Protocol Basics: Definition, Types of Protocols

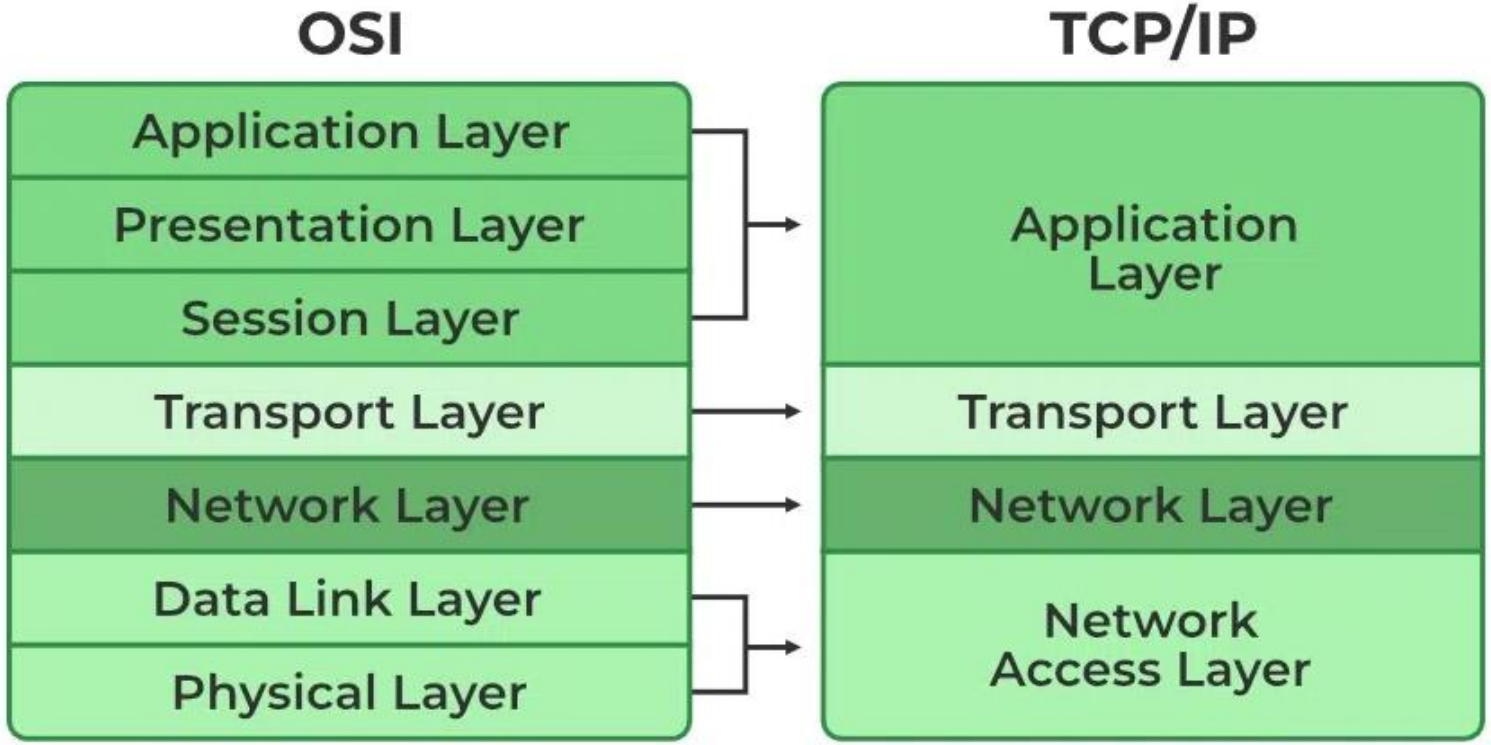
In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other.

