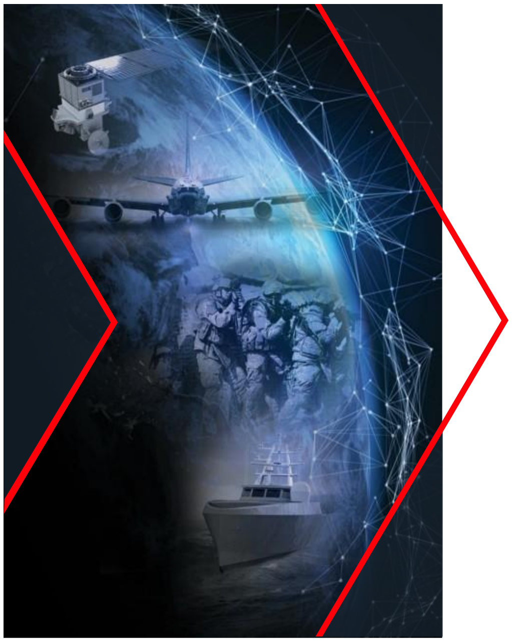


L3HARRIS
FAST. FORWARD.

INTRODUCTION TO NETWORKING

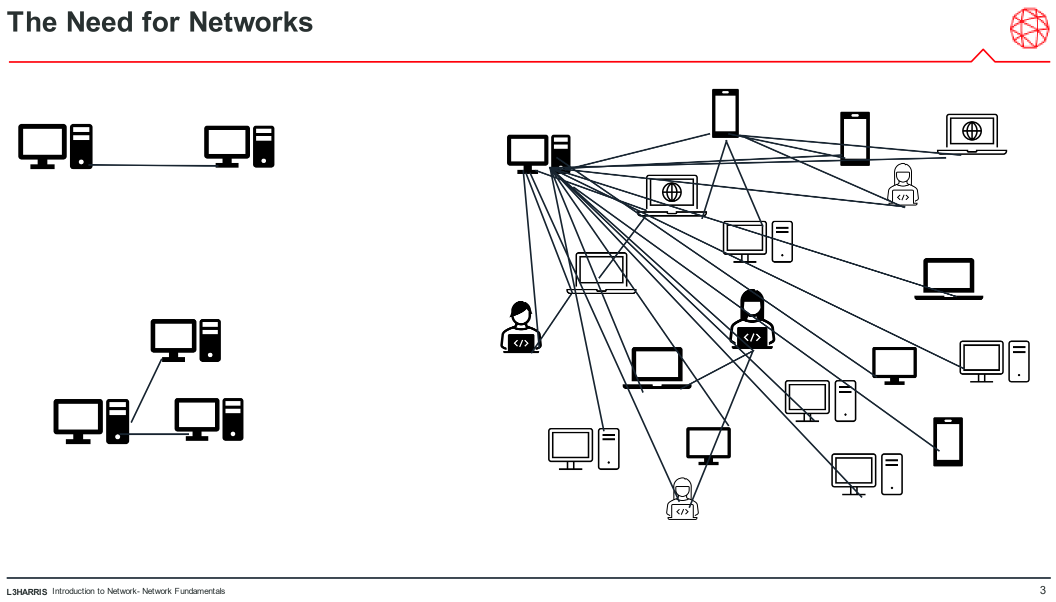
Module 1:
Network Fundamentals

Tanya Wilcox Sr. Specialist Technical Trainer

Use of U.S. DoDvisual information does not imply or constitute DoD endorsement.

Course Objectives

- Compare and contrast the characteristics of network topologies, types, and technologies.
- Recall devices, applications, protocols, and services in relation to the OSI Model.
- Explain the purposes and uses of ports and protocols.
- Understand the properties of transmission media, data signaling, media access, and protocols working at the physical and data link layers.



The Need for Networks

Computer networking refers to interconnected computing devices that can exchange data and share resources with each other.

When two devices need to communicate, they can do so over a point-to-point transmission line.

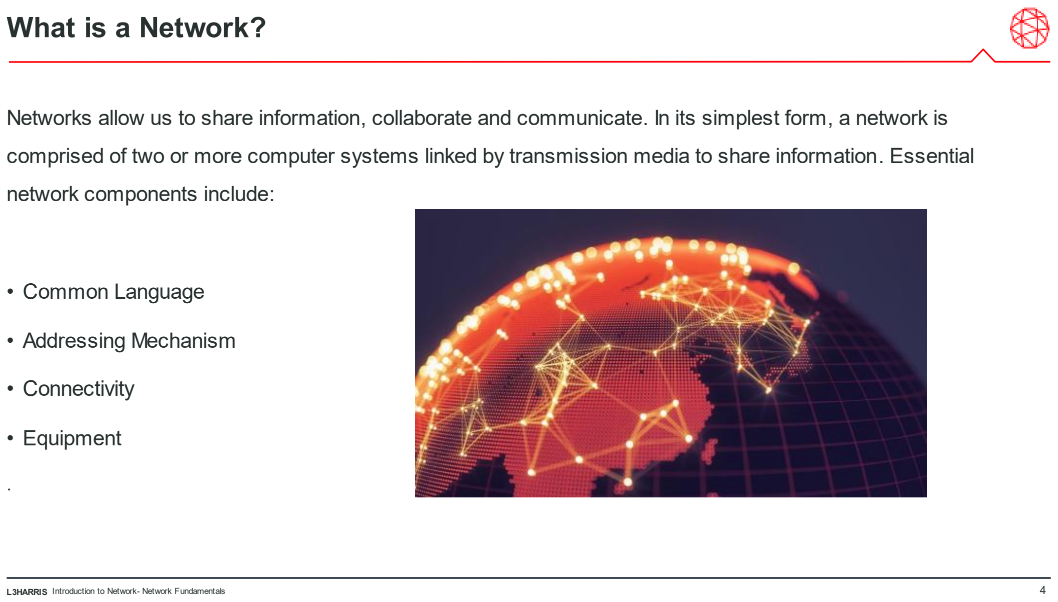
If one device needs to communicate with several devices, multiple transmission lines could be used.

But if multiple devices wish to communicate with a multiplicity of other devices the communication soon becomes complex and difficult to manage.

As a result, the communications industry developed the idea of communications networks: instead of every device having a dedicated connection to every other device, each device could be connected to a network. If all devices follow the same rules, or protocol, communication can occur effectively and efficiently. The idea is easily extended to connecting networks of networks.

Those charged with creating and maintaining these lines of communication require a fundamental knowledge of network terminology, components, standards, types, and configurations.

Throughout this lesson, you will identify the basic concepts of networking theory.



What is a Network?

Networks allow us to share information, collaborate and communicate. In its simplest form, a network is comprised of two or more computer systems linked by transmission media to share information. Essential network components include:

- Common Language
- Addressing Mechanism
- Connectivity
- Equipment

.

L3HARRIS Introduction to Network- Network Fundamentals 4

Networks allow us to share information, collaborate and communicate. In its simplest form, a network is comprised of two or more computer systems linked by transmission media to share information

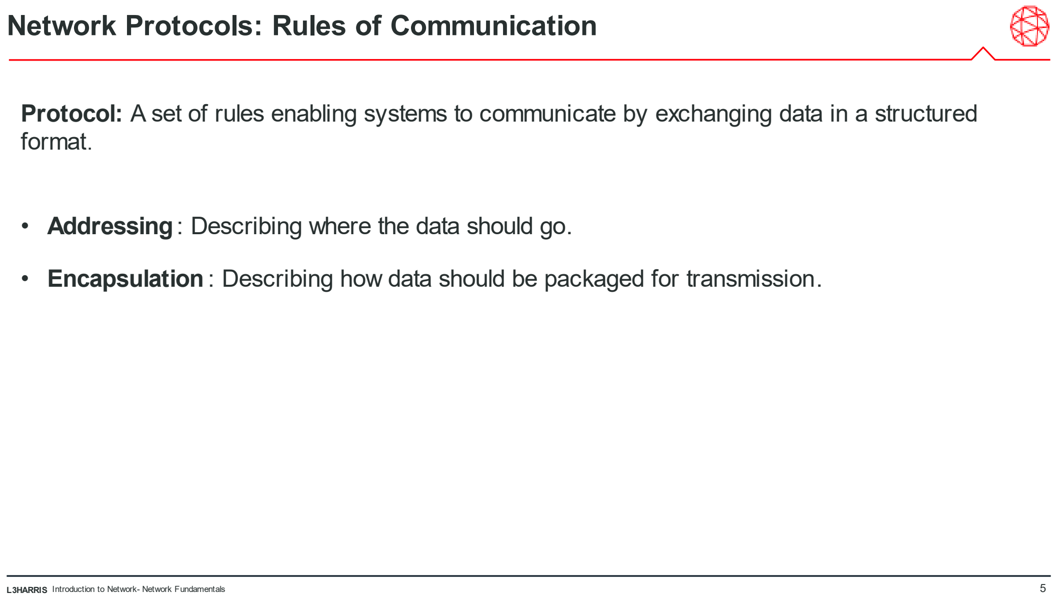
Common Language: There must be a universal language which is agreed upon and understood by all networking components.

Addressing Mechanism: With so many devices in the network that may need to communicate, there must be a way to address a particular machine. Every connected device must have a unique address.

Connectivity: To deploy a network or connect a new user or enterprise to an existing network we must ensure that the connectivity is in place to get data everywhere it needs to go.

Equipment: Every network includes nodes, hosts, and transmission media as essential components to enable communication.

- **Node:** Represents a point of intersection/ connection within a data communication network. Examples of nodes include switches, routers, and endpoints such as computers.
- **Host:** Refers to a networked general-purpose computing device that may offer information resources, services and applications to users or other nodes on the network. Examples of hosts include computers, printers, and servers.
- **Transmission Media:** Cabled or wireless links that transmit information between nodes. Examples of transmission media include copper, fiber, ethernet and 802.11 wireless technologies.



Network Protocols: Rules of Communication

Protocol: A set of rules enabling systems to communicate by exchanging data in a structured format.

- **Addressing** : Describing where the data should go.
- **Encapsulation** : Describing how data should be packaged for transmission.

L3HARRIS Introduction to Network- Network Fundamentals 5

Along with the size and topology of the network, the number of connected devices, and the increasing complexity of computer hardware and software the following are considerations when thinking of networking

- How is universal information exchange made possible?
- How are liabilities and vulnerabilities limited?
- How does authentication work?

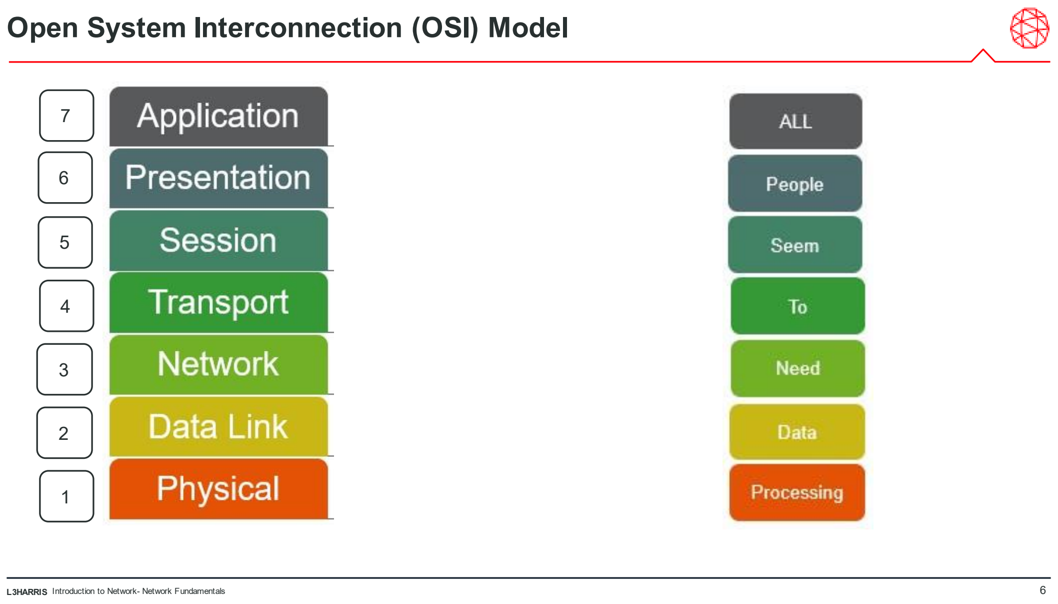
Before networked devices can share information, they need to agree on various aspects of communication. Communication protocols define these rules that govern data transmission. Multilayer protocol stacks use different protocols to communicate at different layers, all while enabling interoperability between systems using different software applications, operating systems and physical network types and are capable of interoperating across geographic and technological boundaries.

The following are common properties that protocols may include packet size, transmission speed, error detection and correction, synchronization techniques, address mapping and formatting, routing information, and flow control.

Two of the most important functions of a protocol are to provide:

- **Addressing**: describing where the data should go.
- **Encapsulation**: describing how data should be packaged for transmission.

Protocol Data Unit (PDU): A protocol is a set of rules enabling systems to communicate by exchanging data in a structured format. A protocol data unit is the basic unit of exchange between entities that communicate using a specific networking protocol.



Open System Interconnection (OSI) Model

7	Application	ALL
6	Presentation	People
5	Session	Seem
4	Transport	To
3	Network	Need
2	Data Link	Data
1	Physical	Processing

L3HARRIS Introduction to Network- Network Fundamentals 6

Open System Interconnection Reference Model is a referenced developed in 1977 by the International Organization for Standardization (ISO). It was designed to support the emergence of diverse computer networking methods that were competing for application in the large national networking efforts in the world.

What emerged was a common understanding of how a network system works for the purpose of systems interconnection. The model accounts for hardware and software used in computer networking and separates the functions of these components into specific layers.

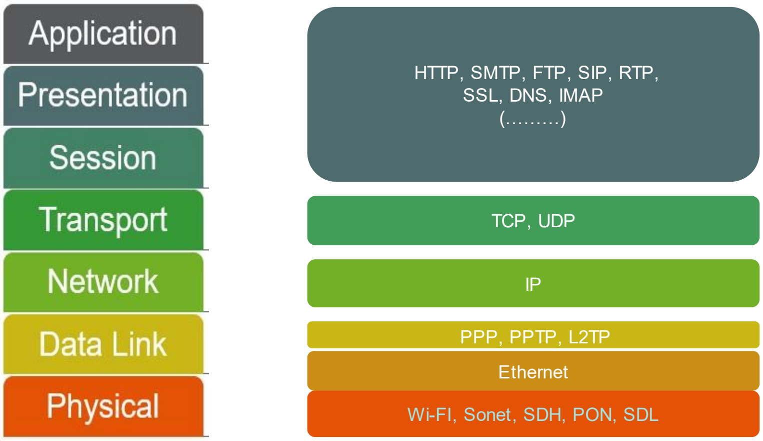
This reference model is comprised of 7 layers, each layer performs a different group of tasks required for network communication.

- It's a way to describe how data moves across the network.
- There are unique protocols at every layer.
- Serves as a functional guideline for designing network protocols, software, and appliances, and for troubleshooting networks.

Note: Each layer performs a different group of tasks required for network communication. Not all network systems implement layers using this structure, however, they all implement each task in some way.

Helpful Tip** Use a nonmonic device to recall the 7 layers of the OSI Model.

OSI Model and Network Protocols



Application

Presentation

Session

Transport

Network

Data Link

Physical

HTTP, SMTP, FTP, SIP, RTP,
SSL, DNS, IMAP
(………)

TCP, UDP

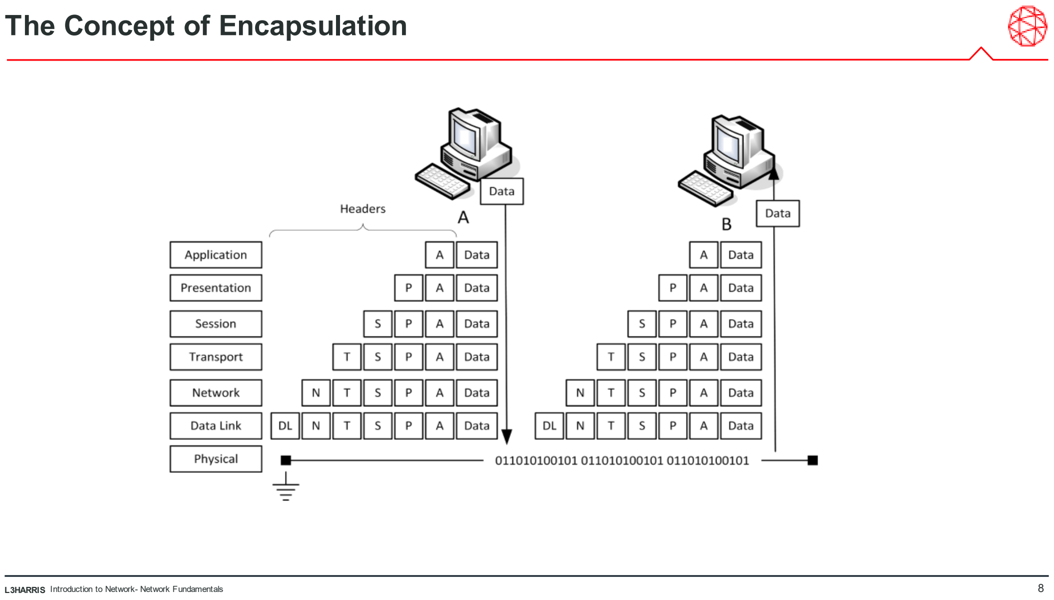
IP

PPP, PPTP, L2TP

Ethernet

Wi-FI, Sonet, SDH, PON, SDL

Notes:



The Concept of Encapsulation

L3HARRIS Introduction to Network- Network Fundamentals 8

The basic process of encapsulation is for the protocol to add fields in a header to whatever data (payload) it receives from an application or other protocol. A network will involve the use of many different protocols.

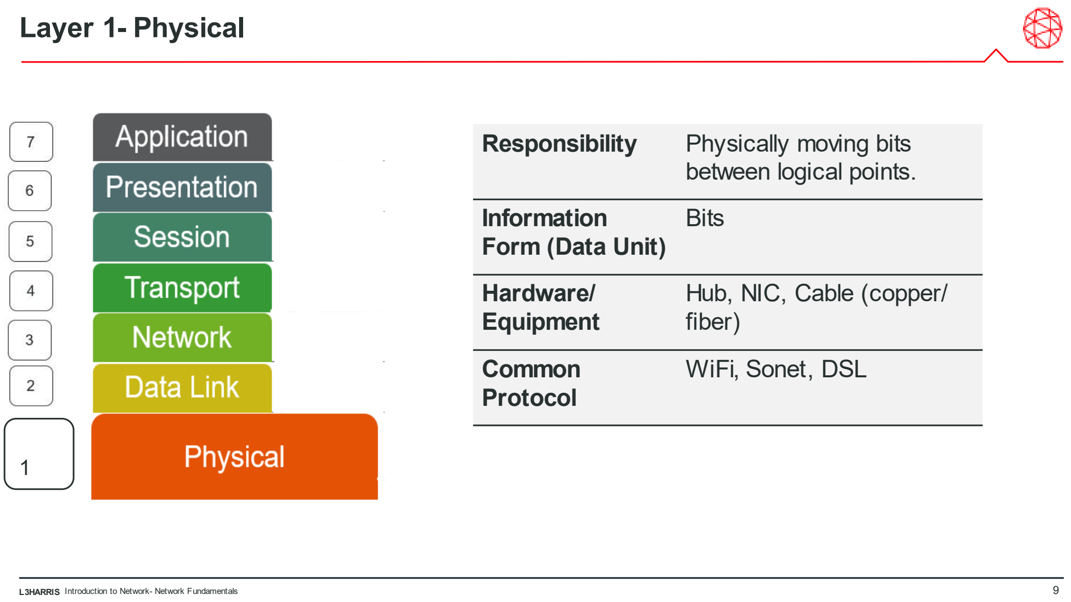
- At each layer, for two nodes to communicate, they must be running the same protocol which is referred to as same layer interaction.
- Each layer will add (or delete) its protocol information as a PDU moves down (or up) each layer.

