSL)

A technology using legacy telecommunication networks to achieve high-speed data delivery.

Dotted-Decimal Notation

An IP address version that is easier for humans to read. Each byte is converted to a decimal equivalent then separated from its neighbour by a dot.

Download

To transfer data from a remote site to a local one or from a server to a client.

DNS Server

A computer that converts user-friendly names into corresponding IP addresses that identify computer systems or resources in a network or on the Internet.

DTE

Data Terminal Equipment. Any piece of equipment at which a communication path begins or ends. A station (computer or host) on the network is capable of initiating or receiving data.

Dynamic Host Configuration Protocol (DHCP)

A protocol that allows a server to automatically assign an IP address to a subscribing device.

Ε

Electromagnetic Interference (EMI)

Also called radio frequency interference (RFI). Electromagnetic energy (usually from an external source) disturbs the data-handling properties of the affected equipment. The source may artificial (such as electrical equipment) or natural (such as radiation from the Sun).

Encapsulation

Placing a lower protocol message into the data field of a higher protocol to utilize the enhanced transportation capability of the higher protocol.

Encoding

A means of combining clock and data information into a self-synchronizing stream of signals.

Error Detection

A method that detects errors in received data by examining cyclic redundancy checks (CRC) or checksum.

Ethernet

A popular LAN technology was first standardized by DEC, Intel, and Xerox (or DIX) and later standardized

by the IEEE 802.3 committee. It operates at the physical and data link layers of the OSI model.

ERPS

Ethernet Ring Protection Switching (ERPS) is a standardized approach to network design. It enables large amounts of Ethernet traffic to flow to multiple connection points with high-level redundancy. There are several ways to implement ring networking topographies, but with Ethernet, ITU-T G.8032 is the gold standard. When used correctly, G.8032 management protects Ethernet traffic and maintains recovery times under 50 milliseconds (ms).

ERPSv2

ITU-T G.8032v2 specifies protection switching mechanisms and a protocol for Ethernet layer network (ETH) Ethernet rings. Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in ITU-T G.8032v2 are highly reliable with stable protection and never form loops, which would negatively affect network operation and service availability. Each ring node is connected to adjacent nodes participating in the same ring using two independent paths, which use ring links (configured on ports or LAGs). A ring link is bounded by two adjacent nodes and a port for a ring link is called a ring port. The minimum number of nodes on a ring is two.

F

Fast Ethernet

A version of Ethernet that operates at 100 Mbps. Although 100 Mbps is no longer the fastest data rate, this term is still used.

Fast Link Pulse

A link pulse that encodes information used in the Auto-Negotiation Protocol. Fast link pulses consist of bursts of the normal link pulses used in 10BASE-T.

Fiber Optic Cable

A cable with a glass or plastic filament which transmits digital signals in the form of light pulses at wavelengths of 850 nm (10BASE-FL and 100BASE-SX) or 1300 nm (100BASE-FX).

Fiber Optic Connector Intermateability Standards (FOCIS)

A set of standards of the Telecommunications Industry Association that insures proper mating of fiber connectors. FOCIS documents are in the series *TIA/EIA-604-XX*.

Firewall

Security firmware (usually in a router) to safeguard

one network from another - typically separating a local network from the Internet.

Flow Control

The process of controlling data transmission at the sender to avoid overfilling buffers and loss of data at the receiver.

FOIRL

Fiber Optic Inter-Repeater Link. An early version of fiber optic link segment. FOIRL was replaced by 10BASE-FL.

Forwarding

The process of moving frames from one port to another in a switching hub.

Frame

The fundamental unit of transmission at the data link layer of the OSI model.

Full-Duplex Operation

A communication method that allows simultaneous transmission and reception of data.

G

Gateway

A device that exchanges data between two networks that use different communication protocols.

Gigabit Ethernet (aka GbE or 1 GigE)

A version of Ethernet that operates at 1000 Mbps.

Н

Half-Duplex Operation

A communication method in which transmissions and receptions can occur in either direction but not at the same time.

Host (Node)

A station on a network.

