4

Ethernet and Ethernet/IP Protocols

Dr. H. K. Verma

Distinguished Professor (EEE)
Sharda University, Greater Noida

(Formerly: Deputy Director and Professor of Instrumentation
Indian Institute of Technology Roorkee)

Website : profhkverma.info

CONTENTS

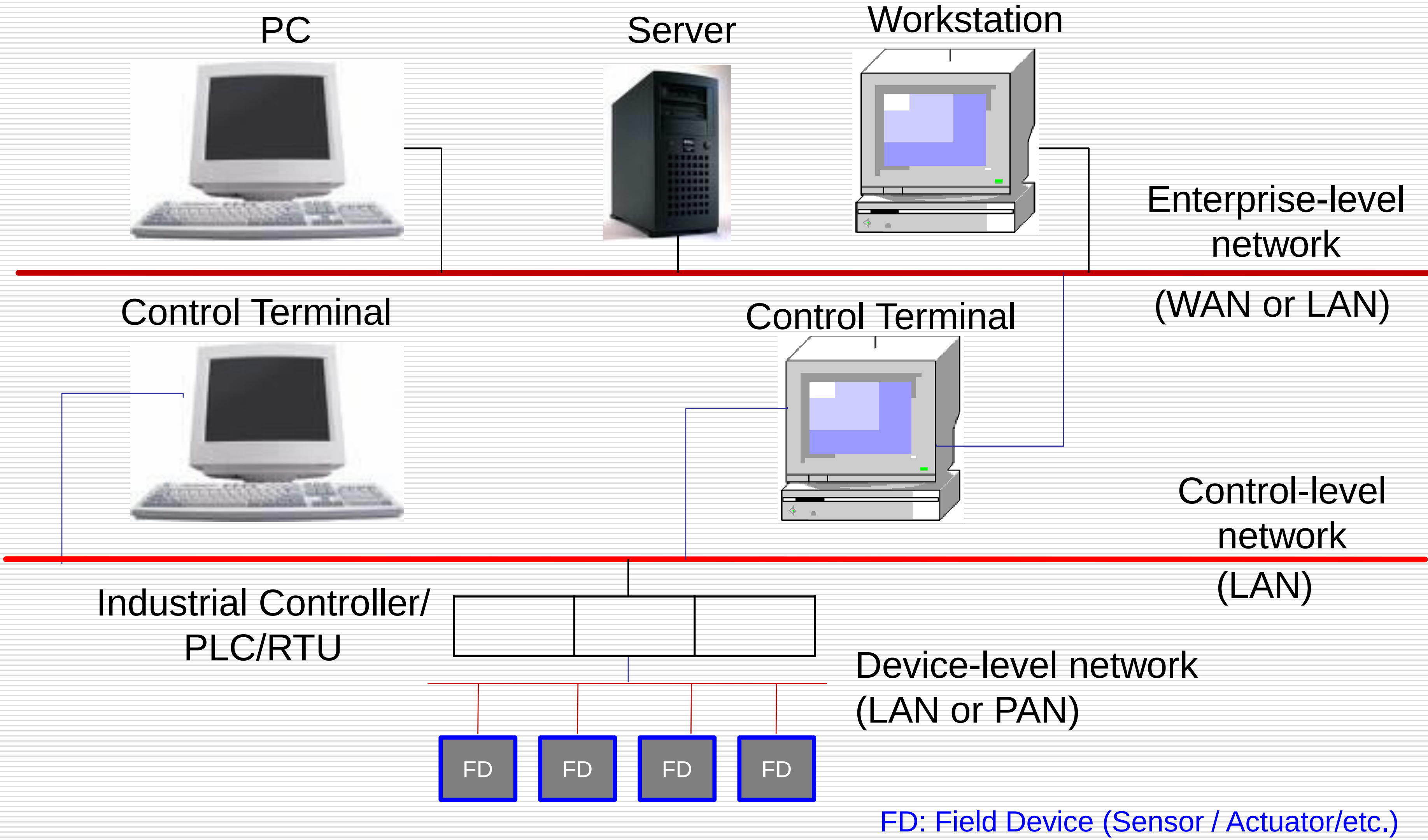
Introduction (1)

- Broadly speaking, data communication networks (or data networks) are used in two types of applications:
  a) General purpose or business applications
  b) Industrial applications
- Examples of general-purpose or business applications are: e-mail, Internet browsing, e-banking/ net-banking, e-commerce, and so on.
- Industrial applications, on the other hand are meant broadly for two purposes:
  i. Data acquisition or monitoring
  ii. Control of an industrial process or plant

Introduction (2)

- If a data network is used for general or business communications, it is referred to as General-Purpose or Business Data Communication Network, or simply as ***Business Data Network***.
- The communicating devices (nodes) in business data networks are generally computers and servers and the most important requirement in general is high data rates or speeds.
- In case a data network is used in industrial applications, it is referred to as Industrial Data Communication Network, or simply as ***Industrial Data Network.***
- The communicating devices (nodes) in industrial data networks are computers, servers, work-stations, control terminals, digital controllers and field devices (sensors, meters, instruments and actuators etc.). Their requirements are different and will be discussed after understanding the hierarchy of industrial networks.