Protocol Data Unit (PDU): A protocol is a set of rules enabling systems to communicate by exchanging data in a structured format. A protocol data unit is the basic unit of exchange between entities that communicate using a specific networking protocol.

When a message is sent from one node to another, it travels down the stack of layers on the sending node, reaches the receiving node using the transmission media, and then passes up the stack on that node. At each level (except the Physical layer), the sending node adds a header to the data payload, forming a "chunk" of data called a protocol data unit (PDU). This process is known as encapsulation.

- When data is encapsulated in a frame, the software or hardware that is responsible for encapsulating the data adds a header and a trailer to the data.
- The header contains the destination and source address, as well as other control information.
- The trailer contains error-checking information.

The receiving node performs the reverse process. For example, it receives the stream of bits arriving at the Physical layer and decodes an Ethernet frame. It extracts the IP packet from this frame and resolves the information in the IP header, then does the same for the TCP and application headers, eventually extracting the application data for processing by a software program.



Layer 1- Physical

Responsibility	Physically moving bits between logical points.
Information Form (Data Unit)	Bits
Hardware/ Equipment	Hub, NIC, Cable (copper/ fiber)
Common Protocol	WiFi, Sonet, DSL

L3HARRIS Introduction to Network- Network Fundamentals 9

The physical layer is concerned with electrically or optically transmitting raw unstructured data bits (1's and 0's) across the network from the physical layer of the sending device to the physical layer of the receiving device.

- A link between network nodes is created using some form of transmission or physical media.
- Responsible for the transmission and receipt of bits from one node to another node.
- Physical topology: The layout of nodes and links as established by the transmission media.
- Physical interface: Mechanical specifications for the network medium.
- The process of transmitting and receiving signals over the network medium, including modulation schemes and timing/synchronization, voltage, and radio frequencies.

Physical Layer Hardware:

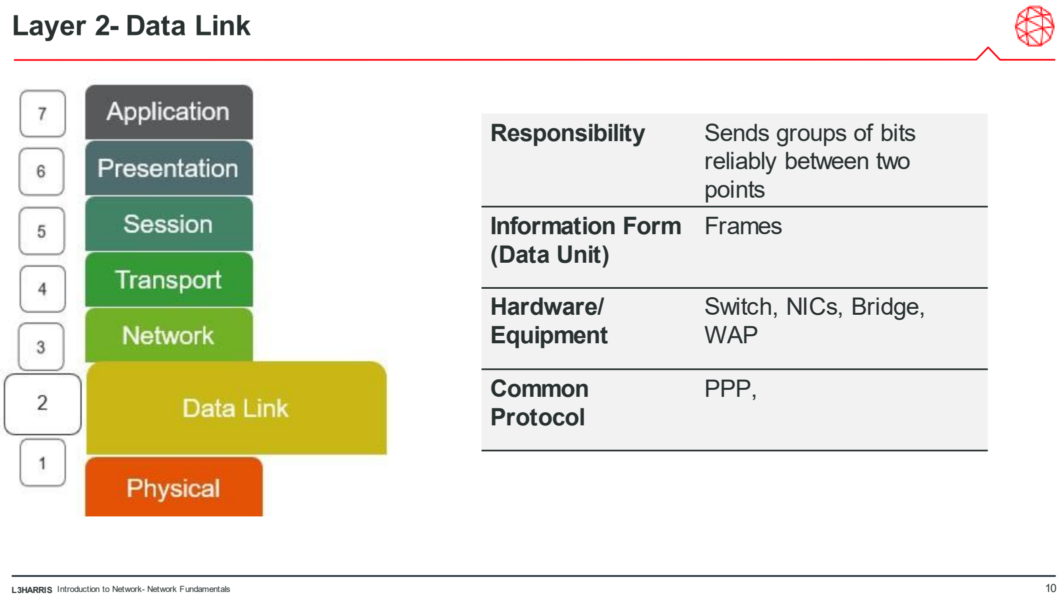
Devices:

- Transceivers—The part of a network interface that sends and receives signals over the network media.
- Repeaters—A device that amplifies an electronic signal to extend the maximum allowable distance for a media type.
- Hubs—A multiport repeater, deployed as the central point of connection for nodes.
- Media converters—A device that converts one media signaling type to another.
- Modems—A device that converts between digital and analog signal transmissions.

Transmission Media:

- Cabled- A physical signal conductor is provided between two nodes. Examples include cable types such as copper or fiber optic cable.

- Wireless- Uses free space between nodes (no signal conductor), such as microwave radio.



Layer 2- Data Link

7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

Responsibility	Sends groups of bits reliably between two points
Information Form (Data Unit)	Frames
Hardware/ Equipment	Switch, NICs, Bridge, WAP
Common Protocol	PPP,

L3HARRIS Introduction to Network- Network Fundamentals 10

The Data Link layer (layer 2) is responsible for transferring data between nodes on the same logical segment. At the Data Link layer, a segment is one where all nodes can send traffic to one another using hardware addresses, regardless of whether they share access to the same media.

- A layer 2 segment might include multiple physical segments. This is referred to as a **logical topology**.
- The Data Link layer organizes the stream of 1s and 0s (bits) arriving from the Physical layer into structured units called frames. Each frame contains a network layer packet as its payload.
- Concerned with local delivery of frames between nodes on the same level of network.
- The Data Link layer adds control information to the payload in the form of header fields. These fields include a source and destination hardware address. The last part of the frame usually contains some sort of error checking.
- The data link layer is responsible for flow control and error control in the intra-network communication.

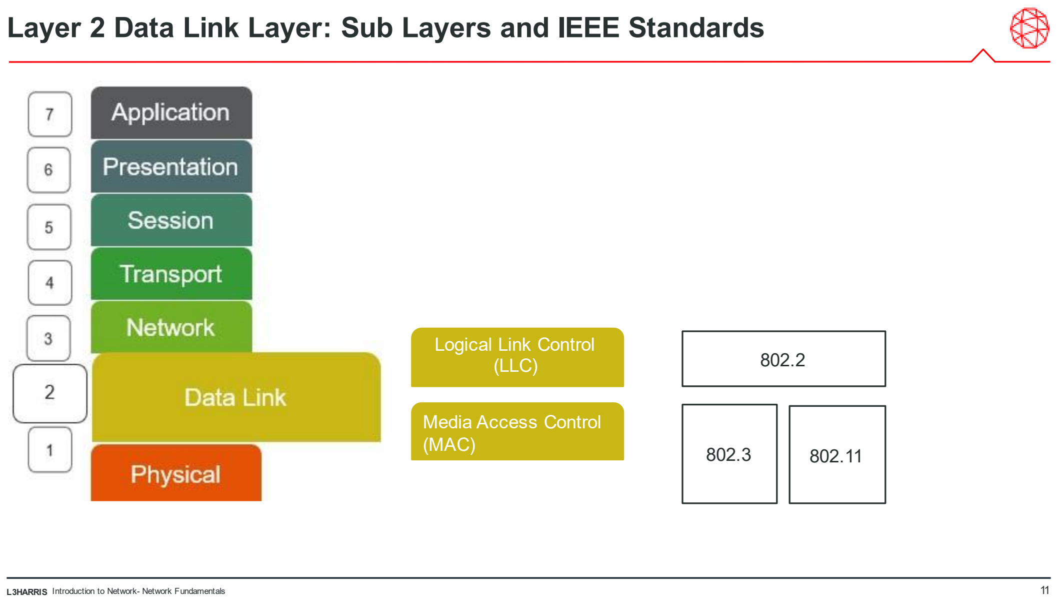
Data Link Layer Hardware:

- Network adapters or network interface cards (NICs)—A NIC joins a host to network media (cabling or wireless) and enables it to communicate over the network by assembling and disassembling frames.

- Bridges—A bridge joins two network segments while minimizing the performance reduction of having more nodes on the same network. A bridge has multiple ports, each of which functions as a network interface.

- Switches—An advanced type of bridge with many ports. A switch creates links between large numbers of nodes more efficiently.

- Wireless access points (APs)—An AP allows nodes with wireless network cards to communicate and creates a bridge between wireless networks and wired ones.



Layer 2 Data Link Layer: Sub Layers and IEEE Standards

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

Logical Link Control (LLC)

Media Access Control (MAC)

802.2

802.3

802.11

L3HARRIS Introduction to Network- Network Fundamentals 11

Over the years, many protocols, standards, and products have been developed to cover technologies working at the Physical and Data Link layers of the OSI model. The most important of these are the IEEE 802 standards, published by the LAN/MAN Standards Committee (ieee802.org) of the Institute of Electrical and Electronics Engineers (IEEE). The IEEE is a professional body that oversees the development and registration of electronic standards.

(Ethernet) and Media Access Control (MAC) Sublayer:

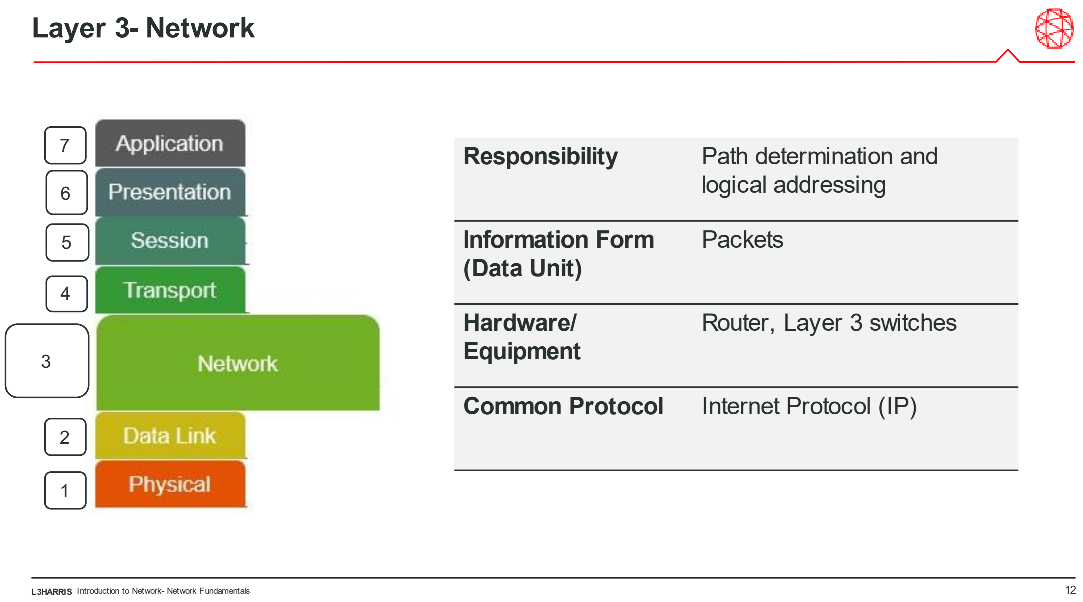
MAC sublayer manages the devices interaction and is responsible for the following:

- Logical topology
- Media access method—contention or token passing
- Addressing—the format for the hardware address of each network interface
- Frame format
- Error checking mechanism

Ethernet is now the only widely supported standard for cabled LANs. The IEEE 802.11 series of standards (Wi-Fi) are used to implement wireless local area networks (WLANs).

Logical Link Control (LLC) Sublayer:

This sublayer of the data link layer deals with multiplexing, the flow of data among applications and other services, and providing error messages and acknowledgements. The LLC protocol provides a standard Network-layer service interface, regardless of which MAC sublayer protocol is used.



Layer 3- Network

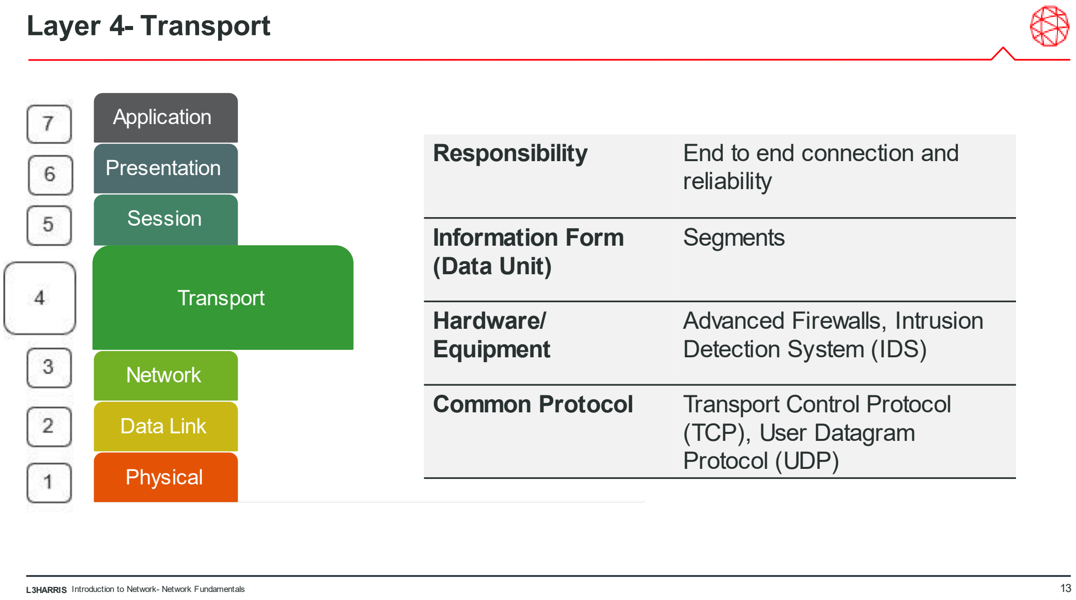
Responsibility	Path determination and logical addressing
Information Form (Data Unit)	Packets
Hardware/ Equipment	Router, Layer 3 switches
Common Protocol	Internet Protocol (IP)

The Network layer (layer 3) is responsible for moving data around a network of networks, known as an internetwork or the Internet. While the Data Link layer is capable of forwarding data by using hardware addresses within a single segment, the Network layer moves information around an internetwork by using logical network and host IDs. The networks are often heterogeneous; that is, they use a variety of Physical layer media and Data Link protocols.

The Network layer transfers information between networks by examining the destination Network-layer address or logical network address and routing the packet through the internetwork by using intermediate systems (routers). The packet moves, router by router (or hop by hop), through the internetwork to the target network. Once it has reached the destination network, the hardware address can be used to deliver the packet to the target node.

Network Layer Hardware:

- Router
- Layer 3 Switches (which combine the function of switches and routers, and basic firewalls)



Layer 4- Transport

7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

Responsibility	End to end connection and reliability
Information Form (Data Unit)	Segments
Hardware/ Equipment	Advanced Firewalls, Intrusion Detection System (IDS)
Common Protocol	Transport Control Protocol (TCP), User Datagram Protocol (UDP)

L3HARRIS Introduction to Network- Network Fundamentals 13

Layer 4 (Transport) is responsible for end-to-end communication between the two devices and the content of the packets starts to become significant.

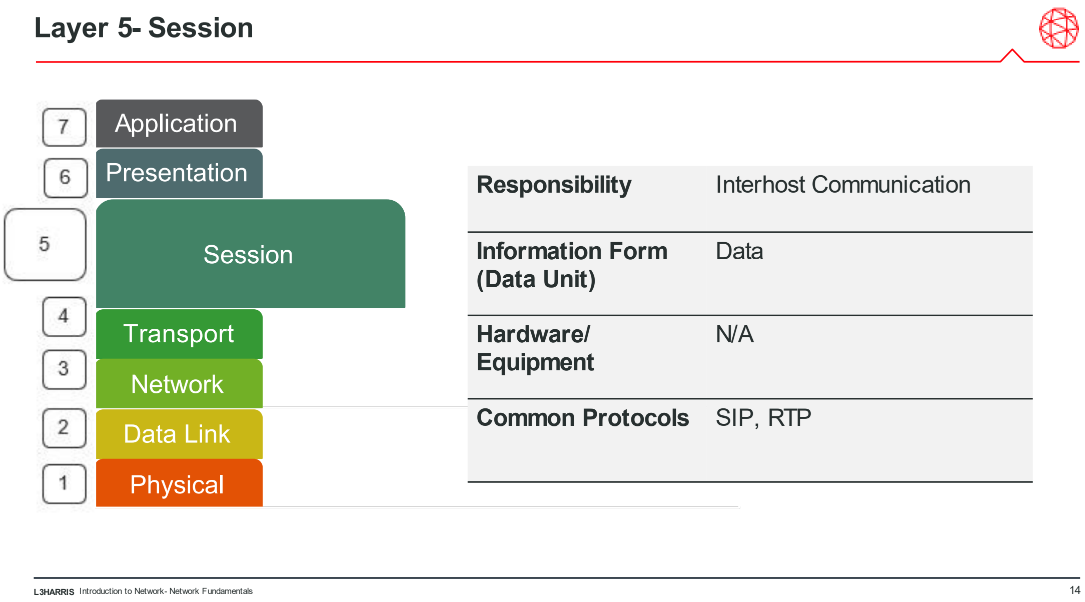
Any host can be transmitting any type of data at any given moment. It is a critical role of the transport layer to identify each type of network application by assigning it a **port number** and the transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

Example: Data from the HTTP web browsing application can be identified as port 80, while data from an email server can be identified as port 25.

The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection does not overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete and requesting a retransmission if it isn't.

Transport Layer Hardware:

- Multilayer switches
- Security appliances
  - Advanced firewalls
  - Intrusion detection systems (IDSs).