Hub

A DCE with three or more ports at the centre of a star topology network. Hubs can usually be cascaded with a hub-to-hub connection. Frequently this name is used to mean repeating hub.

Hypertext

Text that transfers the application focus to other documents via hyperlinks.

Hypertext Markup Language (HTML)

Computer language specifying the content and format of a Web document.

Hypertext Transfer Protocol (HTTP)

Application service for retrieving a Web document.

I

IEEE

Institute for Electrical & Electronics Engineers. A professional organization and standards body.

IGMP Snooping

The ability of a switch to observe Internet Group Multicast Protocol (IGMP) traffic in order to learn IP Multicast group membership for the purpose of restricting multicast transmissions to only those ports which have requested them.

Interface

A means of communicating between components or technologies - involving either hardware (such as a graphics card) or software (such as a browser) or both.

Internet

A worldwide collection of networks based on the use of TCP/IP network protocols. The most common example of an *Internetwork*.

Internet Protocol (IP)

The Network-Layer protocol in the TCP/IP protocol suite provides unguaranteed (connectionless) data exchanges across packet switching networks.

Internet Protocol Suite

The collection of protocols that are used for Internet messaging. The two main protocols are TCP (Transmission Control Protocol) and IP (Internet Protocol). It is commonly called TCP/IP but includes several more protocols.

Internetwork

A network of networks - connected with devices such as routers and gateways.

Intranet

A private network that uses the TCP/IP protocol suite.

ISP

Internet Service Provider.

J

Jumbo Frame

Jumbo frames are Ethernet frames with more than 1500 bytes of payload, the limit set by the IEEE 802.3 standard. Commonly, jumbo frames can carry up to 9000 bytes of payload, but smaller and larger variations exist and some care must be taken using the term. Many Gigabit Ethernet switches and Gigabit Ethernet network interface controllers and some Fast Ethernet switches and Fast Ethernet network interface cards can support jumbo frames. The act of continuously sending data. A jabbering station is one whose circuitry or logic has failed, and which has locked up a network channel with its incessant transmissions.

Java

A programming language used to create interactive Web documents.

L

LAN (Local Area Network)

A network of limited geographical area, high datatransfer rates and no need for leased telecommunication lines - unlike Wide Area Networks (WANs) that typically connect to the Internet.

Late Collision

A failure of the network in which the collision indication arrives too late in the frame transmission to be automatically dealt with by the medium access control (MAC) Protocol. The defective frame may not be detected by all stations requiring that the application layer detect and retransmit the lost frame, resulting in greatly reduced throughput.

Layer 3 Switch (L-3 Switch)

An unofficial marketing term for a device that can route IP messages within an organization but lacks full router functionality - such as a WAN port and firewall that are unneeded for internal routing.

LC (Lucent Connector, aka "Little Connector")

A fiber optic connector which resembles a small <u>SC</u> connector. Both simplex and duplex form factors are in common use. The duplex connector houses both transmit and receive channels in the same assembly. Named after Lucent Technologies which developed it. Standardized in TIA/EIA-604-10 (FOCIS 10).

Link Integrity Test

This test verifies that an Ethernet link is connected correctly and that signals are being received correctly. This is a helpful aid but does not guarantee the link is completely functional.

Link Layer

Short for Data Link Layer. This is layer 2 on the OSI model.

Link Pulse

A test pulse sent between transceivers on a 10BASE-T link segment during periods of no traffic, to test the signal integrity of the link.

Link Segment

A point-to-point segment that connects only two devices and is "capable" of supporting full-duplex operation. Commonly shortened to just *Link*.

Local Access

Using a terminal directly connected to a computer or networking device such as a switch. Since the access does not use a network signal path, greater communication security is provided.

Link Aggregation Control Protocol

Within the IEEE Ethernet standards, the Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical links together to form a single logical link. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to their peer, a directly connected device that also implements LACP.

Μ

MAC

Medium Access Control. A Protocol operating at the data link layer used to manage a station's access to the communication channel.

MAC Address

A unique address assigned to a station interface, identifying that station on the network. With Ethernet, this is the unique 48-bit station address. It is also known as the physical address.