Hierarchy of Industrial Data Networks



Enterprise-Level Network

- Enterprise-level network is used for **transfer of information** among PCs, workstations and servers located in various offices of the enterprise and the control terminals (PCs) located in the control room. Hence also called as **information-level network**.
- ***Most important requirement of enterprise-level network is the data speed*** as volume of data traffic is high to very high.
- As no control commands are sent over enterprise level network, ***latency is rarely an issue***.
- Different types of data network may be used at enterprise-level as under:
  - a) **LAN**, in case the enterprise (organization) is small and communication needs can be taken care by a single LAN.
  - b) **WAN**, where the enterprise is dispersed over multiple premises that can be covered by a WAN but not a single LAN.
  - c) **Intranet or Internet: I**ntranet of the organization or the global Internet may be used, if available, in place of WAN.

Control-Level Network

- Control-level network is used for data communication between:
  a) the control-terminals (PCs) and master-controller, all located in a control room, or
  b) the control-terminals (PCs) located in a control room and industrial controllers/ programmable logic controllers/ remote terminal units located in the field or on factory floor.
- As control commands are sent over the control-level network, ***latency and determinism become the most important requirements***.
- As the volume of data traffic on the control-level network is low or medium, ***high data speed is generally not necessary.***
- The type of the network used at control-level is in most cases a ***LAN***, but sometimes ***multiple LANs*** working on different protocols are used because of the availability of different network ports on the devices to be connected.

Device-Level Network

- Device-level network is used for data communication:

  a) Between an industrial controller/ PLC/ RTU and its field devices (sensors, actuators, etc.) located in the field or on factory floor, or

  b) Among the various field devices located in the field or on factory floor.

- As control commands and status information are generally sent over device-level networks, ***low latency and determinism are their most important requirements.***

- As the volume of data traffic on the device-level network is generally low or very low, ***low data speeds are good enough***.

- The type of the network used at device-level may be either ***a LAN or a PAN,*** depending on the size of the area or the distances to be covered by the network.

Network Protocols Covered

The following two prominent data network protocols are described in detail in this chapter:

1. **Ethernet / IEEE 802.3**

   Used for (a) business data networks and (b) enterprise-level industrial data networks.

2. **Ethernet/IP**

   Used for (a) control-level and (b) enterprise-level industrial data networks.

Ethernet / IEEE 802.3

1. Introduction and Highlights
2. Communication Protocol Stack
3. Data Link Layer
   - MAC Protocol
   - Data Link Frame Format
   - Internet Protocol (IP)
   - Address Resolution Program
4. Physical Layer
5. Ethernet Variants
6. Advantages and Limitations
7. Widespread Use of Ethernet