Layer 5- Session

Responsibility	Interhost Communication
Information Form (Data Unit)	Data
Hardware/ Equipment	N/A
Common Protocols	SIP, RTP

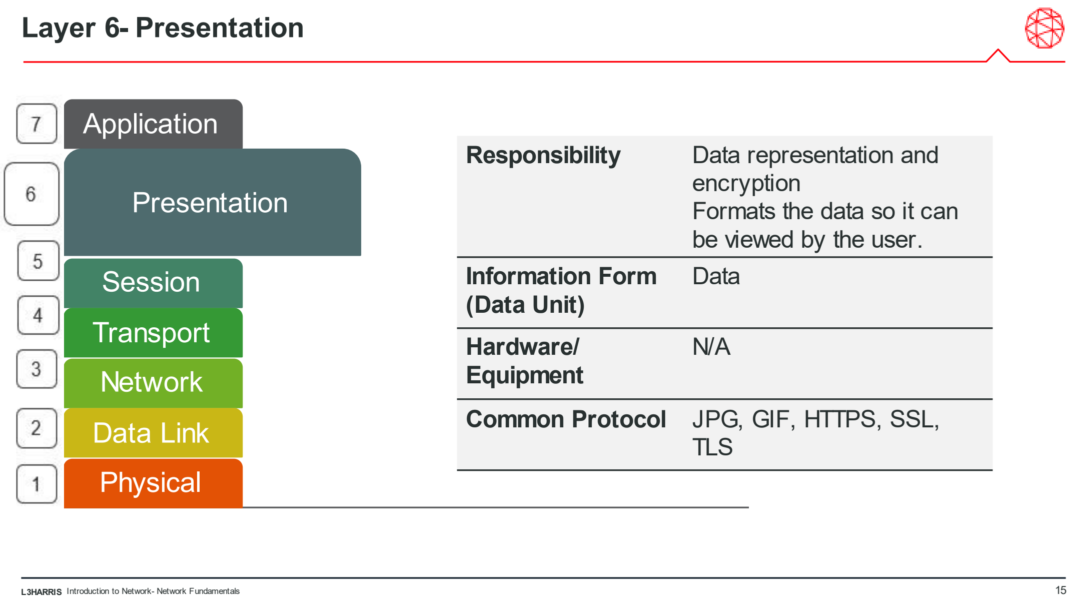
Most application protocols require the exchange of multiple messages between the client and server. This exchange of such a sequence of messages is called a session or dialog. The Session layer (Layer 5) represents the dialog control functions that administer the process of establishing the dialog, managing data transfer, and then ending (or tearing down) the session

Sessions can work in three modes:

- One-way/simplex—Only one system is allowed to send messages; the other only receives.

- Two-way alternate (TWA)/half-duplex—The hosts establish some system for taking turns to send messages, such as exchanging a token.

- Two-way simultaneous (TWS)/duplex—Either host can send messages at any time.



Layer 6- Presentation

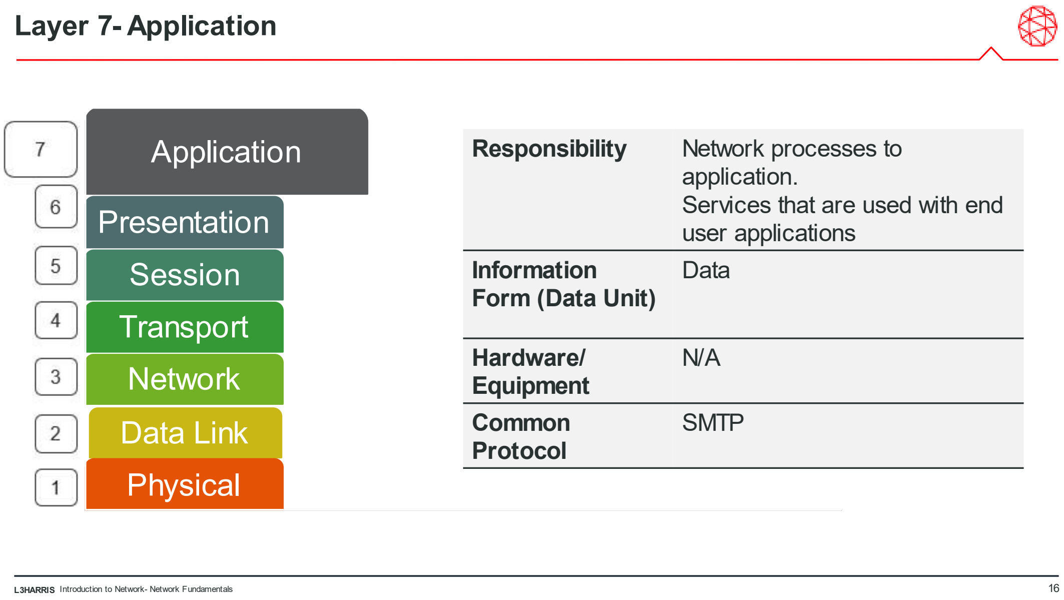
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

Responsibility	Data representation and encryption Formats the data so it can be viewed by the user.
Information Form (Data Unit)	Data
Hardware/ Equipment	N/A
Common Protocol	JPG, GIF, HTTPS, SSL, TLS

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it is also referred to as the syntax layer.

Think of this: Presentation layer is used for character set conversion. The communicating computers may use different character coding systems, such as American Standard Code for Information Interchange (ASCII) and Unicode; the peer Presentation layers agree to translate the data into one of the formats, or they will both translate the data into a third format.

The Presentation layer can also be conceived as supporting data compression and encryption. However, in practical terms, these functions are often implemented by encryption devices and protocols running at lower layers of the stack or simply within a homogenous Application layer.



Layer 7- Application

Responsibility	Network processes to application. Services that are used with end user applications
Information Form (Data Unit)	Data
Hardware/ Equipment	N/A
Common Protocol	SMTP

L3HARRIS Introduction to Network- Network Fundamentals 16

The Application layer (Layer 7) is at the top of the OSI stack. An application-layer protocol doesn't encapsulate any other protocols or provide services to any protocol. Application-layer protocols provide an interface for software programs on network hosts that have established a communications channel through the lower-level protocols to exchange data.

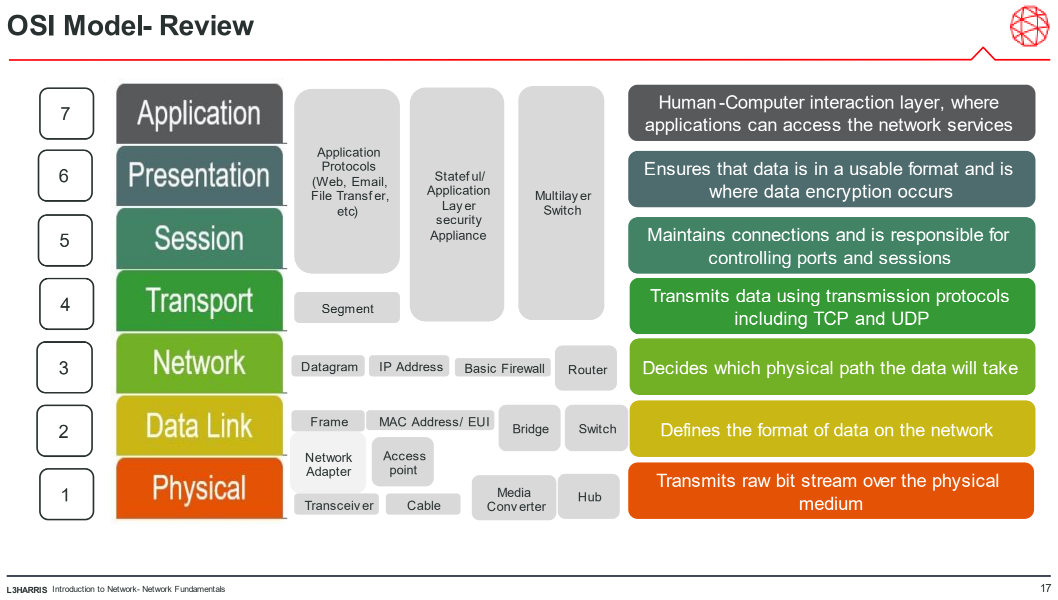
- At this layer, both the end user and the application layer interact directly with the software application.
- This layer sees network services provided to end- user applications such as a web browser or Office 365.
- The application layer identifies communication partners, resource availability, and synchronizes communication.

- An application-layer protocol doesn't encapsulate any other protocols or provide services to any protocol.

It is important to distinguish between network application protocols and the software application code (programs and shared programming libraries) that runs on computers. Software programs and operating systems make use of **application programming interfaces (APIs)** to call functions of the relevant part of the network stack.

Examples of APIs include:

- Network card drivers could use the Network Driver Interface Specification (NDIS) API to implement functions at the Data Link layer.
- The Sockets/WinSock APIs implement Transport- and Session-layer functions.
- High-level APIs implement functions for Application-layer services such as file transfer, email, web browsing, or name resolution.



OSI Model- Review

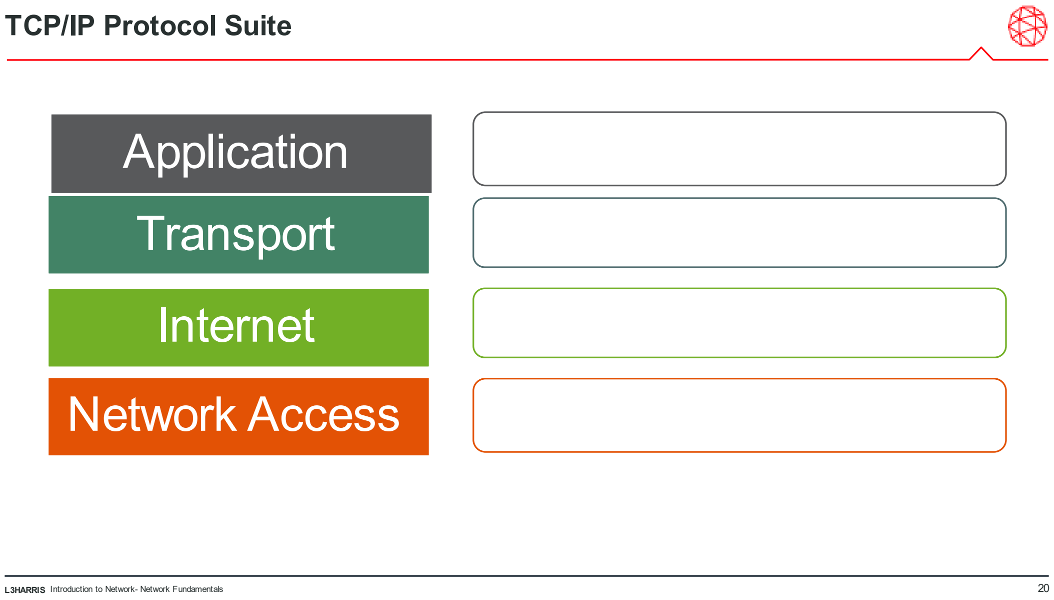
7	Application	Human-Computer interaction layer, where applications can access the network services
6	Presentation	Ensures that data is in a usable format and is where data encryption occurs
5	Session	Maintains connections and is responsible for controlling ports and sessions
4	Transport	Transmits data using transmission protocols including TCP and UDP
3	Network	Decides which physical path the data will take
2	Data Link	Defines the format of data on the network
1	Physical	Transmits raw bit stream over the physical medium

L3HARRIS Introduction to Network- Network Fundamentals 17

The image summarizes the OSI model listing the PDUs at each layer, along with the types of devices that work at each layer.

Answer the following questions to test your understating of the content covered in this topic.

1. What OSI model layer transmits bits from one device to another and modulates the transmission stream over a medium?
2. At which OSI layer do programs on a network node access network services?
3. Which OSI layer is responsible for establishing reliable connections between two devices?
4. Which OSI layer packages bits of data from the physical layer into frames?
5. As which sublayer of the OSI model do network adapter cards operate?
6. Which component is responsible for translating the computers digital signals into electrical or optical signals that travel on network cable?
7. Which OSI layer handles the concept of logical addressing?
8. At which OSI layer is the concept of a port number introduced?



TCP/IP Protocol Suite

Application

Transport

Internet

Network Access

L3HARRIS Introduction to Network- Network Fundamentals 20

The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.

The Transmission Control Protocol/Internet Protocol (**TCP/IP model**) is a concise version of the OSI model designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It contains four layers, unlike seven layers in the OSI model. The layers are:

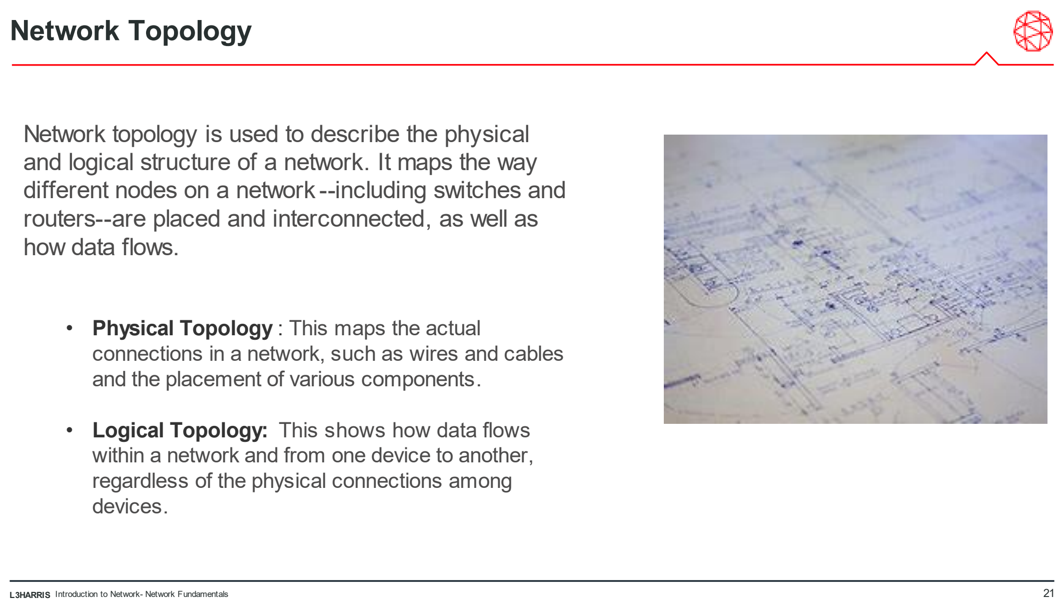
LINK/NETWORK INTERFACE LAYER The Link (or Network Interface) layer is the equivalent of the OSI Physical and Data Link layers. It defines the host's connection to the network media. This layer includes the hardware and software involved in the interchange of frames between hosts. The technologies used can be LAN-based (Ethernet or Wi-Fi) or WAN-based (T-carrier, ISDN, or DSL).

INTERNET LAYER The Internet (or more precisely Internetwork) layer provides addressing and routing functions. It also provides the ability to fragment large frames from the Network Interface layer into smaller packets. The Internet layer uses several protocols, notably the Internet Protocol (IP) and Address Resolution Protocol (ARP), to facilitate the delivery of packets.

TRANSPORT LAYER The Transport layer—or Host-to-Host layer—establishes connections between the different applications that the source and destination hosts are communicating with. It breaks Application-layer information into segments.

APPLICATION LAYER This is the layer at which many TCP/IP services (high-level protocols) can be run, such as FTP, HTTP, and SMTP.

TCP/IP Protocol Suite is supported on nearly every network host and network appliance. It is not the property of any one vendor, however. TCP/IP is an open standard to which anyone can suggest modifications and enhancements. Similarly, TCP/IP and the Internet are inextricably linked. Although no single organization owns the Internet or its technologies, several organizations are responsible for the development of the Internet and consequently TCP/IP.



Network Topology

Network topology is used to describe the physical and logical structure of a network. It maps the way different nodes on a network--including switches and routers--are placed and interconnected, as well as how data flows.

- **Physical Topology** : This maps the actual connections in a network, such as wires and cables and the placement of various components.
- **Logical Topology:** This shows how data flows within a network and from one device to another, regardless of the physical connections among devices.

L3HARRIS Introduction to Network- Network Fundamentals 21

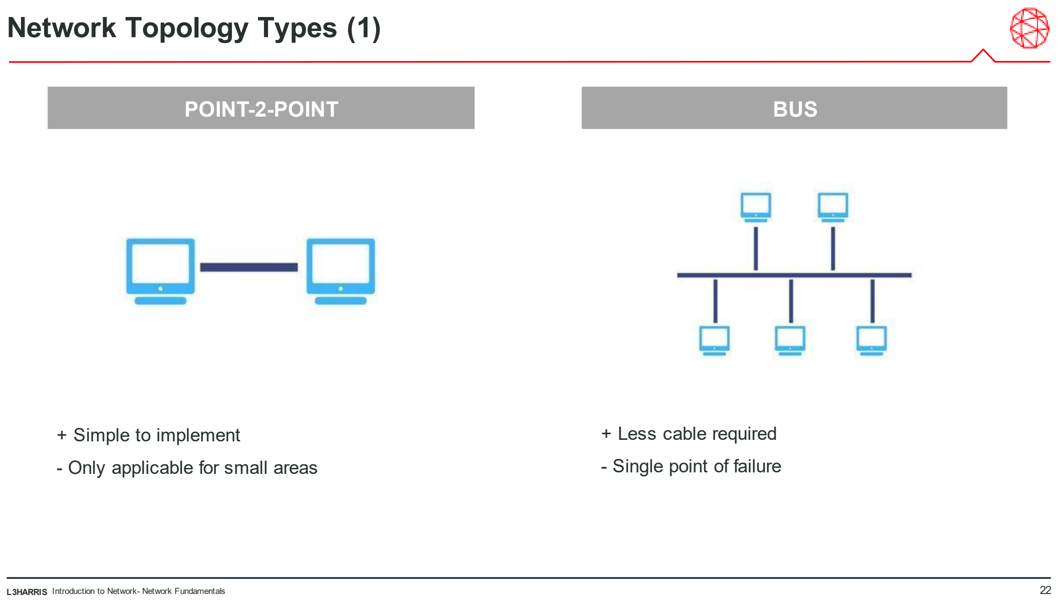
Network Topology refers to the arrangements, either **physical** or l**ogical**, of nodes and connections within a network. In other words, topology explains how a network is physically connected, and how the information in the network flows logically. The structure of a network can directly impact its functioning, therefore, selecting suitable topology for a network will bolster performance, enhance data efficiency, and optimize resource allocation and in turn, minimizes operating costs.

The choice of a topology for a network is influenced by several factors, the most important being the size and scale of the network as well as cost. Additional long-term factors to consider include:

- Configuration management
- Monitoring
- General performance

The network devices are depicted as nodes and the connections between the devices as lines to build a graphical model.

- Network topology diagrams allow IT teams to correctly configure, and maintain/ diagnose network problems related to connectivity, investigate high latency, and troubleshoot other network issues.