Manchester Encoding

Signal encoding method used by all 10 Mbps Ethernet media. Each bit is converted into a "bit symbol" which is divided into a high half and a low half. This yields a 20 Mbaud stream although data is only sent at 10 Mbps.

Mask (Subnet Mask)

In a subnetted IP network, the value (common to all subnet hosts) that determines the subnet prefix value. Each host is then specified with the value of the rest of the IP address.

MAU

Medium Attachment Unit. The MAU provides the physical and electrical interface between an Ethernet device and the media system to which it is connected. It is also known as a transceiver.

MDI

Medium Dependent Interface. The name for the connector used to make a physical and electrical connection between a transceiver and a media

segment. For example, the RJ-45-style connector is the MDI for 10BASE-T and 100BASE-TX.

MDI-X

An MDI port on a hub or media converter that implements an internal crossover function. This means that a "straight-through" patch cable can be used to connect a station to this port, since the required signal crossover is performed inside the port instead of in the cable.

Mesh (Topology)

A network configuration in which each device has a dedicated point-to-point link to every other device.

MIB

Management Information Base. An MIB describes a set of managed objects. An SNMP management console application can manipulate the objects on a specific computer if the SNMP service has an extension agent DLL that supports the MIB. Each managed object in a MIB has a unique identifier. The identifier includes the object's type (such as counter, string, gauge or address), the object's access level (such as read, or read/write), size restrictions and range information.

MII

Medium Independent Interface. Similar to the original AUI function, but designed to support both 10 and 100 Mbps, an MII provides a 40-pin connection to outboard transceivers (also called PHY devices). Used to attach 802.3 interfaces (MACs) to a variety of physical media systems.

Media Converter

A device that converts signals from one media type to that of another.

Modem

A device that converts between digital and analogue signals.

Multicast

A transmission initiated by one station and sent to many stations on the network.

MSTP

The Multiple Spanning Tree Protocol (MSTP) and algorithm, provides both simple and full connectivity assigned to any given Virtual LAN (VLAN) throughout a Bridged Local Area Network.

Ν

NAT (Network Address Translation)

A technology allowing private addresses for internal communication and a Internet addresses for external communication.

Network

A system of connected nodes (hosts) that share data.

Network Layer (Layer 3 in the OSI model)

Provides switching and routing technologies creating logical paths for data exchange between nodes. IP is its most common protocol and IP addressing occurs at this layer.

NIC (Network Interface Card)

Also called an adapter, network interface module, or interface card. The electronic circuitry that connects a computer (node or host) to a network.

Node (aka Host)

An addressable network device (such as a computer or router) where data enters and exits a network.

Noise

Unwanted electromagnetic energy degrades the quality of the signal.

NTP

The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variablelatency data networks.

0

OPC

Originally, OLE for Process Control. A process control communications standard for accessing process data from multi-vendor systems.

OSI (Open Systems Interconnection)

A seven-layer reference model for networks was developed by the International Organization for Standardization (ISO). It describes the interlocking sets of networking hardware and software used to deliver network services. Although a good model, strict compliance is seldom accomplished.

OUI (Organizationally Unique Identifier)

A 24-bit value is assigned to an organization by the IEEE and used by Ethernet vendors as a core part of each unique 48-bit Ethernet address. Contemporary Controls has been assigned a vendor OUI.

Overhead

Control bits are added to the data.

P

Packet

A unit of data is exchanged at the network layer. This is a much-abused definition and the terms "frame" and "packet" are frequently interchanged.

Packet-Switched Network

A network in which data are exchanged using packets.

Packet Buffer

A packet buffer is memory space set aside for storing packets awaiting transmission over networks or storing packets received over networks.

PAM-5

See 4D/PAM5.

Parity

An error-detection method in which an extra bit (the parity bit) is added to the data so the sum of all 1bits becomes either odd (used in Odd Parity) or even (used in Even Parity).

Patch Cable

A twisted-pair or fiber optic jumper cable used to make a connection between a media segment and a network interface (on a station) or a network port (on a hub), or to directly connect stations and hub ports together.

Path

The channel through which a signal travels.

PAUSE

A unique frame is sent by full-duplex capable stations to indicate to the sender to slow down transmissions.