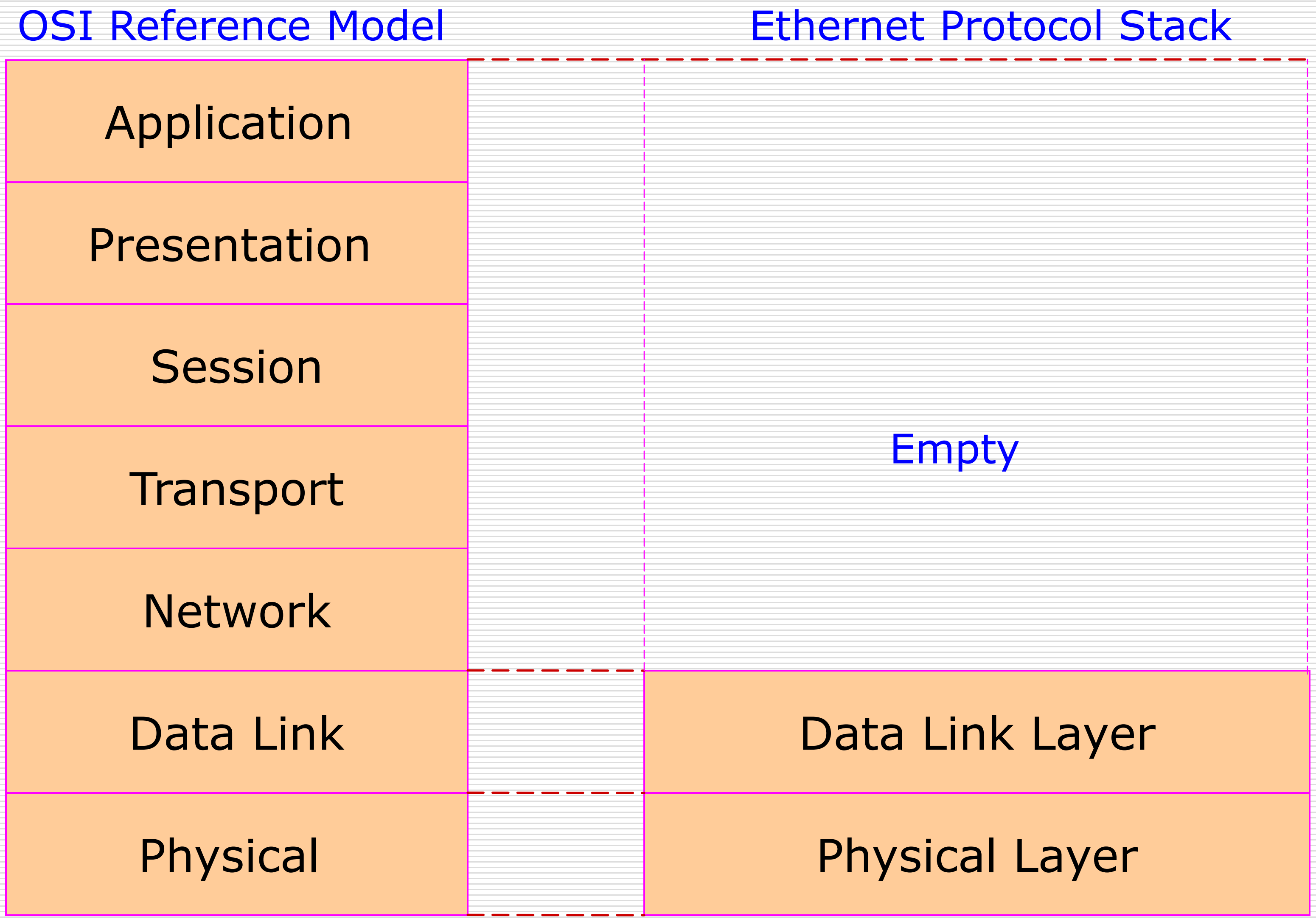
Ethernet/IEEE802.3 : Introduction

- Ethernet is a **data network protocol** for **high-speed LANs**
- Originally developed by Xerox Corporation
- Later improved upon by DEC and Intel
- It is the most widely used protocol for business data networks.
- **Also used for enterprise-level industrial data networks**, which invariably require high data speeds and for which latency is not a critical requirement.
- The Institute of Electrical and Electronic Engineers (IEEE) developed an **Ethernet standard, known as IEEE standard 802.3**.
- This standard (a) defines rules for configuring an Ethernet network and (b) specifies how the elements in an Ethernet network shall interact with one another.

Ethernet/IEEE802.3 : Highlights

- OSI layers defined in the protocol:
  a) Data-Link Layer (DLL)
  b) Physical Layer (PL)
- Ethernet protocol stack is shown in next slide.
- MAC protocol specified: CSMA/CD
- Transmission method specified: Baseband
- Transmission modes specified: Half-duplex and/or full-duplex (as discussed later)
- Following Ethernet variants, based on data rate or speed, are available and described later:
  a) 10 Mbps Ethernet
  b) 100 Mbps Ethernet
  c) 1 Gbps Ethernet
  d) 10 Gbps Ethernet

Ethernet/IEEE802.3 : Protocol Stack



Ethernet/IEEE802.3 : Data-Link Layer

- Data-Link Layer (DLL) of Ethernet includes the following two major functions / specifications:
  a) Medium access control (MAC) protocol
  b) Data-link frame format

Ethernet/IEEE802.3 : MAC Protocol

- Common for all speed variants of Ethernet.
- The MAC protocol specified is:
  "carrier sense multiple access with collision detection" (CSMA/CD)
- The CSMA/CD protocol supports peer-to-peer communication.
- Protocol is based on the principle: "listen before send"
- One node sends (transmits), while all other nodes listen to carrier.
- If two (or more) nodes attempt to send at the same time, collision is detected.
- Consequent to collision detection, all the nodes stop sending and wait for small but random amounts of time before resending.
- ***Advantage of CSMA/CD*** : Supports peer-to-peer communication.
- ***Disadvantage of CSMA/CD*** : High traffic on network can result into multiple collisions.