Network Topology Types (1)

POINT-2-POINT

+ Simple to implement
- Only applicable for small areas

BUS

+ Less cable required
- Single point of failure

L3HARRIS Introduction to Network- Network Fundamentals 22

Point-to-Point Topology

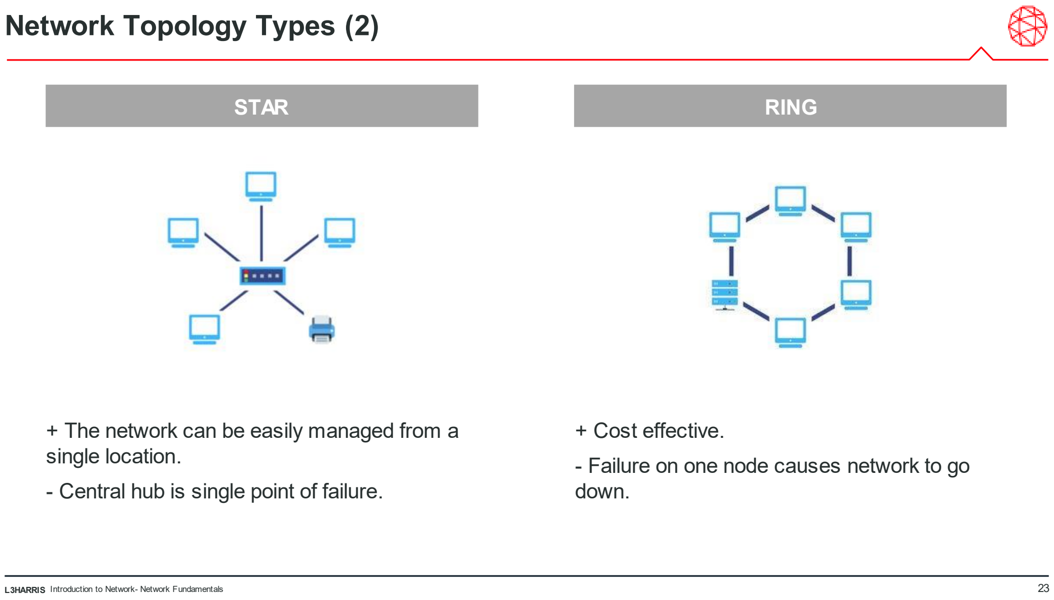
As the name suggests, the point-to-point is a network topology with a dedicated link between two endpoints, hence it is the simplest topology. The advantage of such a network is that all the available network bandwidth is dedicated to the two connected devices. You are not likely to use the point-to-point topology in your office network setup.

- <u>Advantages:</u> superior bandwidth, simple to implement, easy to maintain
- <u>Disadvantages:</u> only applicable for small areas, high dependance on the common link, only useful for 2 nodes

BUS Topology

A bus topology consists of a single cable, also called a bus, running from one end of the network to the other. In this network arrangement, each node is connected to the central cable or bus by interface connectors. A signal containing the address and data transmitted from the source node travels in both directions to all nodes until it reaches the destination noted which accepts the data. If the address of the delivered signal doesn’t match that of the receiving node, the data portion of the signal is ignored.

- <u>Advantages:</u> easy to add/ swap devices without affecting other networked devices, failure in a few devices does not affect other devices or the network, less cable required compared to other topologies.
- <u>Disadvantages:</u> device failure and other network faults can be hard to locate, damage to the backbone cable can halt entire network, increase in bandwidth on a few devices can impact the performance of the network, slower- only one node transmits data at a time, data loss over long distances.



Network Topology Types (2)

STAR

+ The network can be easily managed from a single location.

- Central hub is single point of failure.

RING

+ Cost effective.

- Failure on one node causes network to go down.

L3HARRIS Introduction to Network- Network Fundamentals 23

Star Topology:

A star topology is the one in which each peripheral node is connected to a central hub or switch. It is probably the most used network topology for LAN because it is considered the easiest topology to design and implement. The central hub functions as the server for the peripheral nodes or clients. All the network traffic passes through the central hub, and this is the only requirement for the topology to be classified as a star topology; the network doesn't have to resemble a star in the physical arrangement.

Advantages:

- The design and implementation are simple.
- It uses relatively less cabling, hence it's less labor-intensive.
- The whole network can be easily managed from a single location.
- Since the nodes are independently connected to the hub, a problem with one node won't affect the entire network.
- New nodes can be added or removed without taking the whole network offline.
- Troubleshooting and network maintenance are easier.

Disadvantages:

- Since all the traffic passes through the central hub, it is the single point of failure, which isn't ideal.
- The network performance and overall bandwidth are limited by the technical specifications of the central hub.

Ring Topology:

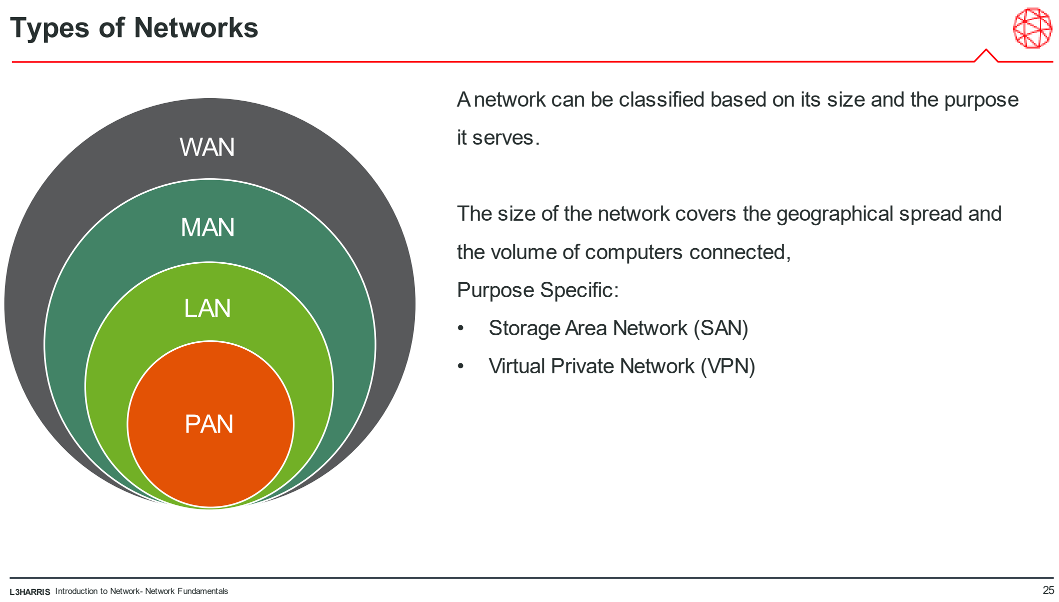
Each node has exactly two peers and the data travels in one direction passing through each intermediate node on the ring until it reaches the destination node. Data can be made to pass in both directions by adding a second connection between the network nodes, creating a dual ring topology. In a ring topology, an electrical “token” circulates around the network. Any node that wants to transmit data must wait until it has possession of the token.

Advantages:

- Since only one node can transmit data at a time, which reduces packet collisions, ring topologies are efficient at data transmission.
- Ring topologies are cost-effective, and installation is relatively inexpensive.
- Identifying and troubleshooting are easier due to the intricate node-to-node connectivity.

Disadvantages:

- If one node fails, the entire network will go down.
- Large ring networks suffer from slow transmission because the network bandwidth is shared by all the devices.
- It is easy to overburden the network resources and capacity.
- Adding or removing nodes requires the entire network to be taken offline.


WAN
MAN
LAN
PAN

Types of Networks

A network can be classified based on its size and the purpose it serves.

The size of the network covers the geographical spread and the volume of computers connected,

Purpose Specific:

- Storage Area Network (SAN)
- Virtual Private Network (VPN)

L3HARRIS Introduction to Network- Network Fundamentals 25

As stated, a network can be classified based on its size and the purpose it serves. The size of the network covers the geographical spread and the volume of computers connected, two common network types are LAN and WAN.

- **PAN- Personal Area Network:** This type of network is used on a personal level using devices such as smartphones, tablets, and laptops. This type of connection is generally via wireless technologies such as Bluetooth, infrared, or NFC. This connection can also be established via cabling such as a USB Cable. PANs are generally used to transfer small files such as music, photos, even payment.
- **Local Area Network (LAN)-** A local area network can span a single building or multiple buildings and are typically owned, controlled, and managed "in house" by the person or organization where they are deployed. Because of the smaller footprint, LANs are generally faster and cost-effective while offering better security and fault tolerance.
- Wireless local area networks are referred to as WLAN's. This type of LAN does not rely on cables to connect the network. One example of this is a printer and/or laptop connected via Wi-Fi.
  - Nodes: Forward communications within the same physical network, referred to switching.
  - Transmission Media: Common examples include ethernet or 802.11 wireless technology
- **Metropolitan Area Network (MAN)-** This term is sometimes used for something smaller than a WAN: a city-wide network encompassing multiple buildings.
- **Wide Area Network (WAN)-** A wide area network footprint is much larger, spanning a broad distance such as cross metropolitan, regional, or national boundaries over a long distance and are comprised of many smaller LAN's. WANs are typically connected through public networks

such as the public switched telephone network (PTSN) and are often established by service providers that then lease to businesses, schools, government, or the public.

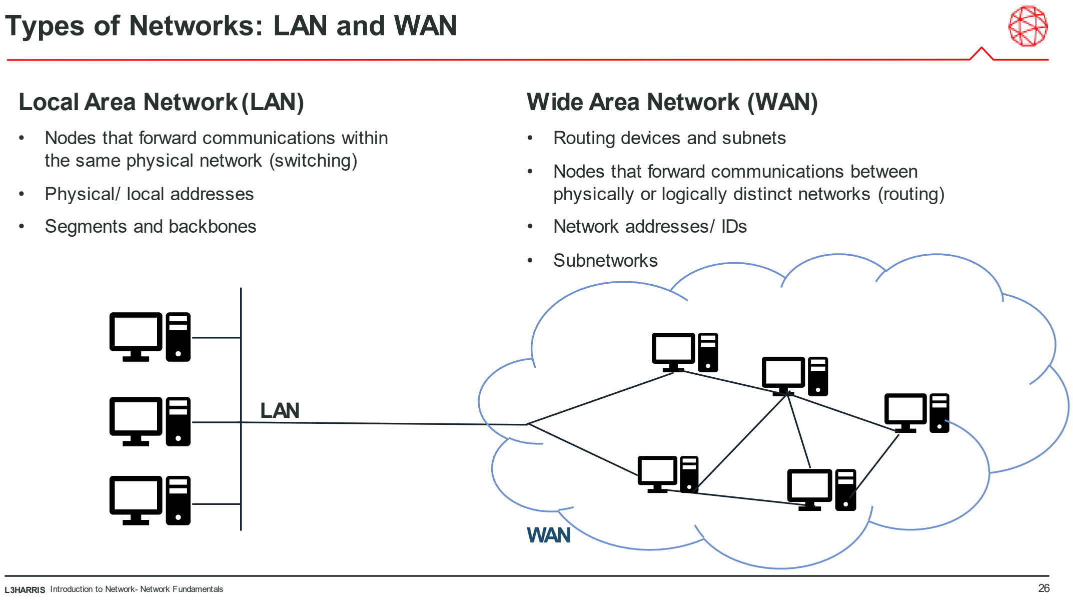
  - Nodes: Forward communications between physically or logically distinct networks, referred to as routing.
  - Transmission Media: Common examples include copper and fiber cabling.

Purpose Specific Network Types:

- **Network Storage Area (NAS**) – Contains multiple drives and can store large amounts of data.
- **Storage Area Network (SAN)**- Designed to handle large data transfers and storage. The purpose of this network is to move larger, more complex storage resources away from the network into a separate high-performance atmosphere. Doing this not only allows for easy retrieval and storage of the data but it also frees up space and improves overall performance of the original network.
- **Virtual Private Network (VPN)-** The point of a VPN is to increase security and privacy while accessing a network. The VPN ats as a middleman between you and the network by encrypting your data and hiding your identity.

The **Internet** is a worldwide network of networks based on the TCP/IP protocol. The uncapitalized term internet (or internetwork) is also used to describe any series of interconnected networks running Internet Protocol (IP).

- An **intranet** uses the same technologies as the Internet, but it is owned and managed by a company or organization. An intranet could be implemented as a LAN or WAN.
- An **extranet** is an intranet that is also accessible to selected third parties, such as customers or suppliers.



Types of Networks: LAN and WAN

Local Area Network (LAN)

- Nodes that forward communications within the same physical network (switching)
- Physical/ local addresses
- Segments and backbones

Wide Area Network (WAN)

- Routing devices and subnets
- Nodes that forward communications between physically or logically distinct networks (routing)
- Network addresses/ IDs
- Subnetworks

L3HARRIS Introduction to Network- Network Fundamentals 26

As stated, a network can be classified based on its size and the purpose it serves. The size of the network covers the geographical spread and the volume of computers connected, two common network types are LAN and WAN.

Local Area Network (LAN)

LAN stands for local area network and is the most common and popular network design found in most businesses and homes. It is a network that interconnects devices in a limited geographical area.

- Nodes that forward communications within the same physical network (switching)
- Physical/ local addresses
- Segments and backbones

Wide Area Network (WAN)

- Routing devices and subnets
- Nodes that forward communications between physically or logically distinct networks (routing)
- Network addresses/ IDs
- Subnetworks

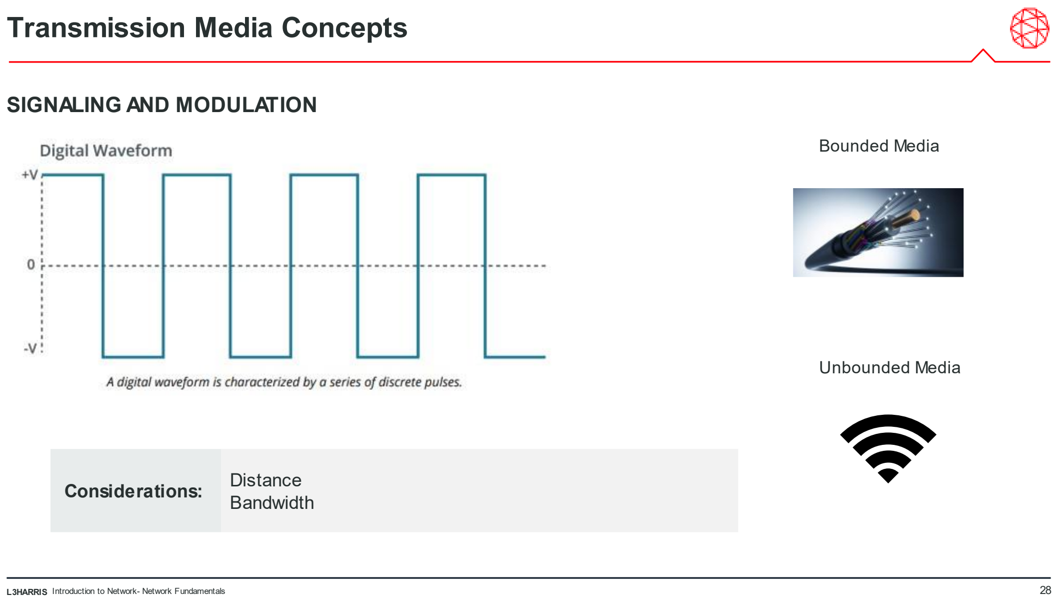
The more you know:

- In most cases, LANs connect to WANs
- An example of a WAN you are familiar with – the internet
- An example of a LAN you are familiar with- your home

Media Types and Access methods

The manner in which data is transmitted between nodes on a network can significantly affect network traffic and performance. Understanding primary data methods is crucial to monitoring network performance and response time.

Notes:



Transmission Media Concepts

SIGNALING AND MODULATION

A digital waveform is characterized by a series of discrete pulses.

Bounded Media

Unbounded Media

Considerations:	Distance Bandwidth

L3HARRIS Introduction to Network- Network Fundamentals 28

Transmission media is a communication channel which uses a transmission medium to carry data from the transmitter to the receiver, providing a pathway over which data can travel from sender to receiver.

Transmission media can be classified into two groups-

- **Bounded Media** (Cabled): A physical signal conductor between two nodes.
  - Ex. Copper, Fiberoptic
- **Unbounded Media** (Wireless): Uses free space between nodes without a wired medium
  - Ex. Microwave, Radio wave

Signaling and modulation:

Computers can only process information in digital format, meaning that information is sent in the form of data by converting information into binary values (1's and 0's). These binary digits are then encoded into a signal, which is essentially a series of discrete pulses that represent the ones and zeros of binary digital data and are implemented by:

- high and low voltages
- on/off light transmission

This makes the transmission less susceptible to interference and makes it easier to regenerate the transmission over longer distances.

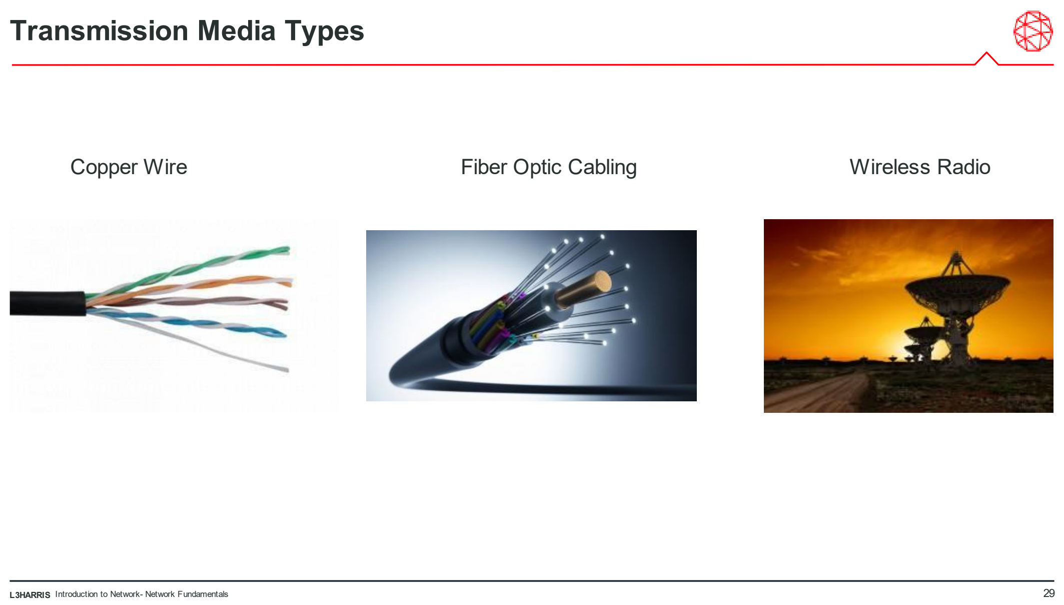
**If the transmission media only supports analog signaling, a more complex modulation scheme is required to represent the digital information as it is transmitted over the analog channel. For a more information on this concept research "Nyquist Theorem".

Distance limitations, attenuation, and noise: Each type of media can consistently support a given data rate only over a defined distance. Some media types support higher data rates over longer distances then others. Attenuation and noise enforce distance limitations on different media types.

- **Attenuation** is the loss of signal strength, expressed in decibels (dB). dB expresses the ration between two measurements: in this case, signal strength at origin and signal strength at destination.
- **Noise** is anything that gets transmitted within or close to the channel that isn't the intended signal. This serves to make the signal itself difficult to distinguish, causing error in data and forcing retransmissions. This is expressed as the signal to noise ratio (SNR).

Bandwidth, baud, and bit rate:

- Bandwidth: The range of frequencies available to the communications channel
  - Channel Capacity: bandwidth is measured in unites of time called hertz (HZ) representing the number of signaling cycles that can be completed per second.
  - Data Rate: Bandwidth is also often used in data communications to explain the amount of information that can be transferred per second. When referring to data rate one must distinguish between the following terms.
    - Baud Rate: The number of symbols that can be transmitted per second, measured in hertz (MHz or GHz).
    - Bit Rate: The amount of information that can be transmitted, measured in bits per second (bps).