PHY

Physical Layer Device. The name is used for a transceiver in Fast Ethernet and Gigabit Ethernet systems.

Physical Address (MAC address)

The address of a device used at the Data Link layer. **Physical Layer (Layer 1 in the OSI model)** The lowest of the OSI layers, it converts physical impulses - electrical, light or radio - into networkusable data using data groups called *symbols*.

Ping (Packet InterNet Groper)

An Internet Control Message Protocol (ICMP) echo request to a specific host who responds by returning an echo. It is a simple, quick means of determining if a working signal path exists between the origin and destination devices. Some machines may not respond if Ping service is disabled or if a firewall gateway interferes.

Plenum Cable

Cable rated as having adequate fire resistance and satisfactorily low smoke-producing characteristics for use in plenums (air-handling spaces). Plenums are often located below machine room floors or above-suspended ceilings, requiring the use of plenum-rated cable.

Point-to-Point Topology

A network system composed of point-to-point links. Each point-to-point link connects two and only two devices-one at each end. Devices could be DTEs or DCEs, but no more than two can be connected on one link.

Poll

A procedure in which the primary station asks a secondary station if it has any data to transmit.

Port (Logical)

A number is associated with an IP address to identify a TCP or UDP channel endpoint for an application or process. This allows different activities to use the same IP address simultaneously. Well-known port numbers are reserved for common services - such as 21 for FTP or 80 for HTML.

Port (Physical)

A connection point for a cable. Repeater hubs and switching hubs typically provide multiple ports for connecting Ethernet devices.

Port Forwarding (Port Mapping)

A firewall modification allows an IP port from one network to be used in another network.

Port Mirroring

Port Mirroring allows a switch port to monitor packets from any or all of its ports so that traffic can be analyzed.

Port Security

Prevents a switch port from learning MAC addresses. Thus, frames pass through only if their destinations are listed in the switch address look-up table. Static addresses are not affected. This feature is typically used to limit device access to a network.

PPP (Point-to-Point Protocol)

A Data Link protocol for building a direct connection between two nodes with the options of authentication, encryption and compression.

PPPoE (Point-to-Point Protocol over Ethernet)

A protocol for encapsulating PPP frames within Ethernet frames. Used mainly with DSL services. It is described by RFC 2516.

PPTP (Point-to-Point Tunneling Protocol)

A method to achieve a VPN using TCP and a tunnelling protocol. Relying on PPP for security, no encryption or authentication is specified - but security is provided by the Windows PPTP stack.

Preamble

The first 7 bytes of an IEEE 802.3 frame - have alternating 1s and 0s that alert and synchronise the receiver.

Presentation Layer (Layer 6 in the OSI model)

In casual discussion, this function (aka the syntax layer) is seldom distinguished from the Application Layer. It translates data from machine-oriented to human-friendly for use at the Application Layer. An example would be the conversion from an EBCDICcoded text file to an ASCII-coded file.

Private Network

A network that is isolated from the Internet.

Promiscuous Mode

A mode of operation where a device receives all frames on a network regardless of their destination address. Typically used by network analyzer tools.

Propagation Delay

The signal transit time through a cable, network segment, or device. Important in making collision domain calculations.

Protocol

A set of agreed-upon rules and message formats for exchanging information among devices on a network.

Q

Quality of Service (QoS)

Some switches support QoS (per 802.1p and 802.1Q standards) whereby tagged measures or messages received on a certain port can be assigned one of eight levels of priority. QoS can be important where time-critical applications can be impaired by data delays.

R

Rapid Spanning Tree (RSTP)

A newer version of Spanning Tree Protocol that is backward compatible while providing a faster recovery time.

RARP (Reverse Address Resolution Protocol)

A TCP/IP protocol for obtaining the Internet address of a node when the physical (MAC) address is known.

RMON

Remote network monitoring (RMON) is the process of monitoring network traffic on a remote Ethernet segment to detect network issues such as dropped packets, network collisions and traffic congestion.