Data-Link Frame Format (1)

- Data-link frame is the data unit passed from DLL to PL.
- It is common for all speed variants of Ethernet and comprises 8 fields.
- Frame format along with field sizes in octets (bytes) are shown below.
- Note that the total size of Data + Pad fields (called as **"Payload"**) is shown as "46 to 1500 octets", which has following meaning:
  - If actual data is less than 46 octets, then necessary number of octets are added as "Pad" to make the total number of octets 46.
  - If actual data is 46 octets or more, then "Pad" is not required.
  - The maximum size of actual data allowed in a frame is 1500 octets.
  - The minimum size is meant to ensure detection of a collision, as and if it occurs.

No. of octets (bytes):	7	1	6	6	2	← 46 to 1500 →		4
Fields:	Preamble	SFD	DA	SA	Length	Data	Pad	CRC

Data-Link Frame Format (2)

❖ Roles of the various fields of data-link frame are as under:

Field	Role of the Field
1. Preamble	• 7 octets of alternating 0's & 1's • Used by receiver to establish bit synchronization
2. Start Frame Delimiter (SFD)	• 1 octet with bit sequence 10101011 • Indicates actual start of the frame
3. Destination Address (DA)	MAC address of destination node
4. Source Address (SA)	MAC address of source node
5. Length	Specifies actual length of data in octets (bytes) in Data Field
6. Data	Actual data being sent
7. Pad	Octets added to data to ensure that the size of data + pad is at least equal to 46 octets
8. CRC	32-bit CRC on fields 3 through 7.

Ethernet/IEEE802.3 : Physical Layer (1)

- Physical layer of Ethernet protocol specifies the following:
  a) Coding method
  b) Transmission method
  c) Transmission mode
  d) Data rate
  e) Signal transmission media
- Coding method specified: Manchester coding
- Transmission method specified: Baseband
- Transmission modes specified: Half-duplex and/or full-duplex, different for the different speed-variants of Ethernet (as discussed later)

Ethernet/IEEE802.3 : Physical Layer (2)

- Data rates specified:
  - a) 10 Mbps (Variant : 10 Mbps Ethernet)
  - b) 100 Mbps (Variant : 100 Mbps Ethernet)
  - c) 1 Gbps (Variant : 1 Gbps Ethernet)
  - d) 10 Gbps (Variant : 10 Gbps Ethernet)
- Following signal transmission media are specified. (But they are different for the different speed variants of Ethernet, as discussed later)
  - a) Copper cables
    - i. Coaxial cable
    - ii. UTP cable
    - iii. STP cable
  - b) Optical fibre cables
    - iv. Multi-mode fibre (MMF) cable
    - v. Single-mode fibre (SMF) cable.

10Mbps Ethernet/IEEE802.3

- Data rate specified: 10 Mbps
- Transmission mode specified: Half duplex
- Cables specified:
  - a) Coaxial
  - b) UTP
  - c) MMF
- 4 Variants of 10-Mbps Ethernet as per signal transmission medium:

S. No.	Variant	Signal transmission medium
1	10 BASE-5	Thick coaxial cable
2	10 BASE-2	Thin coaxial cable
3	10 BASE-T	Cat-3 UTP cable
4	10 BASE-F	MM fibre cable

100 Mbps Ethernet/IEEE802.3

- Also known as Fast Ethernet.
- Data rate specified: 100 Mbps
- Protocol supports both 10-Mbps and 100-Mbps devices
- 10/100 Mbps switching hubs are available for such networks
- Transmission mode specified: Half duplex & Full duplex
- Cables specified:
  a) UTP
  b) STP
  c) MMF
- 3 Variants of 100-Mbps Ethernet as per signal transmission medium:

S. No.	Variant	Signal transmission medium
1	100 BASE-TX	STP or Cat-5 UTP cable
2	100 BASE-T4	4 pairs of cat-3 UTP cable
3	100 BASE-FX	MM fibre cable

1-Gbps Ethernet/IEEE802.3

- Data Rate : 1000 Mbps (1 Gbps)
- Compatible with 10-Mbps and 100-Mbps Ethernets to ensure smooth transition from lower-speed network to higher-speed network
- Application: Backbone Networks
- Transmission Mode: Full duplex
- Cables :
  a) UTP and STP
  b) MMF and SMF
- 4 Variants of 1-Gbps Ethernet as per signal transmission medium:

S. No.	Variant	Signal transmission medium
1	1000 BASE- T	4 pairs of cat-5 UTP cable
2	1000 BASE-CX	2 pairs of STP cable
3	1000 BASE- SX	MMF cable of short wavelength (850 nm)
4	1000 BASE-LX	MMF or SMF cable of long wavelength (1310 nm)