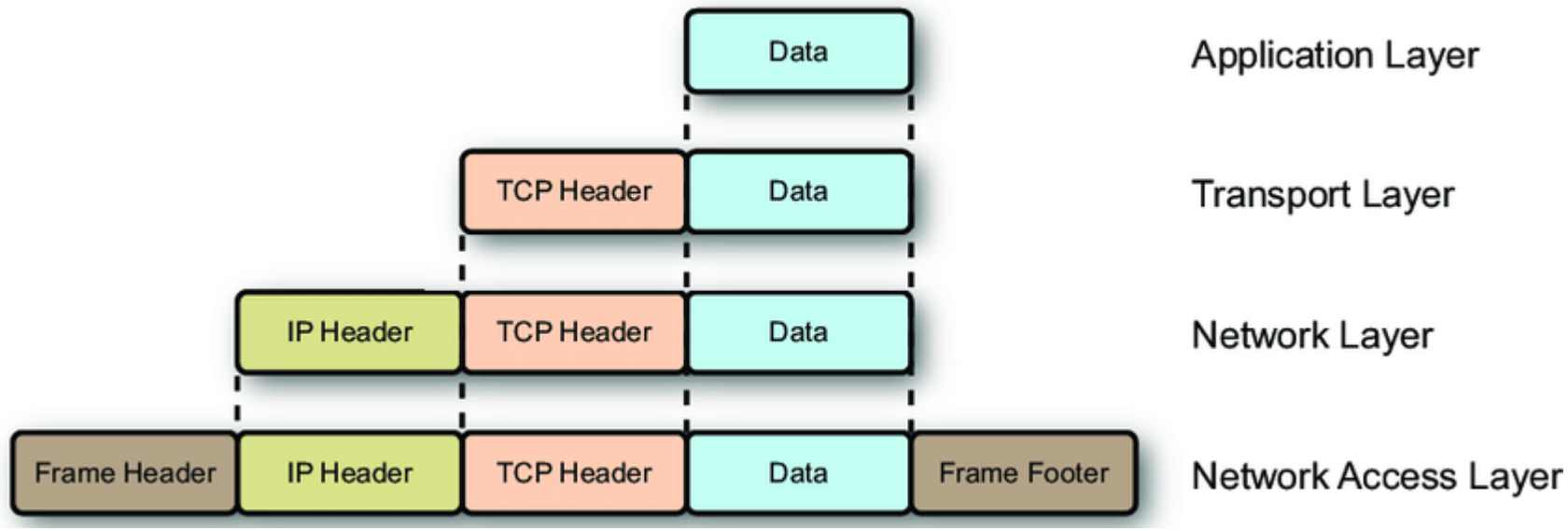
They play a critical role in making the internet work. Without them, there would be no way for servers or devices to communicate with each other. Every piece of online content—from text to images, video and audio—is delivered to the end user via network protocols.

Network communication protocols – A group of protocols used to establish rules and formatting (such as syntax, synchronization and semantics) for exchanging data across a network. Types of network communication protocols include TCP, UDP, IP, HTTP, IRC, BGP and ARP etc.

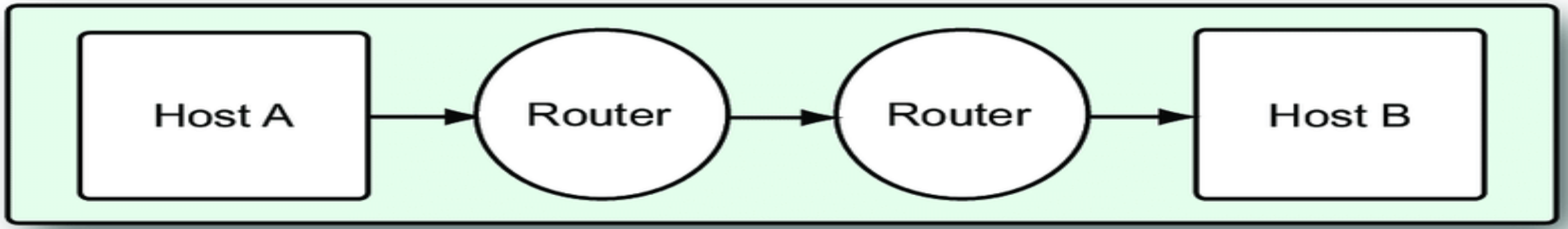
There are three main types of network protocols you need to be aware of:

- **Network management protocols** – These protocols set out policies designed to monitor, manage and maintain a network. Examples include SNMP, FTP, POP3 and Telnet.
- **Network communication protocols** – A group of protocols used to establish rules and formatting (such as syntax, synchronization and semantics) for exchanging data across a network. Types of network communication protocols include TCP, UDP, IP, HTTP, IRC, BGP and ARP.
- **Network security protocols** – Security protocols are protocols that use security measures such as cryptography and encryption to protect data. Examples include SFTP, SSL and HTTPS.