Rate Limiting

The ability of a switch to limit the throughput of

www.fiberroad.com

particular ports on the switch. Used to prevent certain ports from consuming all the bandwidth.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a client-server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

Redundant Cabling

Standby (back-up) cabling is designed to carry network traffic if the primary signal path fails. Since a redundant path creates an unacceptable loop in Ethernet messaging, the redundant path must be deactivated until needed.

Remote Access

Using a terminal that is not directly connected to a computer or networking device such as a switch. Since the access uses a network signal path, less communication security is provided.

Remote Host

A computer accessed by someone at a different computer.

Repeater

A physical layer DCE is used to interconnect segments within the same network. An Ethernet repeater can only link Ethernet segments that are all operating in half-duplex mode and at the same speed. Some repeaters offer media conversion as well.

Repeating Hub

A repeater with more than two ports. This name is frequently shortened to simply "hub".

RJ-45

An 8-pin modular connector used on twisted-pair links.

Route

A path travelled by a packet.

Router

An internetworking device attached to two or more networks (or subnet) for forwarding packets from one network (or subnet) to another.

S

SC (Subscriber Connector)

A type of fiber optic connector used in 100BASE-FX fiber optic media systems. It is designed to be pushed into place and automatically seat itself. It was standardized in TIA/EIA-604-3.

Segment

A cable is made up of one or more cable sections and connections joined together to produce the equivalence of a continuous cable.

Segmentation

Splitting a message into multiple packets; is usually performed at the transport layer.

Server

A computer or application that provides services to other machines, called clients.

Session Layer (Layer 5 in the OSI model)

This layer is seldom distinguished from the Application Layer. It coordinates communication session connections between applications.

Shielded Twisted Pair (STP)

Twisted-pair cable wrapped in a foil or mesh shield that protects against electromagnetic interference. Its use is controversial because it can impart greater signal immunity if properly installed, but it can degrade reliability if improperly installed.

SSL

SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol.

Signal

An electronically encoded message is carried from a transmitter to a receiver through a communications channel where it is decoded for subsequent use.

Signal-to-Noise Ratio (SNR)

Signal strength is divided by noise, both in decibels.

Slot Time

A unit of time used in the medium access control (MAC) Protocol for Ethernet.

SNMP (Simple Network Management Protocol)

The de facto standard for switch management. A familiarity with MIB objects is necessary to manage a switch with an SNMP management program. SNMP is not necessarily limited to TCP/IP networks.

SNMP Trap

SNMP Traps are the most frequently used alert messages sent from a remote SNMP-enabled device (an agent) to a central collector, the "SNMP manager."

SNMPv3

SNMPv3 provides security with authentication and privacy, and its administration offers logical contexts, view-based access control, and remote configuration.

Socket (Logical)

An IP channel endpoint – is specified by the combination of an IP address and a port (which serves this particular channel) into a single identity. Example: 1.2.3.4:80.

Spanning Tree Protocol (STP)

A link management protocol provides path redundancy and prevents network loops by defining a tree to span all switches in a network. It forces redundant data paths into a standby (blocked) state. If a path malfunctions, the topology is reconfigured and the link re-established by activating the standby path.

ST (Straight Tip)

A type of fiber optic connector used in 10BASE-FL and FOIRL links, but also in 100BASE-TX links. The male portion has an inner sleeve with a slot cut into it, and an outer ring with a bayonet latch. The inner sleeve is aligned with a mating key in the socket and the outer ring is turned to complete the bayonet latch. It was standardized in TIA/EIA-604-2 (FOCIS 2).

Star Topology

A network topology in which each station on the network is connected directly to a hub. If multiple hubs are present, the topology is called a *distributed star*.

Straight-Through Cable

A cable where connections at both ends are pinned the same way. Used to interconnect non-peer devices such as a hub to a station. **Station**

·

A unique, addressable device on a network. Sometimes referred to as a node.

Subnet (Subnetwork)

The practice of logically subdividing an IP network is called subnetting. All hosts on a subnet share identical values in the most-significant bits of their IP address - creating two fields: a common network or routing prefix and the rest of the address which uniquely identifies each host.