10-Gbps Ethernet/IEEE802.3

- Aimed at taking care of increase in Intranet and internet traffics
- Data rate: 10 Gbps
- Cables specified: MMF and SMF cables
- Cable length allowed: upto 40 km with SMF cable at 1310 nm
- Transmission Mode: Full duplex
- High data rate enables high-speed backbone connections
- Long cable lengths can make all-Ethernet MANs and WANs possible.
- 4 Variants of 10-Gbps Ethernet as per signal transmission medium:

S. No.	Variant	Signal transmission medium
1	10G BASE-S	MMF cable of short wavelength (850 nm)
2	10G BASE-L	SMF cable of long wavelength (1310 nm)
3	10G BASE-E	SMF cable of extra-long wavelength (1550 nm)
4	10G BASE-Lx4	MMF/SMF cable of long wavelength (1310 nm) using WDM with 4 light waves

More Details of 10-Gbps Ethernet Variants

Variant	OFC Type & Options	Wave-length	Max. Cable Length
10G BASE-S	62.5 µm MMF	850 nm	30 m
	50 µm MMF	850 nm	300 m
10G BASE-L	10 µm SMF	1310 nm	10 km
10G BASE-E	10 µm SMF	1550 nm	40 km
10G BASE-Lx4	This variant uses WDM with 4 light beams		
	62.5 µm MMF	1310 nm	300 m
	50 µm MMF	1310 nm	300 m
	10 µm SMF	1310 nm	10 km

Summary of Ethernet Variants

Ethernet variant	Max data rate	Transmission mode options	Cable options
10 Mbps Ethernet	10 Mbps	Half duplex	Coaxial UTP (cat-3) MMF
100 Mbps (or Fast) Ethernet	100 Mbps	Half duplex Full duplex	UTP (cat-3, 4 pairs) UTP (cat-5, 1 pair) STP MMF
1 Gbps Ethernet	1 Gbps	Full duplex	UTP (cat-5, 4 pairs) STP (2 pairs) MMF (850 nm, 1310 nm) SMF(1310 nm)
10 Gbps Ethernet	10 Gbps	Full duplex	MMF (850 nm, 1310 nm) SMF(1310 nm, 1550 nm)

Ethernet/IEEE802.3 : Advantages

1. Ethernet has several speed variants, capable of supportng fairly high speeds (10 Mbps) to very high speeds (100 Mbps, 1Gbps and 10 Gbps) of data communication.
2. Supports peer-to-peer communication.
3. Specifies alternative signal transmission media for each speed-variant.

Ethernet/IEEE802.3 : Limitations

1. ***High Data-Overhead:*** The minimum Ethernet frame size, excluding Preamble and Start Frame Delimiter, is 64 bytes even when the actual data to be communicated is of zero-byte length. It means a huge data overhead or poor data transmission efficiency for short messages.
2. ***Lack of Determinism:*** Ethernet/IEEE802.3 uses collision detection (CD) as the basis of MAC, which makes it difficult to estimate the transport time for individual data packets, i.e. the transport time is in-deterministic.
3. ***High Latency:*** With increased traffic, an Ethernet/IEEE802.3 network may face repeated collisions, causing long delays in data delivery.
4. ***Packet Loss:*** *Some of the data packets travelling across a network segment may even fail to reach their destination due to congestion in that segment.*

Widespread Use of Ethernet

1. Ethernet is the most widely used protocol for business data communications.
2. Almost all organizations, including industrial organizations, use the global Internet, which uses Ethernet as the dominating LAN.
3. Almost all organizations, including industrial organizations, own a private intranet for distributing information internally. These intranets also use Ethernet as the dominating LAN.
4. Several Application-Layer network protocols, specially developed or particularly suitable for industrial automation, are run on Ethernet networks. Such combinations, known as **Industrial Ethernet**, are becoming popular with industry. Some examples of Industrial Ethernet are: Modbus/TCP, Ethernet/IP, ProfiNet, EtherCAT and Ethernet Powerlink.