Transmission Media Types

Copper Wire

Fiber Optic Cabling

Wireless Radio

L3HARRIS Introduction to Network- Network Fundamentals 29

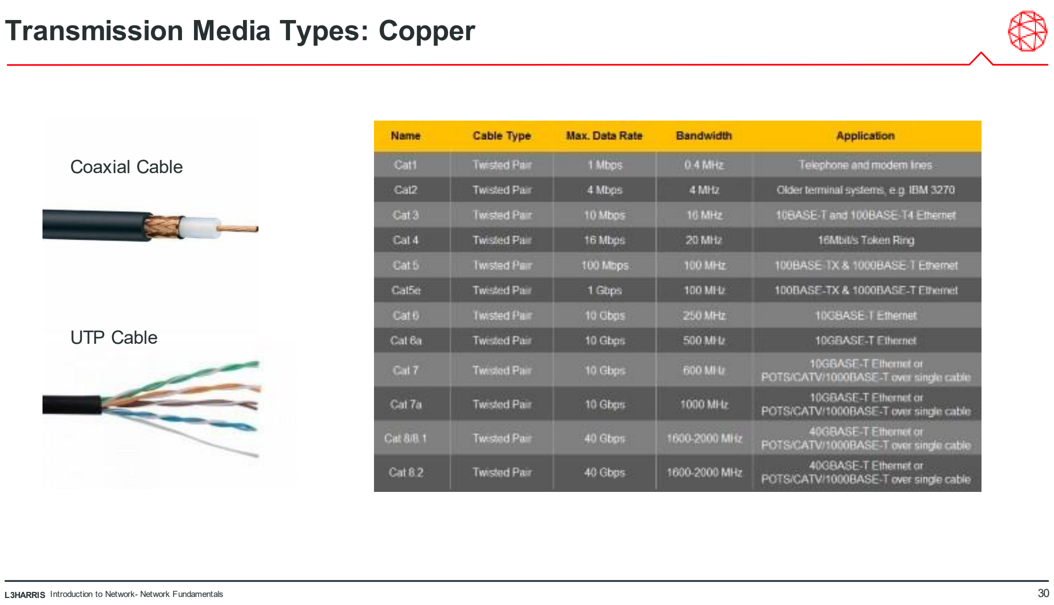
Twisted Pair cabling is the most basic networking media type and is the foundation of our ethernet networks. One pair of insulated wires twisted together forms a balanced pair. The pair carry the same signal but with different polarity; one wire is positive, and the other is negative.

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)- Makes use of a metallic shield to wrap the wires, reducing interference to a better extend than UTP.

Coaxial cable (coax) is a type of electrical cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield.

Fiber Optic Cable carries very high frequency radiation in the infrared light part of the electromagnetic spectrum. Even though high frequencies are used, they are very closely contained within the optical media and can propagate more easily. The light signals are also not susceptible to interference or noise from other sources. Consequently, fiber optic cable supports higher bandwidth over longer links than copper cable.

(Wireless) **Radio Frequency (RF)** carries very high frequency radiation in the infrared light part of the electromagnetic spectrum. Even though high frequencies are used, they are very closely contained within the optical media and can propagate more easily. The light signals are also not susceptible to interference or noise from other sources. Consequently, fiber optic cable supports higher bandwidth over longer links than copper cable.



Transmission Media Types: Copper

Coaxial Cable
UTP Cable

Name	Cable Type	Max. Data Rate	Bandwidth	Application
Cat1	Twisted Pair	1 Mbps	0.4 MHz	Telephone and modem lines
Cat2	Twisted Pair	4 Mbps	4 MHz	Older terminal systems, e.g. IBM 3270
Cat 3	Twisted Pair	10 Mbps	16 MHz	10BASE-T and 100BASE-T4 Ethernet
Cat 4	Twisted Pair	16 Mbps	20 MHz	16Mbit/s Token Ring
Cat 5	Twisted Pair	100 Mbps	100 MHz	100BASE-TX & 1000BASE-T Ethernet
Cat5e	Twisted Pair	1 Gbps	100 MHz	100BASE-TX & 1000BASE-T Ethernet
Cat 6	Twisted Pair	10 Gbps	250 MHz	10GBASE-T Ethernet
Cat 6a	Twisted Pair	10 Gbps	500 MHz	10GBASE-T Ethernet
Cat 7	Twisted Pair	10 Gbps	600 MHz	10GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable
Cat 7a	Twisted Pair	10 Gbps	1000 MHz	10GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable
Cat 8/8.1	Twisted Pair	40 Gbps	1600-2000 MHz	40GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable
Cat 8.2	Twisted Pair	40 Gbps	1600-2000 MHz	40GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable

L3HARRIS Introduction to Network- Network Fundamentals 30

Copper cable is the most common cable used in ethernet networks to connect nodes, creating a low voltage electrical circuit between the interfaces on the nodes, enabling the transmission of electrical signals.

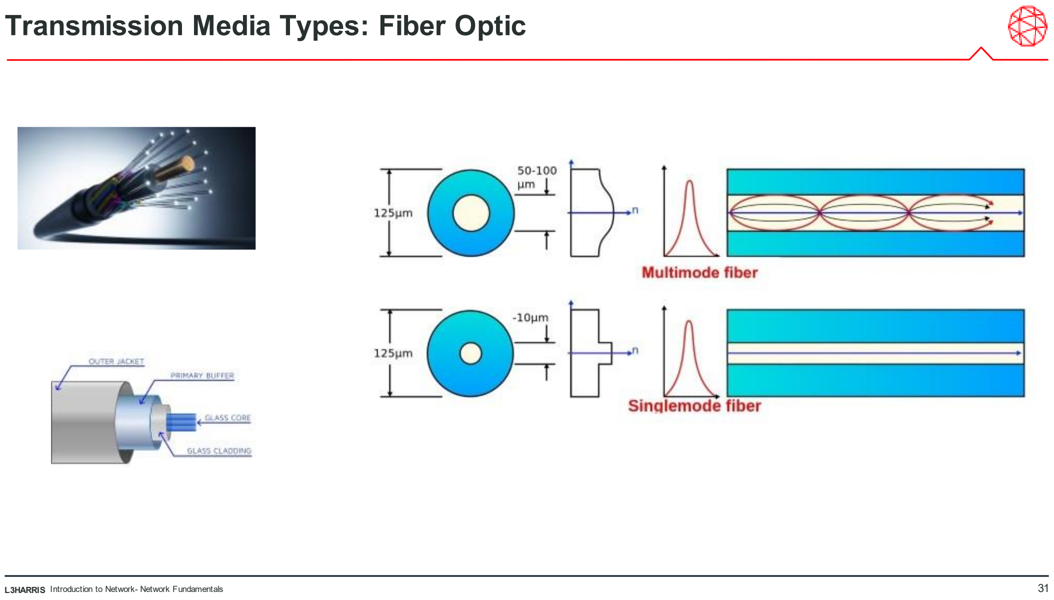
There are two main types of copper cable: twisted pair and coaxial (coax).

- **Twisted Pair** cabling is the most basic networking media type and is the foundation of our ethernet networks. A twisted pair ethernet cable is made of four pairs of wires twisted around each other. These wires send equal and opposite signals down both sides which is referred to as transmit positive (+) and transmit negative (–) or receive positive (+) and receive negative (-). The twisted wire is always moving away from noise or interference that may be occurring close to the cable, this allows us to compare those signals on the other end, reconstruct what may have been damaged or interfered with during the transmission and be able to properly receive the total signal. Note the different pairs have different twist rates, which is another way that we can use to be able to reconstruct that signal on the other side.
- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)

Coaxial cable (coax) is a type of electrical cable consisting of an inner conductor surrounded by a concentric conducting shield, with the two separated by a dielectric (insulating material); many coaxial cables also have a protective sheath or jacket.

<u>Limitations:</u>

Electrical signals are susceptible to interference and dispersion. There is some degree of impedance in the copper conductor; signals can leak easily from the wire, and noise can also leak into the wire. This means that copper cable suffers from high attenuation, meaning that the signal loses strength over long links.



Transmission Media Types: Fiber Optic

L3HARRIS Introduction to Network- Network Fundamentals 31

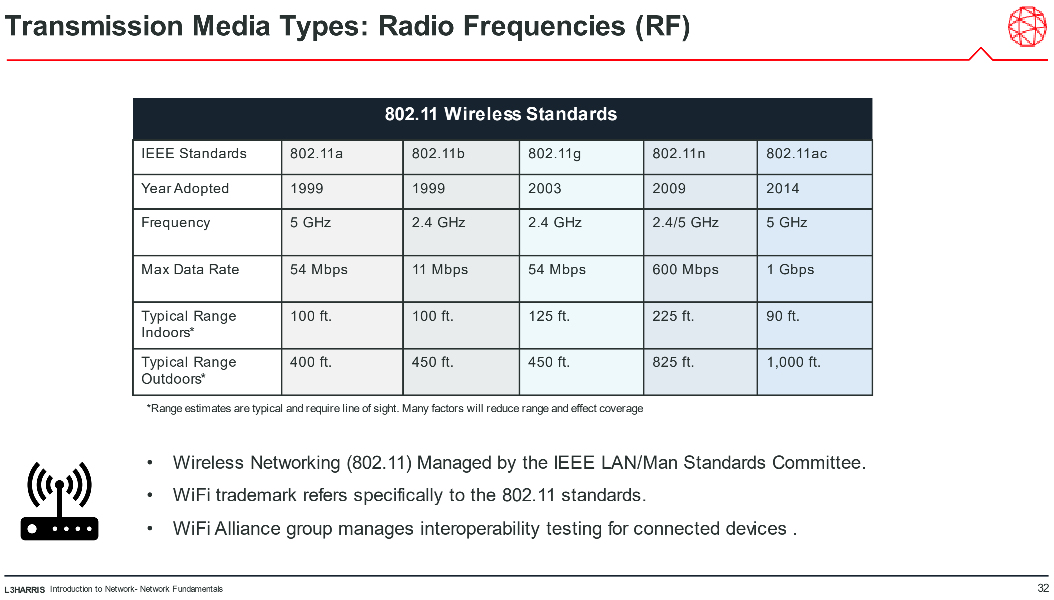
Fiber optic cable carries very high frequency radiation in the infrared light part of the electromagnetic spectrum. Even though high frequencies are used, they are very closely contained within the optical media and can propagate more easily. The light signals are also not susceptible to interference or noise from other sources. Consequently, fiber optic cable supports higher bandwidth over longer links than copper cable.

A single optical fiber is constructed from three elements:

- **Core** provides the transmission path for the light signals (waveguide).
- **Cladding** reflects signals back into the waveguide as efficiently as possible so that the light signal travels along the waveguide by multiple internal reflections.
- **Buffer** is a protective plastic coating. In basic operation modes, each fiber optic strand can only transfer light in a single direction at a time. Therefore, multiple fibers are often bundled within a cable to allow simultaneous transmission and reception of signals or to provide links for multiple applications.

Fiber optic cables fall into two broad categories: single mode and multimode.

- **Single Mode Fiber (SMF)** has a small core (8 to 10 microns) and a long wavelength, near infrared (1310 nm or 1550 nm) light signal, generated by a laser. Single mode cables support data rates up to 10 Gbps or better and cable runs of many kilometers, depending on the quality of the cable and optics.
- **Multimode Fiber (MMF)** has a larger core (62.5 or 50 microns) and shorter wavelength light (850 nm or 1300 nm) transmitted in multiple waves of varying length. MMF uses less expensive optics and consequently is less expensive to deploy than SMF. However, it does not support such high signaling speeds or long distances as single mode and so is more suitable for LANs than WANs.
  - MMF is categorized by Optical Mode designations (OM1, OM2, OM3, and OM4).



Transmission Media Types: Radio Frequencies (RF)

802.11 Wireless Standards					
IEEE Standards	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

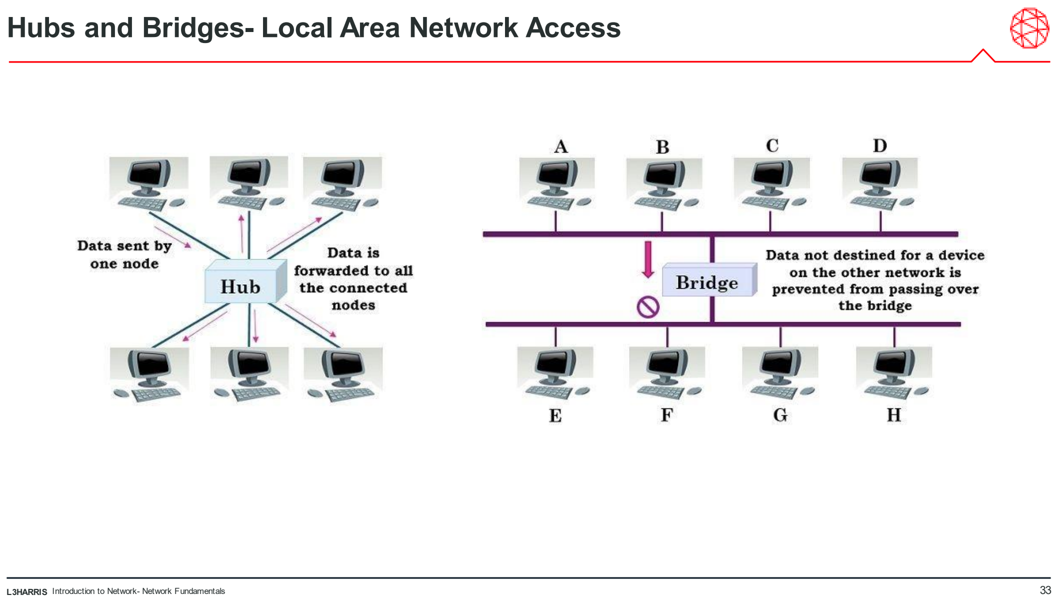
*Range estimates are typical and require line of sight. Many factors will reduce range and effect coverage

- Wireless Networking (802.11) Managed by the IEEE LAN/Man Standards Committee.
- WiFi trademark refers specifically to the 802.11 standards.
- WiFi Alliance group manages interoperability testing for connected devices .

L3HARRIS Introduction to Network- Network Fundamentals 32

Radio frequency (RF) waves can propagate through the air between sending and receiving antennas. This requires much more power than with electrical signals passing over copper conductors, however. The use of the radio part of the electromagnetic spectrum is regulated by national governments and (to some extent) standardized internationally by the International Telecommunications Union (ITU). Use of many frequency bands requires a license from the relevant government agency.

Wireless radio networking products operate in the high-frequency (microwave), unregulated Industrial, Scientific, and Medical (ISM) bands (2.4 GHz and 5 GHz). In these bands, there is a limit on power output, and there is also often substantial interference, which means range is limited. Also, each product must work within a narrow frequency range, allowing bandwidths in the MHz ranges only.



Hubs and Bridges- Local Area Network Access

Data sent by one node
Hub
Data is forwarded to all the connected nodes
A
B
C
D
Bridge
Data not destined for a device on the other network is prevented from passing over the bridge
E
F
G
H

L3HARRIS Introduction to Network- Network Fundamentals 33

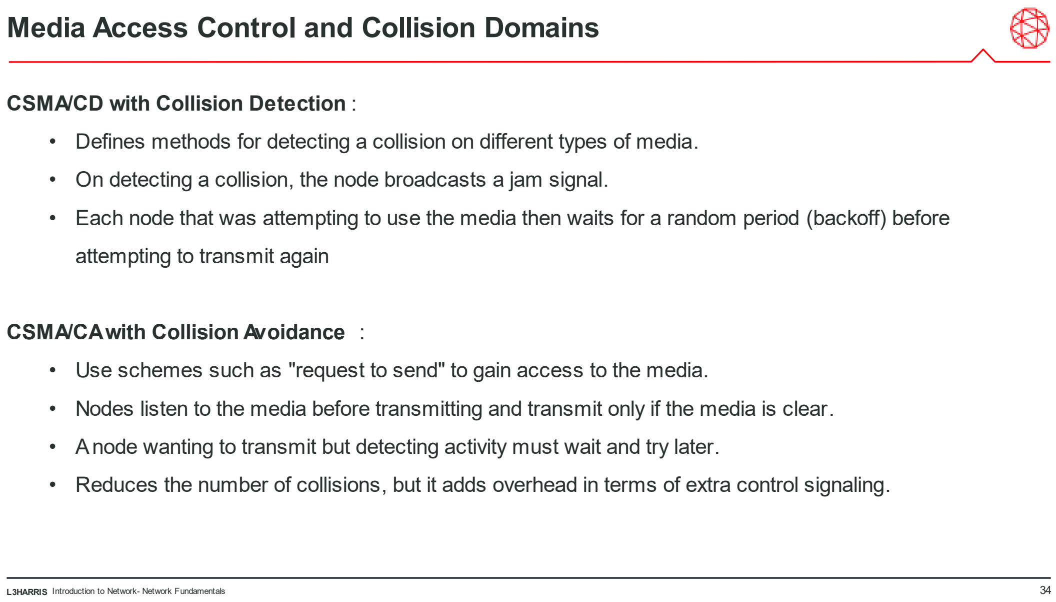
Most Ethernet networks are implemented so that each node is wired to a central networking device, such as a hub, bridge, or switch. The crucial difference between the hub and bridge is that the hub works on the **physical layer**, but the bridge operates on the **data link layer** of the OSI model. Both hub and bridge serve the different purpose.

A hub transmits the data to each device connected to it **broadcasting** the data.

On the other hand, a bridge is more intelligent which checks and filter data before forwarding it, this mechanism significantly reduces the network traffic and improve security.

Key Differences Between Hub and Bridge:

1. A hub is used as a central device for providing the connection among the various nodes. On the contrary, the bridge serves the purpose of filtering and forwarding of the data in the network.
2. Hubs are of two types – active and passive. As against, transparent, translational and source route are the three types of bridges.
3. Data filtration is carried out in the bridge while it is not performed in the hub.
4. Hub uses multiple ports while the bridge employs a single incoming and outgoing port for the specific data.



Media Access Control and Collision Domains

CSMA/CD with Collision Detection :

- Defines methods for detecting a collision on different types of media.
- On detecting a collision, the node broadcasts a jam signal.
- Each node that was attempting to use the media then waits for a random period (backoff) before attempting to transmit again

CSMA/CA with Collision Avoidance :

- Use schemes such as "request to send" to gain access to the media.
- Nodes listen to the media before transmitting and transmit only if the media is clear.
- A node wanting to transmit but detecting activity must wait and try later.
- Reduces the number of collisions, but it adds overhead in terms of extra control signaling.

L3HARRIS Introduction to Network- Network Fundamentals 34

A multiple access area network must share the available communications capacity between the various nodes that use it. Media access control (MAC) refers to the methods a network technology uses to determine when nodes can communicate on the media and to deal with possible problems, such as two devices attempting to communicate simultaneously.

Controlled or deterministic media access: A central device or system specifies when and for how long each node can transmit. (ex. Token Ring) Deterministic access methods are beneficial when network access is time critical. For example, in an industrial setting, key control and safety equipment, such as flow-shutoff sensors in chemical storage facilities, must have a guaranteed transmission time. Deterministic systems ensure that a single node cannot saturate the media allowing all nodes a chance to transmit.