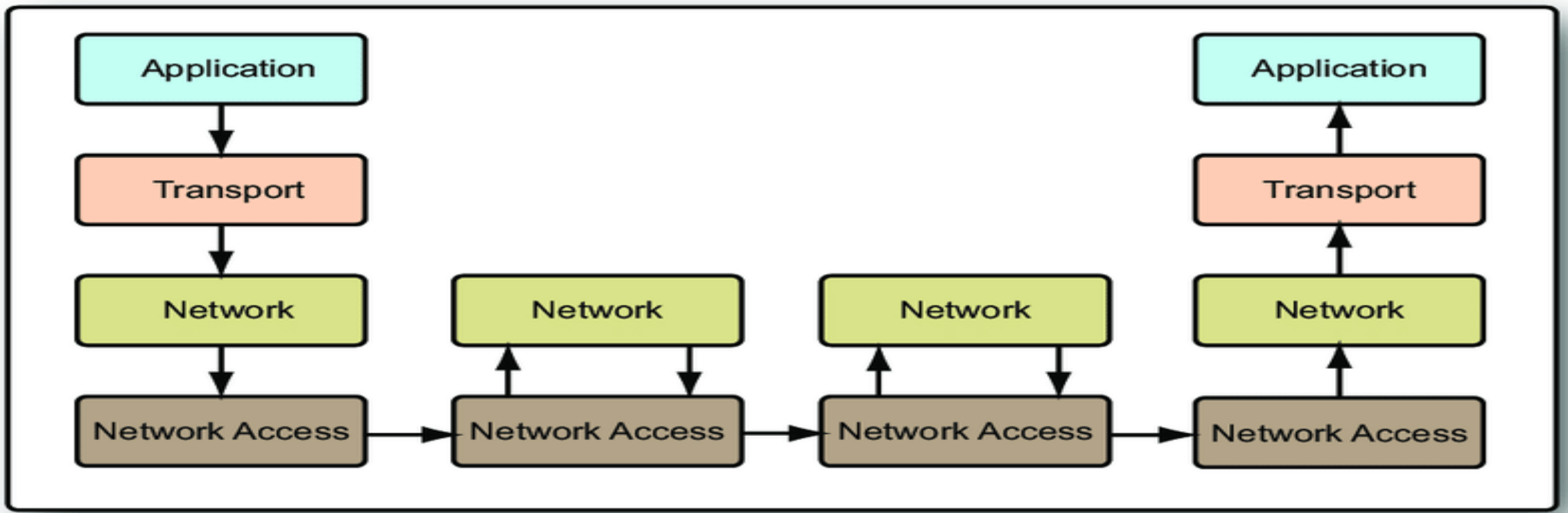

OSI
TCP/IP
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Network Layer
Network Access Layer


Data
TCP Header
Data
IP Header
TCP Header
Data
Frame Header
IP Header
TCP Header
Data
Frame Footer
Application Layer
Transport Layer
Network Layer
Network Access Layer

Network Connections View



TCP/IP Model



Feature	TCP (Transmission Control Protocol)	IP (Internet Protocol)
Purpose	Ensures reliable, ordered, and error-checked delivery of data between applications.	Provides addressing and routing of packets across networks.
Type	Connection-oriented	Connectionless
Function	Manages data transmission between devices, ensuring data integrity and order.	Routes packets of data from the source to the destination based on IP addresses.
Error Handling	Yes, includes error checking and recovery mechanisms.	No, IP itself does not handle errors; relies on upper-layer protocols like TCP.
Flow Control	Yes, includes flow control mechanisms.	No
Congestion Control	Yes, manages network congestion.	No
Data Segmentation	Breaks data into smaller packets and reassembles them at the destination.	Breaks data into packets but does not handle reassembly.
Header Size	Larger, 20-60 bytes	Smaller, typically 20 bytes
Reliability	Provides reliable data transfer	Does not guarantee delivery, reliability, or order.
Transmission Acknowledgment	Yes, acknowledges receipt of data packets.	No

Usage of Various Protocols & Port numbers: TCP/IP, NetBeui, VPN, SNMP, FTP/SMTP/POP/HTTP, SSL/TSL

A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

Ports are standardized across all network-connected devices, with each port assigned a number. Most ports are reserved for certain protocols — for example, all Hypertext Transfer Protocol (HTTP) messages go to port 80. While IP addresses enable messages to go to and from specific devices, port numbers allow targeting of specific services or applications within those devices.