Ethernet / IP

1. Introduction
2. Communication Protocol Stack
3. CIP-Based Application Layer
4. TCP/IP Protocol Suite
   - Transmission Control Protocol (TCP)
   - User Datagram Protocol (UDP)
   - Internet Protocol (IP)
   - Address Resolution Program
5. Messaging in Ethernet/IP
6. Advantages
7. Challenges

Ethernet/IP : Introduction

- Defined in simplest terms, Ethernet/Industrial Protocol or Ethernet/IP is the **"Common Industrial Protocol (CIP) over Ethernet network".**
- The standard Ethernet (that is, Ethernet/IEEE802.3) has very limited acceptance in industrial automation applications because of its limitations enumerated in an earlier slide.
- But to take advantage of the wide-spread availability of Ethernet networks in industrial enterprises, some popular industrial automation protocols that specify only the Application Layer have adapted to standard Ethernet protocol. The outcome is **"Industrial Ethernet" protocols.**
- Ethernet/IP is one of these industrial Ethernet protocols, wherein "Common Industrial Protocol (CIP) adapts to Ethernet".
- Some of other industrial Ethernet protocols are: Modbus/TCP, ProfiNet, EtherCAT, SERCOS III and Ethernet Powerlink.

Ethernet/IP : Communication Protocol Stack

- With respect to the 7-layer OSI reference model of communication system, Ethernet/IP* comprises 5 layers as under:
- It uses the Common Industrial Protocol (CIP) **with necessary adaption** for its Application Layer. (Details will be discussed later)
- It uses the Ethernet protocol for the two bottom-most layers (Data-Link and Physical Layers). (Ethernet protocol has already been discussed in this chapter)
- It uses the TCP/IP* protocol suite of the global Internet for the two middle layers (Transport and Network layers). (Details will be discussed later)
- The communication protocol stack of Ethernet/IP is shown in next slide.

** Note that IP in Ethernet/IP stands for Industrial Protocol, while in TCP/IP it stands for Internet Protocol.*

Ethernet/IP : Communication Protocol Stack

	OSI Reference Model	Ethernet/IP Stack	
7	Application	CIP-based Application Layer	
6	Presentation	Empty	
5	Session		
4	Transport	TCP, UDP	TCP/IP protocol suite
3	Network	IP, ARP	
2	Data Link	Ethernet Data Link Layer	
1	Physical	Ethernet Physical Layer	

CIP-Based Application Layer

- **Common Industrial Protocol (CIP) was designed for industrial control and information applications.**
- It was originally developed and owned by Rockwell Automation, and was known as Control and Information Protocol.
- It is now an open protocol managed and promoted by ODVA (Open DeviceNet Vendors' Association) and supported by hundreds of vendors globally.
- Application Layer of EtherNet/IP is based on CIP. In fact, the CIP protocol is adapted here to the Ethernet protocol.
- CIP includes a complete set of messages and services for various industrial automation functions.
- It is designed to comprehensively serve all the needs of automation of manufacturing processes/plants, namely control, data collection, configuration, safety, synchronization and motion.
- Other well-known industrial network protocols based on CIP are DeviceNet and ControlNet.

Common Industrial Protocol (CIP)

- CIP is characterized by the following features:
  a) It is **media-independent**.
  b) It is an **object-oriented protocol.**
  c) It implements a **distributed object model**.
- In CIP protocol, each **device** in the network is represented by a series of objects and each **object** is a grouping of related data values in the device.
- ‘**Distributed objects**’ are the objects that are **distributed across different address spaces.**
- ‘Different address spaces’ means either ‘different processes on the same computer’ or ‘**multiple computers** connected via a network and working together by sharing data’.

TCP/IP Protocol Suite

- ***TCP/IP is the protocol suite of the Internet.***
- Though TCP/IP will run on other than Ethernet networks also and, likewise, the Ethernet supports other than TCP/IP communication protocols also, yet the Ethernet protocol and the TCP/IP protocol suite have been increasingly used together. The combination is called Ethernet/TCP protocol.
- TCP/IP protocol suite comprises the following 4 major protocols:

  i. Transmission control protocol (TCP)
  ii. User datagram protocol (UDP)
  iii. Internet protocol (IP)
  iv. Address resolution protocol (ARP)
- Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the ***protocols of Transport Layer (TL)***.
- Internet Protocol (IP) and Address Resolution Protocol (ARP) are the ***protocols of Network Layer (NL)***.
- Only basic information on the above protocols is given here.

Transport and Network Layers

- **Transport Layer (TL)**
  - ***TL is the end-to-end data transfer layer.***
  - It serves the upper layers (Application Layer, Presentation Layer and Session Layer, whichever are present in the system) to provide data transfers and in turn uses the services provided by the lower layers (Network, Data-Link and Physical Layers).

- **Network Layer (NL)**
  - NL transmits data packets from source to destination *across the network.*
  - It hides the network topology from the upper layers, so that they can work without bothering about the network topology being used.