Contention-based MAC system: Each network node within the same collision domain competes with the other connected nodes for use of the transmission media. A collision domain includes all the hosts attached to the same cable segment or connected via the same hub. When two nodes transmit at the same time, the signals are said to collide and neither signal can reach its destination. This means that they must be re-sent, reducing available bandwidth.

The collisions become more frequent as more nodes are added, and consequently the effective data rate is reduced.

The Ethernet protocols governing contention and media access are called **Carrier Sense Multiple Access (CSMA) protocols**:

Carrier sense—detect activity on the media

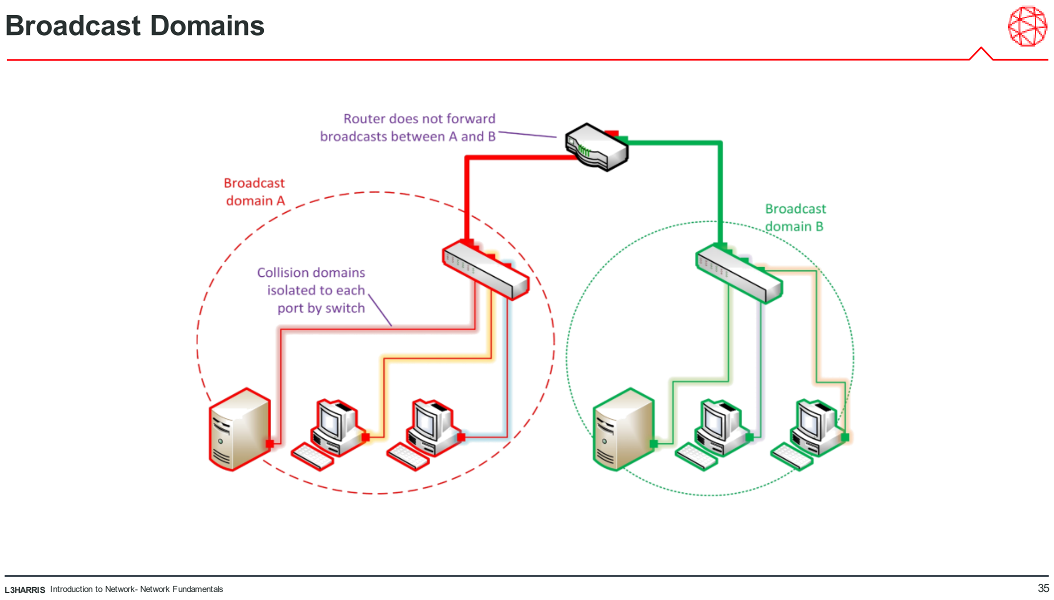
Multiple access—multiple nodes using the same media

Use of these protocols enforces limitations on the minimum and maximum lengths of cable that can be used, and the size of frames transmitted. Each frame must fill the cable segment before the end of transmission is reached, or a frame could be sent and involved in a collision and lost without the sending node being aware of it. Ethernet shared access using CSMA protocols use **half-duplex transmissions**. This means that a node can transmit or receive but it cannot do both at the same time. There are two types of CSMA protocols:

- **CSMA/CD with Collision Detection**:
    - Ethernet's Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol defines methods for detecting a collision on different types of media. In most cases, this is when a signal is present on the interface's transmit and receive lines simultaneously. On detecting a collision, the node broadcasts a jam signal. Each node that was attempting to use the media then waits for a random period (backoff) before attempting to transmit again.
- **CSMA/CA with Collision Avoidance**:
    - CSMA WITH COLLISION AVOIDANCE The Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocols use schemes such as "request to send" to gain access to the media. Nodes listen to the media before transmitting and transmit only if the media is clear. A node wanting to transmit but detecting activity must wait and try later. This reduces the number of collisions, but it adds overhead in terms of extra control signaling. The IEEE 802.11 WiFi standard uses CSMA/CA

Switched Networks: Contention-based access methods do not scale to large numbers of nodes within the same collision domain. This problem is overcome by using switches as each switch port is in a separate collision domain. By eliminating the effect of contention, switches allow for **full-duplex transmissions**, where a node can transmit and receive simultaneously. When a link is configured as full duplex, the CSMA/CD protocol is not used.

With switches, collisions occur only if the device attached to a switch port is operating in half-duplex mode.



Broadcast Domains

Router does not forward broadcasts between A and B
Broadcast domain A
Broadcast domain B
Collision domains isolated to each port by switch

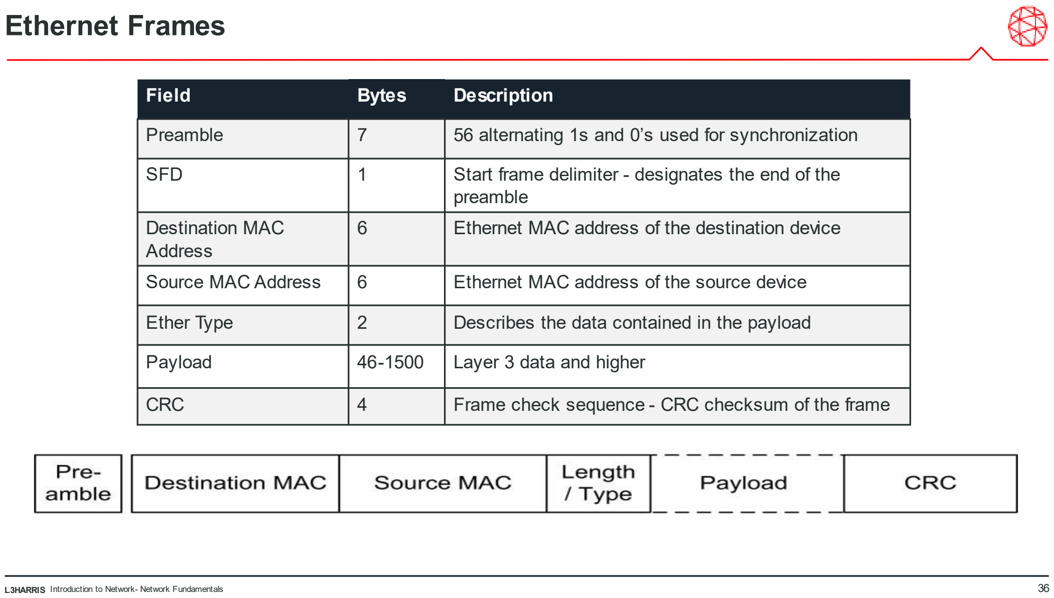
Within a collision domain on a shared medium, any given node will receive all the traffic transmitted within that domain. However, it will choose to process only traffic that is specifically addressed to it. This is referred to as **unicast traffic**, which is traffic that is addressed by the sender to a single recipient.

It is useful to have a mechanism to transmit the same traffic to multiple nodes. This is referred to as **broadcast traffic**. This is accomplished using a special type of destination address.

- Broadcast traffic is often used when a host needs to discover the address of another host or when it needs to autoconfigure its own address.
- Broadcasts are also used by routers to communicate updates to one another.
- Nodes that share the same broadcast address are said to be within the same broadcast domain.
- Broadcast traffic introduces efficiencies in some circumstances but inefficiencies in others.
- If the broadcast domain is very large, the amount of broadcast traffic will be correspondingly great and consume a disproportionate amount of bandwidth. This becomes an important factor in designing a network that works efficiently.

Network designers can take advantage of the virtual LAN (VLAN) feature of modern Ethernet switches.

- A VLAN is a means of creating separate layer 2 broadcast domains on the same switch or configuring separate broadcast domains across a fabric of distributed switches.
- VLANs are a means of overcoming the physical topology to match the layer 2 logical topology to the layer 3 logical topology.



Ethernet Frames

Field	Bytes	Description
Preamble	7	56 alternating 1s and 0's used for synchronization
SFD	1	Start frame delimiter - designates the end of the preamble
Destination MAC Address	6	Ethernet MAC address of the destination device
Source MAC Address	6	Ethernet MAC address of the source device
Ether Type	2	Describes the data contained in the payload
Payload	46-1500	Layer 3 data and higher
CRC	4	Frame check sequence - CRC checksum of the frame

Pre-amble	Destination MAC	Source MAC	Length / Type	Payload	CRC

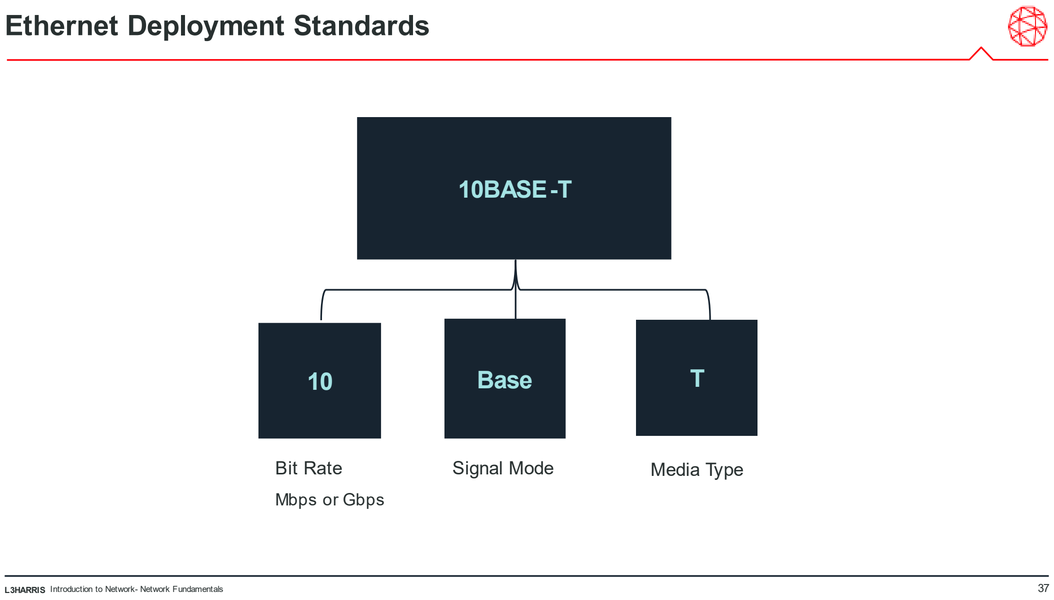
Preamble: The preamble and Start Frame Delimiter (SFD) are used for clock synchronization and as part of the CSMA/CD protocol to identify collisions early. The preamble consists of 8 bytes of alternating 1s and 0s with the SFD being two consecutive 1s at the end. This is not technically considered to be part of the frame.

Addressing: The destination and source address fields contain the MAC addresses of the receiving and sending nodes. A Media Access Control (MAC) address is a unique identifier for each Ethernet network adapter interface. A MAC address is also referred to as a local or hardware/physical address. A MAC address is 48 bits long (6 bytes).

Frame length and maximum transmission unit (MTU): The official 802.3 standard defines a 2-byte field to specify the size of the data field or payload. The payload can normally be between 46 and 1500 bytes. The upper limit of the payload is also referred to as the maximum transmission unit (MTU). However, most Ethernet products follow the original DIX specification, referred to as Type II frames, and use the field to indicate the type of network layer protocol contained in the frame—IPv4 or IPv6, for instance. These Ethertypes are values of 1536 or greater; anything less than that is interpreted as the data length. For example, IPv4 is coded as the hex value 0x0800, or 2048 in decimal, while IPv6 is 0x86DD.

To comply with CSMA/CD, the minimum length of an Ethernet frame is 64 bytes, so the payload must be at least 46 bytes. If this is not the case, it is automatically padded with redundant data. The maximum size of an Ethernet frame is normally 1518 bytes, excluding the preamble. Some Gigabit and 10GbE Ethernet products support jumbo frames with much larger MTUs. Such products are not standardized, however, making interoperability between different vendors problematic.

Error checking: The error checking field contains a 32-bit (4-byte) checksum called a Cyclic Redundancy Check (CRC) or Frame Check Sequence (FCS). The CRC is calculated based on the contents of the frame; the receiving node performs the same calculation and, if it matches, accepts the frame. There is no mechanism for retransmission if damage is detected nor is the CRC completely accurate at detecting damage; these are functions of error checking in protocols operating at higher layers.



Ethernet Deployment Standards

10BASE -T

10

Bit Rate

Mbps or Gbps

Base

Signal Mode

T

Media Type

Ethernet deployment standards provide a network designer the assurance that infrastructure will meet the bandwidth requirements of applications.

The standards specify the bit rate that should be achieved over different types of media up to the supported distance limitations.

These Ethernet media specifications are named using a three-part convention, which is often referred to as xBASE-y. This describes:

• The bit rate in megabits per second (Mbps) or gigabits per second (Gbps).

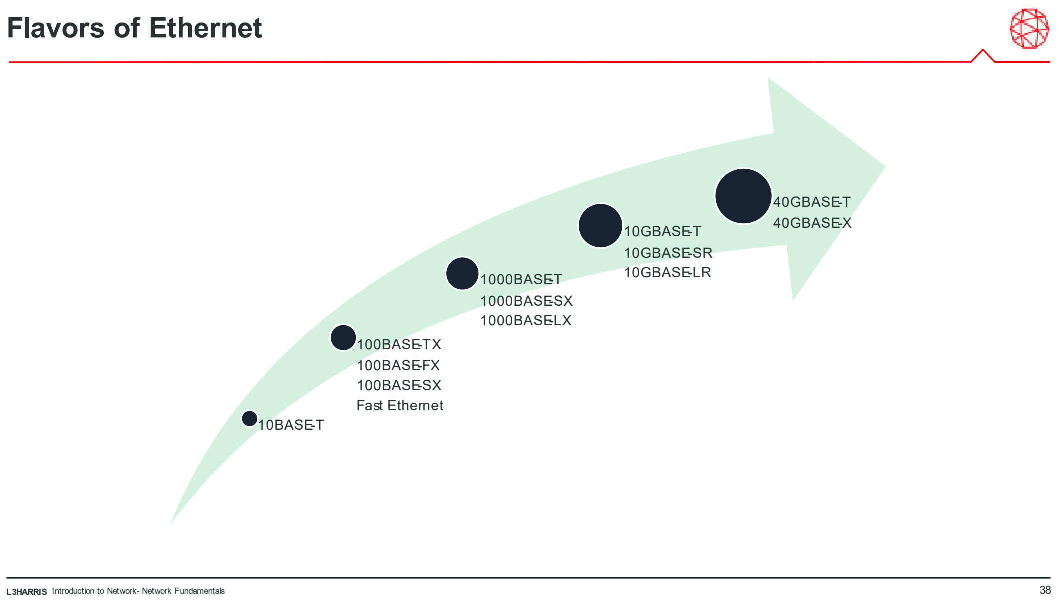
• The signal mode (baseband or broadband). All types of Ethernet use baseband transmissions, so you will only see specifications of the form xBASE-y.

• A designator for the media type.

For example, 10BASE-T denotes an early implementation that works at 10 Mbps, uses a baseband signal, and uses twisted pair copper cabling. Ethernet can use Unshielded Twisted Pair (UTP) rated to a particular Cat standard or fiber optic cabling.

BASE (Baseband)

- Single frequency using the entire medium.



Flavors of Ethernet

L3HARRIS Introduction to Network- Network Fundamentals 38

Fast Ethernet: uses the same CSMA/CD protocols as the original Ethernet specifications but with higher frequency signaling and improved encoding methods, raising the bit rate from 10 Mbps to 100 Mbps.

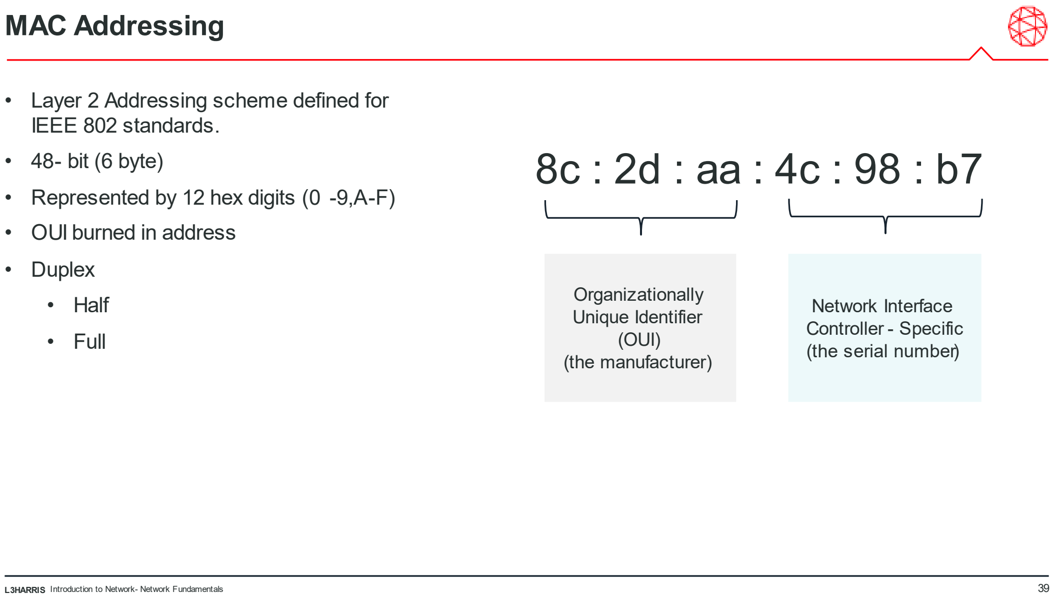
- The 100BASE-TX standard refers to Fast Ethernet working over Cat 5 (or better) Unshielded Twisted Pair (UTP) copper cable with a maximum supported link length of 100 meters.
- Fast Ethernet also introduced an autonegotiation protocol to allow devices to choose the highest supported connection parameters.

Gigabit Ethernet: Gigabit Ethernet builds on the standards defined for Ethernet and Fast Ethernet.

- The bit rate is 10 times faster than Fast Ethernet. The Gigabit Ethernet standard over fiber is documented in IEEE 802.3z.
- There are variants for long wavelength optics (LX), required for long distance transmission, and short wavelength optics (SX).
- The various fiber standards are collectively known as 1000BASE-X. The IEEE also approved 1000BASE-T, a standard utilizing Cat 5e (or better) copper wiring. This is defined in IEEE 802.3ab.

10 Gigabit Ethernet (10GbE) multiplies the nominal speed of Gigabit Ethernet by a factor of 10. 10GbE is not deployed in many access networks, however, as the cost of 10GbE network adapters and switches is high. The major applications of 10GbE Ethernet are:

- Increasing bandwidth for server interconnections and network backbones, especially in data centers and for storage area networks (SAN).
- Replacing existing switched public data networks based on proprietary technologies with simpler Ethernet switches (Metro Ethernet).