OSI Model

	Protocol
Application Layer	HTTP, HTTPS, FTP, DNS, SNMP, Telnet
Presentation Layer	SSL, TLS
Session Layer	NetBIOS, PPTP
Transport Layer	TCP, UDP
Network Layer	IP, ARP, ICMP, IPSec
Datalink Layer	MAC, PPP, ATM
Physical Layer	RJ-45, Ethernet Cable, Optical Fiber

There are 65,535 possible port numbers, although not all are in common use. Some of the most commonly used ports, along with their associated networking protocol are:

- **Ports 20 and 21:** File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.
- **Port 22:** Secure Shell (SSH). SSH is one of many tunneling protocols that create secure network connections.
- **Port 25**: Simple Mail Transfer Protocol (SMTP). SMTP is used for email.
- **Port 53:** Domain Name System (DNS). DNS is an essential process for the modern Internet; it matches human-readable domain names to machine-readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses.
- **Port 80:** Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible.
- **Port 123:** Network Time Protocol (NTP). NTP allows computer clocks to sync with each other, a process that is essential for encryption..

- **Port 179:** Border Gateway Protocol (BGP). BGP is essential for establishing efficient routes between the large networks that make up the Internet (these large networks are called autonomous systems). Autonomous systems use BGP to broadcast which IP addresses they control.
- **Port 443:** HTTP Secure (HTTPS). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port.
- **Port 500:** Internet Security Association and Key Management Protocol (ISAKMP), which is part of the process of setting up secure IPsec connections.
- **Port 587:** Modern, secure SMTP that uses encryption.
- **Port 3389:** Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.

The Internet Assigned Numbers Authority (IANA) maintains the full list of port numbers and protocols assigned to them

Arcnet, Ethernet, MAN, SAN, NAS, Virtual LANs, ATM's:- Definition, Need, Significance, Application

- A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group.
- A LAN is a group of computers or other devices in the same place -- e.g., the same building or campus -- that share the same physical network. A LAN is usually associated with an Ethernet (Layer 2) broadcast domain, which is the set of network devices an Ethernet broadcast packet can reach.
- Computers on the LAN connect to the same network switch, either directly or through wireless access points (APs) connected to the same switch. Computers can also connect to one of a set of interconnected switches, such as a set of access switches that all connect up to a backbone switch. Once traffic crosses a router and engages Layer 3 (IP-related) functions, it is not considered to be on the same LAN, even if everything stays in the same building or floor. As a result, a location could have many interconnected LANs.
- A VLAN, like the LAN it sits atop, operates at Layer 2 of the network, the Ethernet level. VLANs partition a single switched network into a set of overlaid virtual networks that can meet different functional and security requirements. This partitioning avoids the need to have multiple, distinct physical networks for different use cases.

ARCNET and Ethernet

ARCNET (Attached Resource Computer NETwork) The first local area network (LAN) introduced in 1968 by Datapoint Corporation. Although ARCNET gave way to Ethernet for office networks, it is still used in industrial control applications.

ARCNET — An Embedded Real-Time Network. ARCNET, once quite popular in office automation, has reinvented itself into an embedded networking technology that is frequently found in applications such as industrial control, building automation, transportation, robotics and gaming.

ARCNET is a bus network and Ethernet is a star network. This means that with ARCNET, all devices are connected to a single cable, while with Ethernet, each device is connected to a central hub.

On the local area network, each device must have a unique address. ARCNET uses one-byte addresses which are typically selected when devices are installed. Ethernet uses six-byte addresses which are typically programmed into an EEPROM when a network interface card or device is manufactured.

Both ARCNET and Ethernet are data link technologies with varied medium access methods, frame sizes and link layer protocols. With Ethernet, the most popular transport layer protocol is TCP/IP, but ARCNET is more commonly found in embedded applications that do not use TCP/IP.

ARCNET established a communication link between multiple computers and enabled them to share information with each other. The network worked by dividing messages into small packets of data, which were then transmitted over the network to their intended destination.

Significance of Fast Ethernet

- Increased Data Transfer Rates.
- Enhanced Network Performance.
- Cost Effectiveness.
- Scalability.
- Flexibility.
- Support for Bandwidth intensive applications (Video Conferencing, Multimedia streaming, Large File Transfers).

Ethernet is used to connect different devices in a network with each other and even now this method is the best one for creating a Local Area Network that is LAN or Wide Area Network that is WAN. Ethernet is also used to connect Wi-Fi router or modem to the internet entry port or telephone line.

The purpose of a VLAN

- Network engineers use VLANs for multiple reasons, including the following:
- to improve performance
- to tighten security
- to ease administration

The devices that are in the same physical network are divided into logical groups by VLAN. VSAN separates the storage devices into different logical storage groups and can set its own policies. The devices that are connected in the same virtual group can communicate with each other.