Transmission Control Protocol (TCP) (1)

- Transmission Control Protocol (TCP) is the main Transport Layer protocol of the Internet.
- TCP provides fully ***connection-oriented data-transport service***.
- It provides a reliable end-to-end connection between two processes of an ***application*** running in two different hosts (computers).
- For the data transport, the hosts are identified as ***source host*** and ***destination host***.
- TCP runs only in the end hosts and not in intermediate network equipment, such as routers and bridges.
- The sending-end application in the source host would generate a block of data and send to the transport layer for sending it to the receiving-end application.
- Transport layer would break this data block from the application layer into several pieces, called ***data units***, to make data transport more manageable.

Transmission Control Protocol (TCP) (2)

- For a reliable data-transport service, TCP has following provisions:
  1. Error detection
  2. Acknowledgement
  3. Retransmission
  4. Sequence numbering
- TCP adds a header of 20 bytes (called as ***TCP header*** and meant for control of flow of data) to each data unit.
- The combination of TCP header and data from the next higher level is called ***Transport Protocol Data Unit or TPDU.***
- ***TCP header*** has 9 fields in all, including the following 4 fields:
  - ***Source port address*** (2 bytes) that identifies the process of an application that initiated the connection at the source host
  - ***Destination port address*** (2 bytes) that identifies the process of the application at the destination host to which the connection is being made
  - ***Sequence number*** (4 bytes) to ensure that the data units are reassembled at the destination in the correct sequence even if they reach in a wrong sequence
  - ***Check-sum*** (2 bytes) for error detection.

Transmission Control Protocol (3)

- The process of TCP connection between ***source host (S)*** and ***destination host (D)*** involves 5 steps:

1. S sends connection request to D
   ↓
2. D sends back "ACCEPTED" message to S
   ↓
3. S sends data units to D (one by one)
   ↓
4. S sends termination request to D after it has sent all the data units
   ↓
5. D sends back "TERMINATED" message to S.

User Datagram Protocol (UDP)

- User Datagram Protocol (UDP) is an alternative Transport Layer protocol of the Internet.
- UDP provides ***connection-less data-transfer service***, that is, no connection is set up before the actual data transfer.
- UDP provides so-called ***unreliable*** data-transfer, that is, reliability of data transfer should be taken care by the application.
- UDP adds a header of ***8 bytes*** only to the data unit.
- UDP header has 4 fields as under:
  - ***Source port address*** (2 bytes) that identifies the process on the source host that sources the data.
  - ***Destination port address*** (2 bytes) that identifies the process on the destination host to which the data is intended to be delivered.
  - ***Length of data*** (2 bytes)
  - ***Check-sum*** (2 bytes)

TCP- UDP Comparison

Feature	TCP	UDP
Connection between source and destination hosts	Connection is established before sending data from source host to destination host and continues until all data units have been transferred.	Connection is not established before sending data from source host to destination host.
Header size (overhead)	20 bytes (High overhead)	8 bytes (Low overhead)
Reliability of data transfer	TCP takes care of error detection and sequencing of data units	Application has to take care of error detection and sequencing of data units
Use of protocol	Used where flow of data is continuous	Used where flow of data is intermittent.

Internet Protocol

- Internet Protocol (IP) is the Network Layer protocol used by the Internet.
- IP provides connection-less data-gram service.
- It adds an ***IP Header*** to each TPDU received from Transport Layer.
- ***IP Header + TPDU = IP Datagram***
- IP Header includes ***Source IP-address*** and ***Destination IP-address***.
- IP address is assigned by IP to not only source and destination hosts, but to each and every device connected in the Internet (e.g. switches and routers).
- IP address is:
  - 4 byte-long in IPv4 (IP version 4)
  - 16 byte-long in IPv6 (IP version 6)

IP Addresses in IPv4

- 4-byte or 32-bit long **numeric addresses** are assigned to all the devices connected in the Internet.
- In **dot-decimal notation**, IP address is written as four decimal numbers, each equivalent of a binary byte, separated by dots. For example: 192.168.207.8
- In **binary notation**, IP address is written as 32 bits in continuation without any dots. For example, the above address would be written as: 11000000 10101000 11001111 00001000
- IP addresses are assigned to hosts in run time.
- Number of IP addresses = 2 ∩ 32 = 4.3 billion (approx.)
- IP address has two parts:
  - First part of address = network address
  - Second part of address = address of host in that network.

IP Addresses in IPv6

- 16-byte or 128-bit long addresses.
- Number of IP addresses = 2 ∩ 128

  ≈ Infinite number
- An IPv6 address is represented as 8 groups of 4 hexadecimal digits (2 bytes) each. The groups are separated by colons (:). For example:

  2001:0db2:8fa3:0000:0000:8a8e:0770:7564
- While IPv4 uses ARP (Address Resolution Protocol - to be discussed later) to map IP addresses to MAC addresses, IPv6 uses NDP (Neighbour Discovery Protocol) to map IP addresses to MAC addresses.
- For some time both schemes of addressing (IPv4 and IPv6) will have to co-exist, until a complete changeover to IPv6 takes place.