Switching Hub

A switching hub is another name for a bridge; a DCE that interconnects network segments at the data link layer. Switching hubs are typically located in the centre of a star topology, and provide multiple ports for connections to network stations. Frequently this name is shortened to switch.

Switched Ethernet

An Ethernet LAN that uses switches (instead of repeating hubs) to direct a message to its destination.

Store and Forward

In this switching method, the frame has to be received entirely before a forwarding decision is made based on destination MAC address lookup. Once received and buffered, the switch will compare the FCS field of the frame against its frame-checksequence (FCS) calculations to ensure the integrity and correctness of the data.

SNTP

SNTP is a simplified access strategy for servers and clients using NTP. SNTP synchronizes a computer's system time with a server that has already been synchronized by a source such as a radio, satellite receiver or modem.

Т

Table

A collection of address/port associations that allows a switch or router to pass network traffic to the proper destination.

TCP (Transmission Control Protocol)

A core protocol of the Internet Protocol Suite.

TCP/IP (TCP/IP Suite)

A common casual name for the Internet Protocol Suite and so-named because its principal protocols are TCP (Transmission Control Protocol) and IP (Internet Protocol) - although many more protocols are involved.

Terminator

A device to prevent signal reflection at the end of a cable.

TELNET (Terminal Network)

An Application Layer protocol that provides interactive text-oriented communications using a virtual terminal connection. Useful for remote login.

Throughput

The number of bits passing through a point in one second.

TIA-568A and TIA-568B

Two standards are used to define RJ-45 pin connectors and wire colour-coding schemes. **Topology**

The physical layout of a network.

TOS (Type of Service)

A type of priority using the second octet (the TOS field) of the IP frame header. ToS priority is now largely superseded by *DiffServ*, but is provided as a QoS option in managed switches from Contemporary Controls to serve legacy equipment. This octet has been used inconsistently over the years - defined differently by five RFCs.

Traffic

Messages on a network.

Transceiver

A combination of the words transmitter and receiver. A transceiver is the set of electronics that sends and receives signals on a media system. Transceivers may be internal or external. Sometimes called a MAU.

Transport Layer (Layer 4 in the OSI model)

Ensures reliable data transfer between end systems (hosts) using error recovery and flow control. TCP is its most common protocol.

Trunking

Two or more ports grouped together as one logical path to increase bandwidth between a switch and a network node when a single path cannot handle the traffic. Loops are avoided because specific paths are designated. Often a single link is designated for flooding broadcasts and packets of unknown destination. Trunks can provide redundancy to critical devices.

Twisted-Pair Cable

A multiple-conductor cable whose wires are paired together, twisted, and enclosed in a single jacket. A *Category 5* twisted-pair segment is a cable with 4 pairs in a single jacket. Each pair consists of two insulated copper wires that are twisted together. The twisted-pair cable may be shielded *(STP)* or unshielded *(UTP)*.

U

Unicast

A message sent to just one destination.

Unshielded Twisted Pair (UTP)

Twisted-pair cable that lacks a shield. Although shielded cable *(STP)* can impart greater signal immunity, if improperly installed STP can degrade reliability. Consequently, UTP is often preferred over STP.

Upload

To send a local file or data to a remote site or from a client to a server.

URL (Uniform Resource Locator)

A string of characters (address) identifying a document (file) on the World Wide Web.

User Datagram Protocol (UDP)

The IP protocol for simple, connectionless (nonguaranteed) data delivery.

V

VLAN (Virtual Local Area Network)

A LAN that maps stations on a basis other than location - such as by department, user type or application. Managing traffic, workstations, and bandwidth can be easier with a VLAN and improve network efficiency.

VPN (virtual Private Network)

A technology that creates a network that is physically public, but virtually private because it logically includes/excludes specified stations (hosts).

W

WAN (Wide Area Network)

A network of large geographical area that uses leased telecommunication lines and has slower data-transfer rates than Local Area Networks (LANs). Typically, a WAN connects to the Internet.

Web Page

A hypertext document viewable by a Web browser.

Web Server

A computer or device that serves up Web pages. By installing server software into a computer or device and connecting it to a network, it can become a Web server. Every Web server has an IP address and possibly a domain name.