Few examples of where VLANs can be used for:

- To separate network management traffic from end-user or server traffic.
- To isolate sensitive infrastructure, services, and hosts such as corporate users from guest users.
- To prioritize or implement Quality of Service (QoS) rules for specific services, such as VoIP Phones.

Types of VLAN

- Management VLAN.
- Data VLAN.
- Voice VLAN.
- Default VLAN.
- Native VLAN.

The value range for VLAN IDs is 1 to 4094.

There are four types of networks

- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN). Generally, it is several LANs interconnected by dedicated backbone connections.

Devices used for transmission of data through MAN are Modem and Wire/Cable. Examples of a MAN are part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

A WAN network will have a larger coverage area that can range up to 100,000 KM and in some cases, stretches globally or over international borders. A LAN network is limited to between 100-1000 meters coverage. A MAN network will stretch up to an area of 100 KM.

TCP/IP (Transmission Control Protocol/Internet Protocol), and MPLS (Multiprotocol Label Switching) are commonly used in MAN networks to ensure reliable and efficient data transmission.

A personal area network is a computer network for interconnecting electronic devices within an individual person's workspace. A PAN provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants. Bluetooth is a form of personal area network, typically the range is 10–15 m.

NSA stands for Non-Standalone. The basic meaning of the 5G NSA mode is clued in the name – A network that can't stand alone.

Network-attached storage (NAS) is a file-dedicated storage device that makes data continuously available for employees to collaborate effectively over a network. Any computer network has interconnected server machines and client machines that send requests to the servers.

A NAS system is a storage device connected to a network that allows storage and retrieval of data from a centralized location for authorized network users and heterogeneous clients. NAS systems are flexible and scale-out, meaning that as you need additional storage, you can add on to what you have.

Benefits of NAS: Lower cost; can significantly reduce wasted space over other storage technologies like SAN. Easy data backup and recovery, with granular security features. Centralization of data storage in a safe, reliable way for authorized network users and clients. Supports a large variety of applications.

Limitations of NAS: Network Dependency: The performance of a NAS is limited to what the network it is connected to can provide. Highly congested networks will lead to degraded performance. Power outages can affect access to files, and a large amount of network bandwidth is needed to store large files.

ATM

Asynchronous Transfer Mode (ATM) is a transfer mode for switching and transmission that efficiently and flexibly organizes information into cells; it is asynchronous in the sense that the recurrence of cells depends on the required or instantaneous bit rate.

ATM removes the distinction between LANs and WANs. ATM can be used to connect end stations or to interconnect LANs. However, ATM ultimately failed to become the dominant networking technology for reasons like: Complexity and Cost: Implementation Complexity: ATM is based on cell-switching and requires complex hardware and software to implement.

ATM is a core protocol used in the synchronous optical networking and synchronous digital hierarchy (SONET/SDH) backbone of the public switched telephone network and in the Integrated Services Digital Network (ISDN) but has largely been superseded in favor of next-generation networks based on IP technology.