Address Resolution Protocol (ARP)

- Another Network Layer protocol used by the Internet.
- ARP finds out MAC address corresponding to an IP address
- It uses ARP tables, which contain mapping between IP addresses and MAC addresses.
- MAC address is the address assigned to the network interface card (NIC), so it is a fixed hard-coded number.

Messaging in Ethernet/IP

- Two types of messaging services are carried out:
  a) Explicit messaging
  b) Implicit messaging.

Explicit Messaging

- **Based on client/server relationship.**
- The client (such as master controller located in the control room) asks or requests information from a server (which is field device like VFD, water-level measuring unit, temperature control unit, etc.)
- The server (the addressed field device) sends the requested information back to the client (PLC controller in this example)
- Because the client requests information from the server via TCP/IP services, the **request shall contain** all the information needed by the server to respond explicitly to the request.
- Used for communicating data which is not time critical, like configuration and diagnostic data.

Implicit Messaging

- Meant for sending input and output related messages, hence **also called as I/O messaging.**
- **Based on master-slave relationship.**
- Controller is called as I/O scanner and field devices as I/O adapters, and they work as master and slaves, respectively.
- Communication is much more efficient than that with explicit messaging as the two ends are pre-configured as I/O scanner and I/O adapter and they **know implicitly** what to expect in terms of communication. The message has mostly the data with minimal additional information.
- Meant for time-critical data such as real-time status data (from field devices to controller) and real-time control data (from controller to field devices).

Comparison of Explicit & Implicit Messaging

Feature	Explicit Messaging	Implicit or I/O Messaging
Relationship between two ends	Client-server (Controller is client, Field devices are servers)	Master-slave (Controller is Master or I/O Scanner, Field devices are slaves or I/O Adapters)
Two ends pre-configured?	No	Yes, as I/O scanner and I/O adapter
Purpose of message	Not implicit, hence needs to be explicitly included in the message	Implicit, hence only data is given in the message
Size of messages	Long	Short
Suitable for time-critical data?	No	Yes

Advantages of Ethernet/IP

(a) Due to CIP

1. CIP includes a complete set of messages and services for all industrial automation functions.
2. CIP permits users to integrate their industrial control applications at the control-level with information services at the enterprise-level, and thereby have a unified communication architecture throughout the industrial enterprise.
3. CIP allows ‘control services’ and ‘information services’ to co-exist on a single Ethernet network.
4. A single configuration tool can configure all devices connected to different networks from a single access point without using vendor-specific software, because all the devices are classified as CIP-objects.
5. Classification of all devices as CIP-objects decreases the training and start-up time required when new devices are connected to the network.
6. Ethernet/IP can conveniently link devices right from the device-level to the control-level to the enterprise-level because of a consistent application layer at all levels.

Advantages of Ethernet/IP

(b) Due to Ethernet and TCP/IP

1. Ethernet/IP uses the tools and technologies of the standard (traditional) Ethernet. It also uses the standard TCP/IP protocol suite, which is the very basis of the Internet. As stated earlier, almost all organizations, including industrial organizations, use the global Internet and Ethernet networks. Therefore, Ethernet/IP can be launched on the existing Ethernet / Internet infrastructure without spending money and time.
2. Ethernet/IP works with all the standard off-the-shelf Ethernet devices, which are readily available in the market at very competitive prices.
3. Since standard PCs and all their derivatives support the Internet and the Ethernet, Ethernet/IP can be easily supported on all standard PCs and their derivatives.
4. Since Ethernet/IP is based on three very popular and standard technologies, namely CIP, Ethernet and the Internet, it will always have the advantage of moving forward as these base technologies evolve in the future.

Challenges of Ethernet/IP

There are some challenges in the implementation of Ethernet/IP, which need to be handled as explained below:

1. The first challenge is the scarcity of engineers and trained staff who understand both, data networks and automation concepts. Very often the first-time implementation is carried out by close collaborative efforts of the experts and staffs from these two domains.

2. Another challenge is the inherent lack of **determinism** of the standard Ethernet. Recent developments in intelligent network switches for Ethernet networks can largely overcome this problem. Larger networks should be segmented by using these switches to create smaller collision domains, thereby achieving better determinism in data transportation from source to destination.

3. Network equipment has to work in **harsh industrial environment** in terms of higher levels of temperature, humidity, vibrations and electrical noise. Only the rugged switches, connectors and other components designed to withstand these conditions must be employed. Optical fibre cables should be used because of their high immunity to electrical noise.