MAC Addressing

- Layer 2 Addressing scheme defined for IEEE 802 standards.
- 48- bit (6 byte)
- Represented by 12 hex digits (0 -9,A-F)
- OUI burned in address
- Duplex
  - Half
  - Full

8c : 2d : aa : 4c : 98 : b7

Organizationally Unique Identifier (OUI) (the manufacturer)

Network Interface Controller - Specific (the serial number)

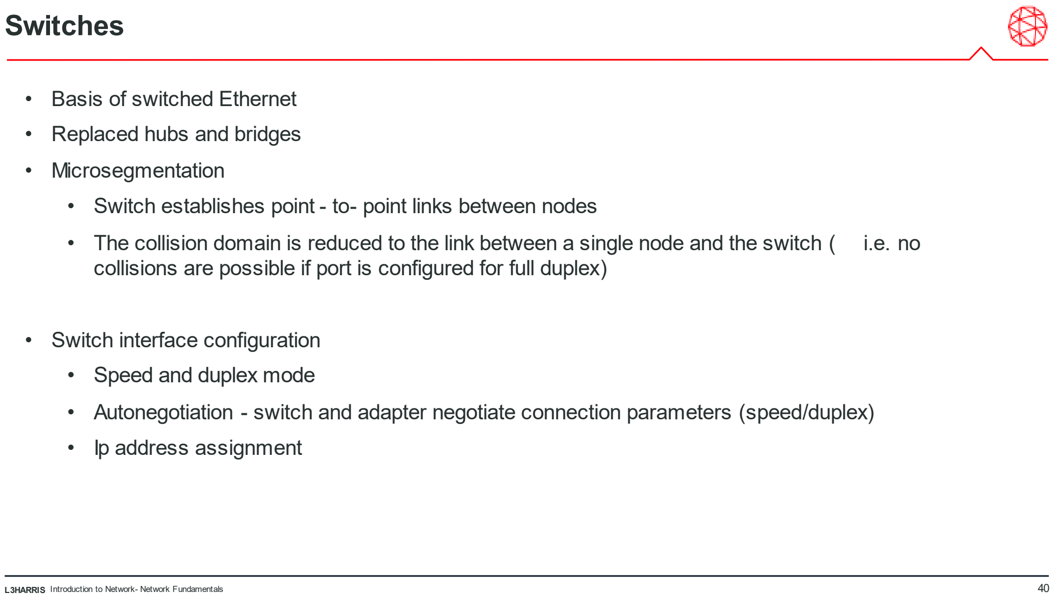
NETWORK INTERFACE CARDS (NICs) The transceiver component responsible for physically connecting the node to the transmission medium is implemented in a network adapter, network adapter card, or network interface card/controller (NIC). At the Data Link layer, the NIC is also responsible for organizing data into frames and providing each interface with a hardware address. A multiport NIC may have more than one interface. Each Ethernet network interface port has a unique hardware address known as the Media Access Control (MAC) address. This may also be referred to as the Ethernet address (EA) or, in IEEE terminology, as the extended unique identifier (EUI).

Ethernet **Media Access Control (MAC) address:** The physical address of a network adapter which is unique to every device and consists of 48 binary digits (6 bytes) which is typically displayed in hexadecimal format.

- Example: 8c : 2d : aa : 4c : 98 : b7

Organizationally Unique Identifier (OUI): The IEEE gives each card manufacturer a range of numbers, and the manufacturer hard-codes every interface produced with a unique number from their range. This is called the burned-in address. The first six hex digits (3 bytes or octets), also known as the Organizationally Unique Identifier (OUI), identify the manufacturer of the adapter.

Network Interface Controller- Specific: The last six digits are a serial number. An organization can decide to use locally administered addresses in place of the manufacturers' universal coding systems. This can be used to make MACs meaningful in terms of location on the network, but it adds a significant amount of administrative overhead. A locally administered address is defined by changing the U/L bit from 0 to 1. The rest of the address is configured using the card driver or network management software. It becomes the network administrator's responsibility to ensure that all interfaces are configured with a unique MAC.



Switches

- Basis of switched Ethernet
- Replaced hubs and bridges
- Microsegmentation
  - Switch establishes point - to- point links between nodes
  - The collision domain is reduced to the link between a single node and the switch (i.e. no collisions are possible if port is configured for full duplex)
- Switch interface configuration
  - Speed and duplex mode
  - Autonegotiation - switch and adapter negotiate connection parameters (speed/duplex)
  - Ip address assignment

Ethernet technology is designed to solve the problem of packet collision in a shared network by having network-connected devices follow a set of rules that allow devices to talk to each another without talking over each other. These network-connected devices are physically connected with a cable to an Ethernet switch that then manages the flow of data between devices, applications, data, cloud services and the internet.

Switches have now almost completely replaced legacy devices such as hubs and bridges as such, Gigabit Ethernet and Ethernet 10GbE cannot be installed without using switches.

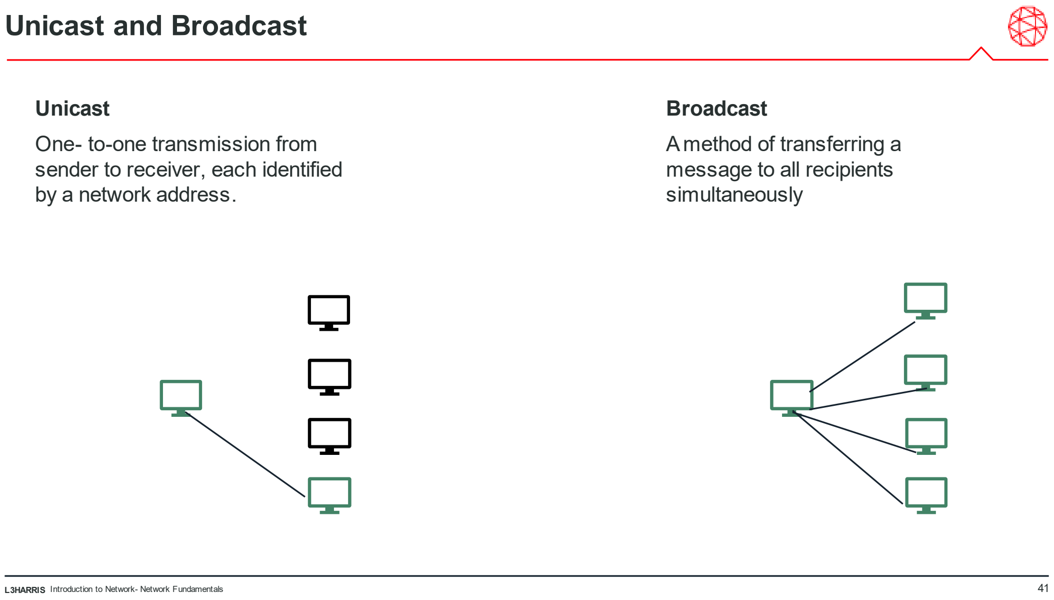
An Ethernet switch performs the same sort of function as a bridge, but in a more granular way and for many more ports than are supported by bridges. Each switch port is a separate collision domain. In effect, the switch establishes a point-to-point link between any two network nodes. This is referred to as microsegmentation.

- The role of a switch is to forward traffic based on the destination MAC address inside of an ethernet frame. This means the switch needs to keep an ongoing and active list of all the devices it happens to know about based on the MAC address of those devices. The switch builds this list by looking at inbound traffic and examining the source MAC address and tying that source MAC address to a specific physical interface.

Configuration of a managed switch can be performed either over a web interface or at some sort of command line.

Ethernet switches can be distinguished using the following general categories:

- Unmanaged versus managed
- Stackable
- Modular versus fixed
- Desktop versus rack-mounted



Unicast and Broadcast

Unicast

One- to-one transmission from sender to receiver, each identified by a network address.

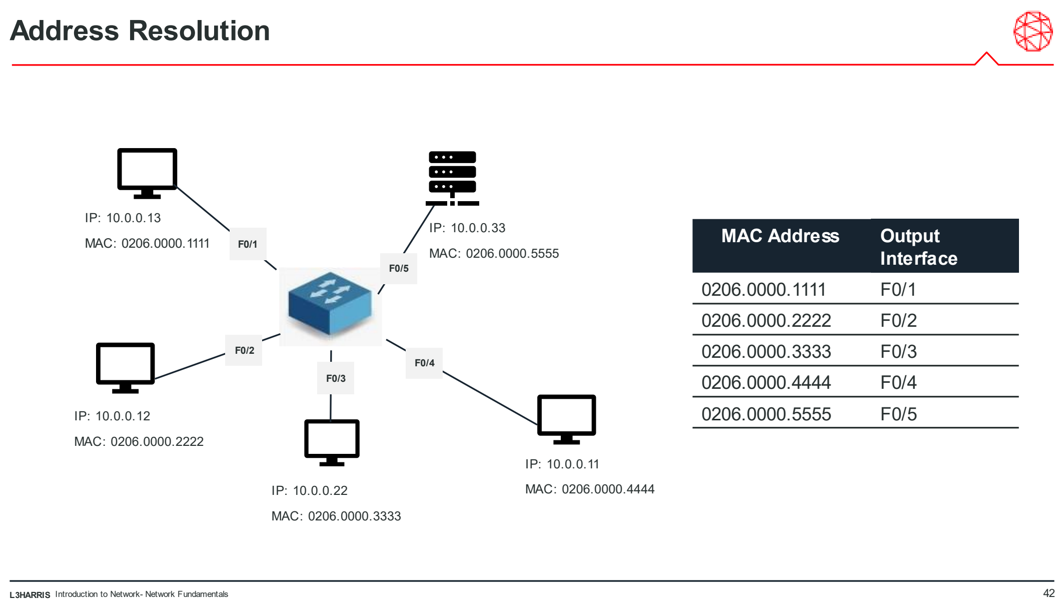
Broadcast

A method of transferring a message to all recipients simultaneously

Unicast delivers a message to a single specific node using a *one-to-one* association between a sender and destination: each destination address uniquely identifies a single receiver endpoint.

Broadcast delivers a message to all nodes in the network using a *one-to-all* association; a single datagram (or packet) from one sender is routed to all of the possibly multiple endpoints associated with the broadcast address. The network automatically replicates datagrams as needed to reach all the recipients within the scope of the broadcast, which is generally an entire network subnet.

Note: This is the case for unmanaged switches. With managed switches, this behavior can be changed by configuring virtual LAN’s (VLAN).



Address Resolution

MAC Address	Output Interface
0206.0000.1111	F0/1
0206.0000.2222	F0/2
0206.0000.3333	F0/3
0206.0000.4444	F0/4
0206.0000.5555	F0/5

When two hosts communicate using TCP/IP, an Internet Protocol (IP) address is used at the Network layer to identify each host. However, transmission of data must take place at the Physical and Data Link level using the local or hardware/MAC address of the interface. The TCP/IP suite includes the Address Resolution Protocol (ARP) to perform the task of resolving an IP address to a hardware address on an IPv4 network.

When both sending and receiving hosts are on the same local network (connected to the same hub, for instance), local address resolution takes place as follows:

- When the destination IP address has been determined to be a local address, the source host checks its ARP table cache for the required hardware address (MAC address) of the destination host.
- If the MAC address is not present in cache, ARP builds a request and broadcasts (flooding) it onto the network.
- The broadcast is processed by all the hosts on the local segment, but unless the request contains its own IP address, most hosts ignore it.
- If the target host recognizes its own address, it updates its cache with the MAC address of the source host. It then replies to the source host.
- The source host receives the reply, updates its cache table, and communication is established.

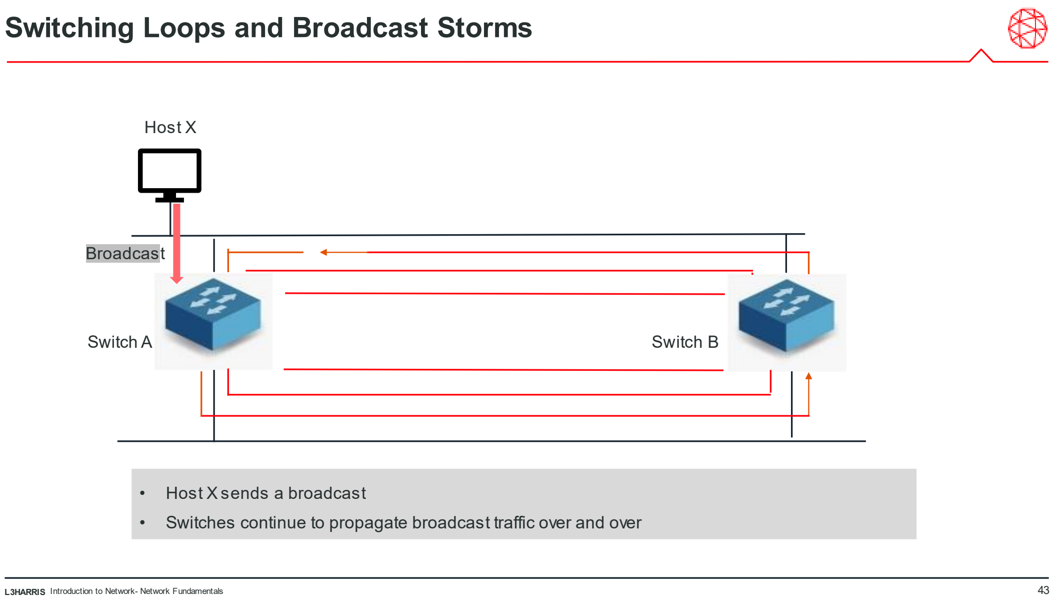
If the host is on a remote network, then the local host must use a router (its default gateway) to forward the packet. Therefore, it must determine the MAC address of the gateway using ARP.

- When the destination IP address has been determined to be a remote address, the sending host determines the IP address of its default gateway (router). The sending host then examines its ARP table cache for the necessary IP address/MAC address mapping of the gateway.

- If the mapping for the gateway address is not found in the cache, it broadcasts an ARP request for the default gateway's IP address (not the IP address of the remote destination host).
- Hopefully, the router will respond to the request by returning its hardware address. The sending host then forwards the packet to the default gateway to deliver to the remote network and the destination host. At the router, IP determines whether the destination is local or remote. If local, it uses ARP for the address resolution. If remote, it checks its routing table for an appropriate gateway to the remote network.

ARP Cache and arp Utility: The arp utility can be used to perform functions related to the ARP table cache. You would use this to diagnose a suspected problem with local addressing and packet delivery.

- arp -a (or arp -g) shows the ARP cache contents. You can use this with IPAddress to view the ARP cache for the specified interface only. The ARP cache will not necessarily contain the MAC addresses of every host on the local segment. There will be no cache entry if there has not been a recent exchange of frames.
- arp -s IPAddress MACAddress adds an entry to the ARP cache. Under Windows, MACAddress needs to be entered with hyphens between each hex byte.
- arp -d * deletes all entries in the ARP cache; it can also be used with IPAddress to delete a single entry.



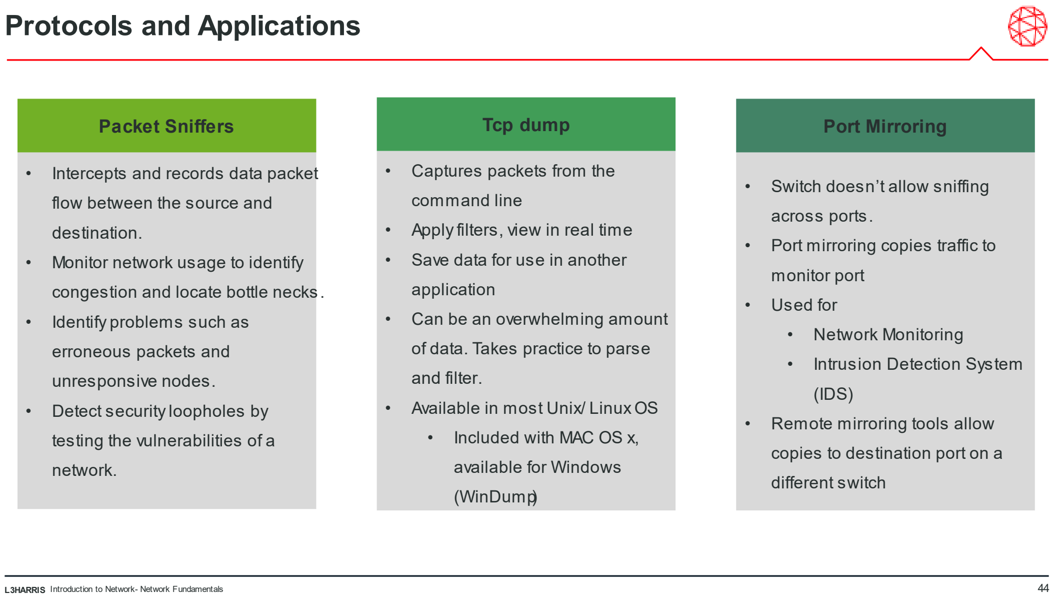
Switching Loops and Broadcast Storms

- Host X sends a broadcast
- Switches continue to propagate broadcast traffic over and over

L3HARRIS Introduction to Network- Network Fundamentals 43

In a network with multiple bridges, implemented these days as switches, there may be more than one path for a frame to take to its intended destination. Multiple paths are part of good network design as they increase resilience; if one link fails, then the network can remain operational by forwarding frames over a different path.

- As a layer 2 protocol, Ethernet has no concept of "time to live," so layer 2 broadcast traffic could continue to loop through a network with multiple paths indefinitely.
- Switching loops cause flooded frames to circulate the network perpetually, causing what is often called a broadcast storm. A broadcast storm may quickly consume all link bandwidth and crash network appliances.
- Because switches flood broadcasts and unicast frames with an unknown destination MAC address out all ports, ARP broadcasts in a looped network will cause a Layer 2 broadcast storm.
- The ARP broadcast will go down one link to the next switch, which will send the broadcast back up the redundant link. This feedback loop will continue indefinitely until there is manual intervention by an administrator. It will cause network utilization to go to near maximum capacity, and the CPU utilization of the switches to jump to 80 percent or more.
- This makes the switched segment effectively unusable until the broadcast storm stops. Layer 2 loops are prevented using the Spanning Tree Protocol (STP), defined in the IEEE 802.1D MAC Bridges standard.



Protocols and Applications

Packet Sniffers

- Intercepts and records data packet flow between the source and destination.
- Monitor network usage to identify congestion and locate bottle necks.
- Identify problems such as erroneous packets and unresponsive nodes.
- Detect security loopholes by testing the vulnerabilities of a network.

Tcp dump

- Captures packets from the command line
- Apply filters, view in real time
- Save data for use in another application
- Can be an overwhelming amount of data. Takes practice to parse and filter.
- Available in most Unix/ Linux OS
  - Included with MAC OS x, available for Windows (WinDump)

Port Mirroring

- Switch doesn't allow sniffing across ports.
- Port mirroring copies traffic to monitor port
- Used for
  - Network Monitoring
  - Intrusion Detection System (IDS)
- Remote mirroring tools allow copies to destination port on a different switch

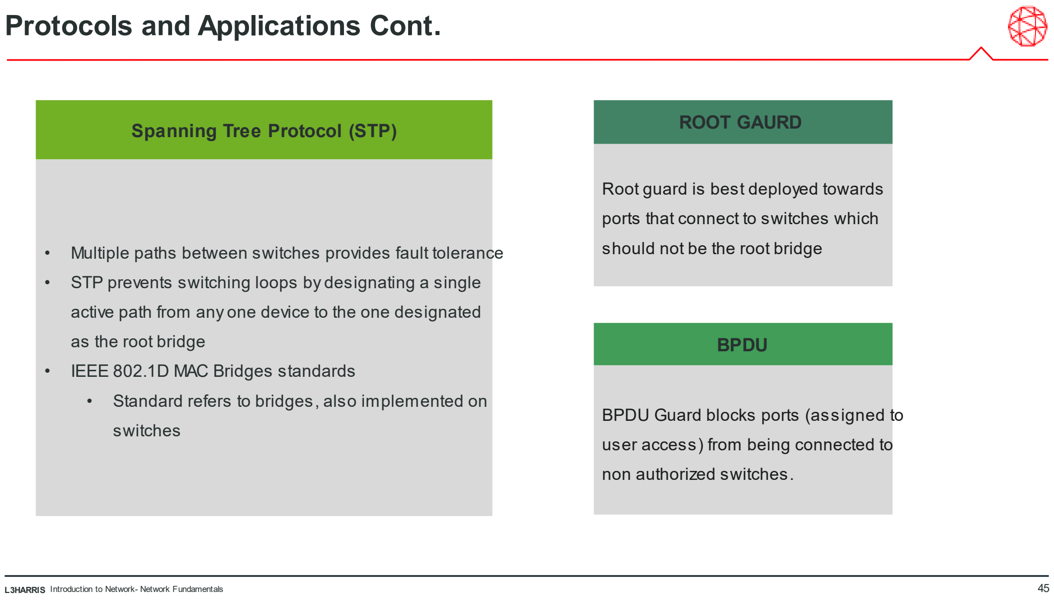
L3HARRIS Introduction to Network- Network Fundamentals 44

Packet Sniffers One of the most important tools used for network support is a protocol analyzer. This is the tool that allows inspection of traffic received by a host or passing over a network link. A protocol analyzer depends on a packet sniffer. A sniffer captures frames moving over the network medium. This might be a cabled or wireless network.

TCP dump tcpdump is a command-line packet capture utility for Linux, though a port of the program (windump) is available for Windows (winpcap.org/windump). The basic syntax of the command is: tcpdump -i eth0 Where eth0 is the interface to listen on. The utility will then display captured packets until halted manually (by pressing Ctrl+C). The operation of the basic command can be modified by switches. For example, the -w and -r switches write output to a file and read the contents of a capture file respectively. The -v, -vv, and -vvv can be used to increase the amount of detail shown about each frame while the -e switch shows the Ethernet header.

PORT MIRRORING Port mirroring copies all packets sent to one or more source ports to a mirror (or destination) port. On a Cisco switch, this is referred to as a switched port analyzer (SPAN).

- The mirror port would be used by management or monitoring software, such as a packet sniffer, network analyzer, or intrusion detection system (IDS) sensor. Either ingress or egress traffic, or both, can be captured.
- Optionally, to avoid overloading the monitoring system, packets may be filtered based on criteria such as protocol ID or TCP/UDP port number. This describes local port mirroring where the source and destination ports are on the same switch. On advanced switches, it is possible to perform remote port mirroring by making the destination port a port on another switch.



Protocols and Applications Cont.

Spanning Tree Protocol (STP)

- Multiple paths between switches provides fault tolerance
- STP prevents switching loops by designating a single active path from any one device to the one designated as the root bridge
- IEEE 802.1D MAC Bridges standards
    - Standard refers to bridges, also implemented on switches

ROOT GAURD

Root guard is best deployed towards ports that connect to switches which should not be the root bridge

BPDU

BPDU Guard blocks ports (assigned to user access) from being connected to non authorized switches.

L3HARRIS Introduction to Network- Network Fundamentals 45

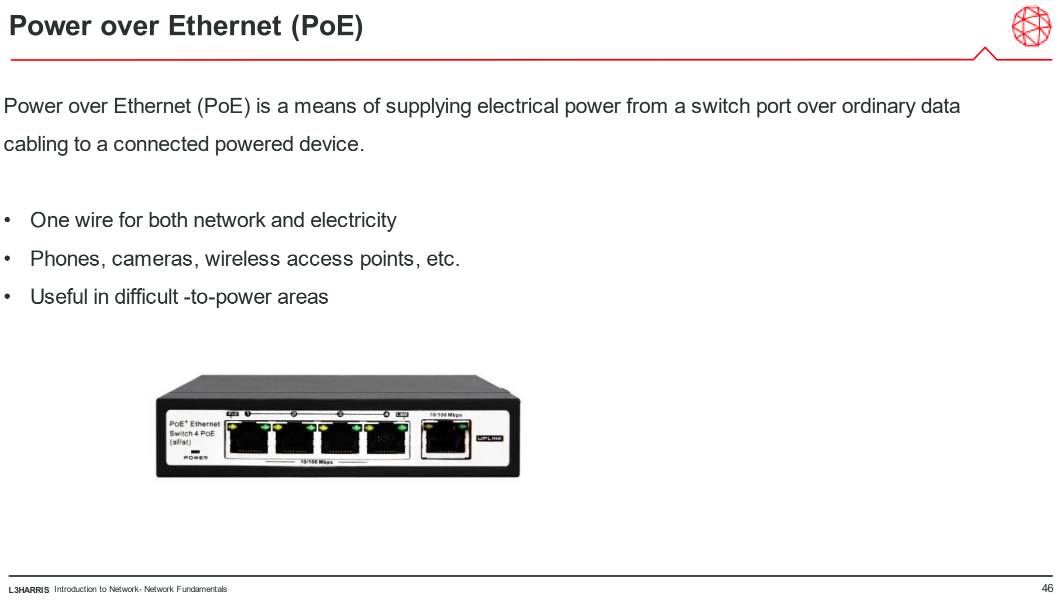
SPANNING TREE PROTOCOL (STP) Spanning tree is a means for the bridges to organize themselves into a hierarchy. The bridge at the top of the hierarchy is the root bridge. The switch with the lowest bridge ID, comprising a priority value and the MAC address, will be selected as the root. An administrator can (and should) set the priority value to make the choice of one bridge over another more likely.

- The root bridge will usually be part of a high-bandwidth backbone or core switch group; performance will suffer if a switch on a low-bandwidth segment becomes root.
- Each bridge then determines the shortest path to the root bridge by exchanging information with other bridges. This STP information is packaged as bridge protocol data unit (BPDU) multicast frames.
- A port that forwards "up" to the root bridge, possibly via intermediate bridges, is identified as a root port.
- Ports that can forward traffic "down" through the network with the least cost are identified as designated ports.
- A port that would create a loop is identified as a blocking or non-designated port.
- Subsequently, bridges exchange Topology Change Notifications if devices are added or removed, enabling them to change the status of forwarding/blocked ports appropriately.

Some commands that can be used to filter STP traffic include:

BPDU Guard: This causes a port configured with PortFast that receives a BPDU to become disabled. BPDUs are not expected on access ports so this protects against misconfiguration or a possible malicious attack.

Root Guard: This setting means that a switch will not accept attempts from switches connected to the guarded port to become the root.



Power over Ethernet (PoE)

Power over Ethernet (PoE) is a means of supplying electrical power from a switch port over ordinary data cabling to a connected powered device.

- One wire for both network and electricity
- Phones, cameras, wireless access points, etc.
- Useful in difficult -to-power areas

L3HARRIS Introduction to Network- Network Fundamentals 46

Power over Ethernet (PoE) is a means of supplying electrical power from a switch port over ordinary data cabling to a connected powered device, such as a VoIP handset or wireless access point.

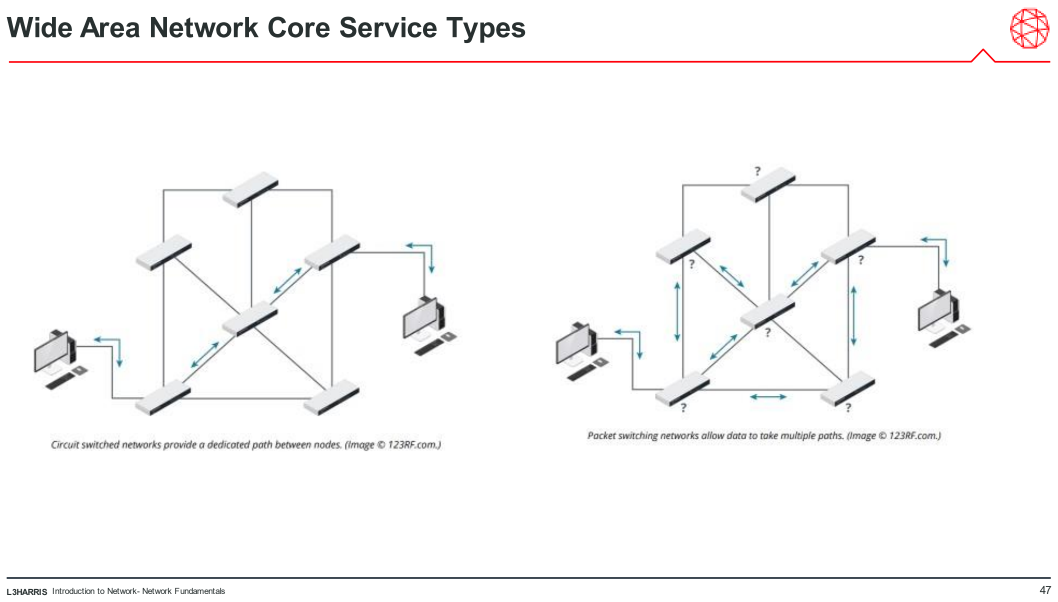
PoE is defined in two IEEE standards (now both rolled into 802.3-2018):

- **802.3af**—Powered devices can draw up to about 13 W over the link. Power is supplied as 350mA@48V and limited to 15.4 W, but the voltage dropped over the maximum 100 feet of cable results in usable power of around 13 W.
- **802.3at** (PoE+)—Powered devices can draw up to about 25 W, with a maximum current of 600 mA. Various proprietary schemes were used prior to the ratification of 802.3at.

PoE switches are referred to as endspan (or endpoint) power sourcing equipment (PSE). If an existing switch does not support PoE, a device called a power injector (or midspan) can be used. Power can either be supplied over pairs 1/2 and 3/6 (referred to as Mode A or phantom power, as these are the ones also used for data in 10/100BASE) or over 4/5 and 7/8 (Mode B). Gigabit Ethernet only uses the Mode A method.

When a device is connected to a port on a PoE switch, the switch goes through a detection phase to determine whether the device is PoE-enabled. If not, it does not supply power over the port and, therefore, does not damage non-PoE devices. If so, it determines the device's power consumption and sets the supply voltage level appropriately.

Powering these devices through a switch is more efficient than using a wall-socket AC adapter for each appliance. It also allows network management software to control the devices and apply schemes, such as making unused devices go into sleep states and power capping.



Wide Area Network Core Service Types

Circuit switched networks provide a dedicated path between nodes. (Image © 123RF.com.)

Packet switching networks allow data to take multiple paths. (Image © 123RF.com.)

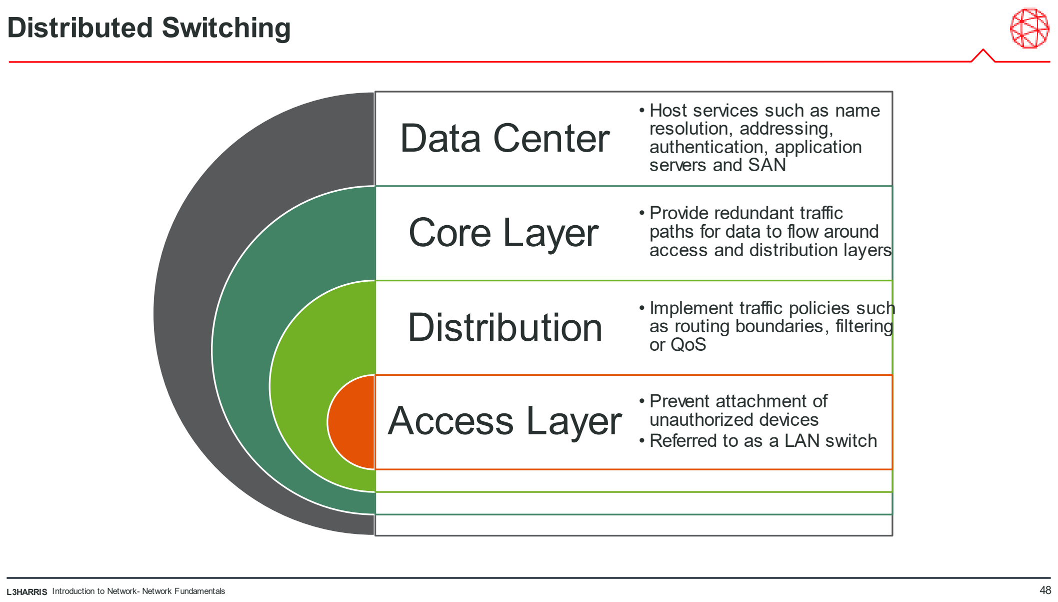
WANs have historically made more use of **circuit switched networks.** Circuit switched networks provide guaranteed predicable levels of bandwidth via a dedicated connection. On the downside, circuit switched networks make inefficient use of the media as, by definition, a dedicated channel cannot be shared even when it is not being used. The technology is also impractical for some applications because they time-out before a circuit is established

Packet switching technology was developed on the basis that subscribers share the network infrastructure and pay only for the bandwidth they consume. It is a cost-effective alternative to dedicated lines and provides more efficient use of the network infrastructure than circuit switched technology.

- **Frame Relay:** evolved from the earlier packet switching protocol X.25 in the 1990s. It provides data packet forwarding for services running over T-carrier lines, ISDN, or even dial-up. Frame Relay is now considered a legacy protocol in many parts of the world and is not often offered as a service by telecom providers.

- **Asynchronous Transfer Mode (ATM):** is a transport mechanism for all types of data, including voice and video. ATM uses a cell switching technology. ATM can make use of a variety of physical media, but in most implementations, it runs over either T1/T3 links or SDH/SONET. For end customers in many parts of the world, ATM is not widely offered as a service by telecom providers anymore. It does remain supported for the organizations that have installed it already.

- **Multiprotocol Label Switching (MPLS)** was developed by Cisco from ATM as a means of providing traffic engineering, Class of Service (CoS), and QoS within a packet switched network. In effect, MPLS achieves a marriage of layer 3-based routing with layer 2-based switching. Where Frame Relay and ATM provide connection-oriented transfer by establishing a virtual circuit/channel, MPLS establishes connections via Label Switched Paths (LSPs) enabled by a mesh network of Label Switched Routers (LSRs).



Distributed Switching

Data Center
- Host services such as name resolution, addressing, authentication, application servers and SAN

Core Layer
- Provide redundant traffic paths for data to flow around access and distribution layers

Distribution
- Implement traffic policies such as routing boundaries, filtering or QoS

Access Layer
- Prevent attachment of unauthorized devices
- Referred to as a LAN switch

To accommodate the design goals of adaptability and scalability, a hierarchical model is often adopted. A hierarchical model breaks down a large and complex network design into smaller sections based on the functions performed. Each function can be assessed by network designers to identify the most efficient hardware and software to implement.

Distributed Switching: This model is especially useful for medium to large networks. Systems can be grouped by location, with the smaller groups each attached to an access switch which form the bottom level of the hierarchy.

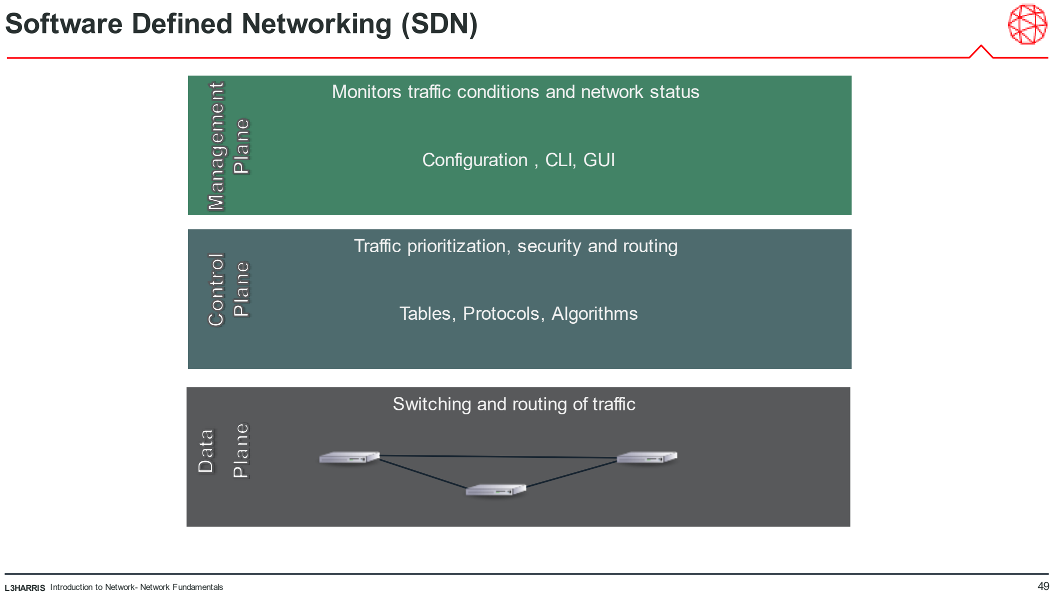
- Access switches are not directly connected to one another. Each access switch forwards traffic to switches in a distribution layer.
- Switches at the distribution layer are highly interconnected, with redundant paths for failover.
- Policies can be implemented at the distribution level to prioritize traffic for optimal network performance.
- This model also assists with isolating issues that may occur within the network.

Access Layer: allows end-user devices, such as computers, printers, and smartphones to connect to the network.

Distribution Layer: provides fault-tolerant interconnections between different access blocks and either the core or other distribution blocks.

Core Layer: provides a highly available network backbone. Devices such as client and server computers should not be attached directly to the core.

Data Center: a network area that hosts network services.



Software Defined Networking (SDN)

Management Plane

Monitors traffic conditions and network status

Configuration , CLI, GUI

Control Plane

Traffic prioritization, security and routing

Tables, Protocols, Algorithms

Data Plane

Switching and routing of traffic

SOFTWARE DEFINED NETWORKING (SDN) As networks become more complex—perhaps involving thousands of physical and virtual computers and appliances—it becomes more difficult to implement network policies, such as ensuring security and managing traffic flow. With so many devices to configure, it is better to take a step back and consider an abstracted model about how the network functions.

In this model, network functions can be divided into three "planes":

- **Management plane:** monitors traffic conditions and network status.
- **Control plane:** makes decisions about how traffic should be prioritized and secured and where it should be switched.
- **Data plane:** handles the actual switching and routing of traffic and imposition of access control lists (ACLs) for security.

A software defined networking (SDN) application (or suite of applications) can be used to define policy decisions on the control plane. These decisions are then implemented on the data plane by a network controller application, which interfaces with the network devices using application programming interfaces (APIs). The interface between the SDN applications and the SDN controller is described as the "northbound" API, while that between the controller and appliances is the "southbound" API.

At the device level, SDN can use virtualized appliances or physical appliances. The appliances just need to support the southbound API of the network controller software. This architecture saves the network administrator the job and complexity of configuring each appliance with appropriate settings to enforce the desired policy. It also allows for fully automated deployment (or provisioning) of network links, appliances, and servers. This makes SDN an important part of the latest software deployment and disaster recovery technologies.