Disadvantages

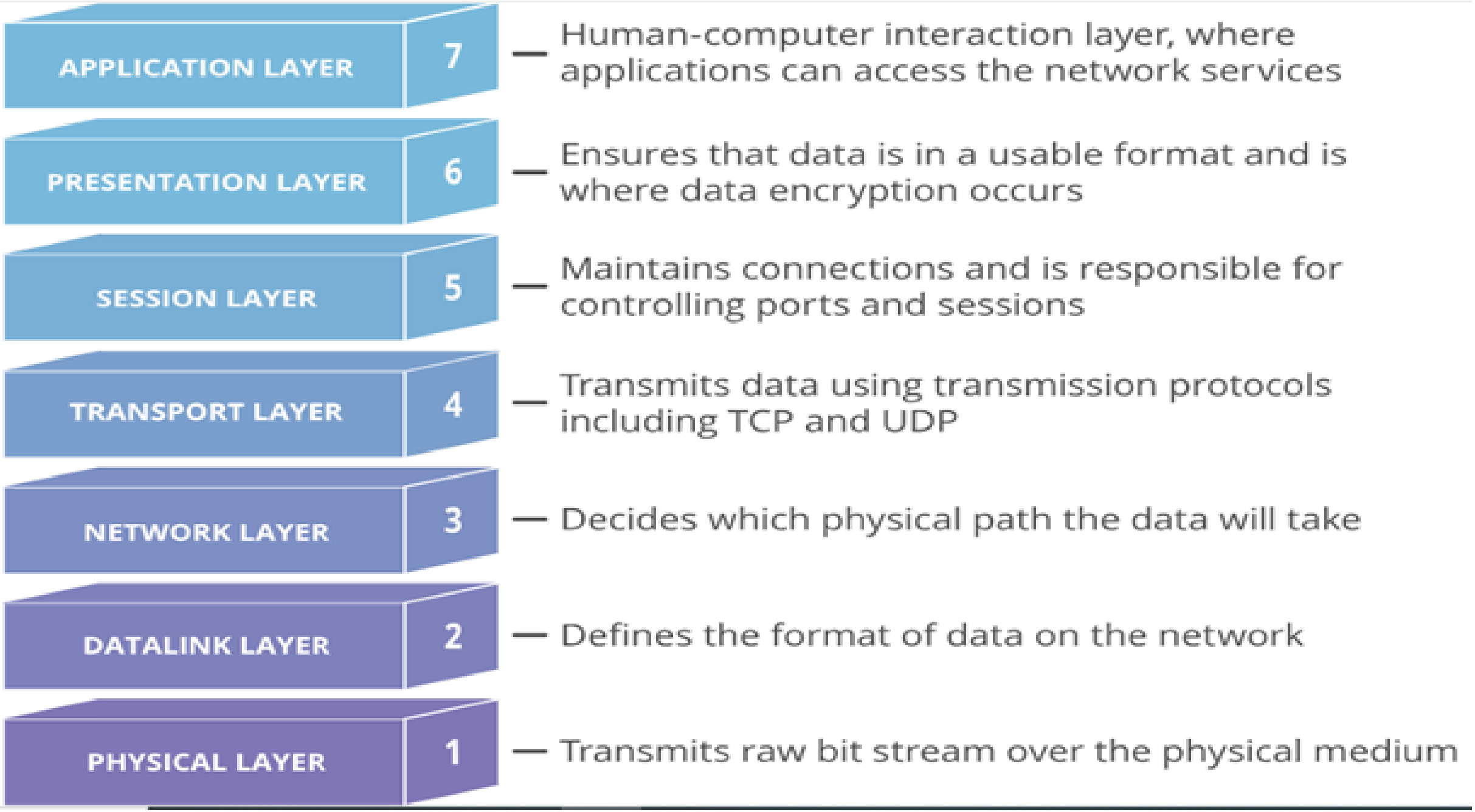
- There is an overhead of the cell header (5 bytes/cell)
- Achieving QoS has a complex mechanism.(Quality of service (QoS) is the use of mechanisms or technologies that work on a network to control traffic and ensure the performance of critical applications with limited network capacity. It enables organizations to adjust their overall network traffic by prioritizing specific high-performance applications.)
- There may be a condition of cell loss due to congestion.
- Compared to LAN hardware, ATM switches are very expensive.

ARCNET was originally classified as a local area network or LAN. The intent of ARCNET when it was originally introduced as an office automation LAN by Datapoint Corporation in the late 1970s. Datapoint envisioned a network with distributed computing power operating as one larger computer. This system was referred to as ARC (attached resource computer) and the network, that connected these resources, was called ARCNET.

ARCNET continues to find success in the industrial automation industry because its performance characteristics are well suited for control. ARCNET has proven itself to be very robust.

ARCNET also is fast, provides deterministic performance and can span long distances making it a suitable fieldbus technology. ARCNET is an ideal fieldbus. ARCNET's token-passing protocol provides this timeliness. ARCNET packet lengths are variable from 0 to 507 bytes with little overhead and coupled with ARCNET's high data rate, typically 2.5 Mbps, yields quick responsiveness to short messages. ARCNET has built-in CRC-16 (cyclic redundancy check) error checking and supports several physical cabling schemes including fiber optics. Finally there must be low software overhead. ARCNET's data link protocol is self-contained in the ARCNET controller chip. Network functions such as error checking. flow control and network configuration are done automatically without software intervention.

In terms of the International Organization of Standards OSI (Open Systems Interconnect) Reference Model, ARCNET provides the Physical and Data Link layers of this model. In other words. ARCNET provides for the successful transmission and reception of a data packet between two network nodes. A node refers to an ARCNET Controller chip and cable transceiver connected to the network. Nodes are assigned addresses called MAC (medium access control) IDs and one ARCNET network can have up to 255 uniquely assigned nodes.


APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATALINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium