

Networking 101



March 1, 2021

ANDROMEDA PRODUCTIONS

# Physical and Logical Topologies

## Physical Topologies

A physical topology is a schematic representing how the devices, nodes and hardware within a network are connected to each other. The following is a description of some of the most common topologies used in corporate networks in the past twenty years or so

### Star

All devices connect to a switch, allowing new devices to be added with ease, providing the switch or switches have enough free ports. This is by far the most common topology I have encountered in my professional career.



March 2021 | Star Topology. [Online image] Available from: https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages [Accessed 28 March 2021]

**Pros**

* Centrally managed location
* Easy installation of new nodes and equipment
* Highly durable
* More efficient to diagnose when something goes wrong

**Cons**

* Usually requires employees to be trained in the use of networking hardware
* Single point of failure If the switch dies (usually countered with switches working in - failover)
* Can be quite costly to set up reliably
* LAN speed is 100 percent dependant on the maximum throughput of the switch.

### Mesh

All devices are directly connected to each other.



March 2021 | Star Topology. [Online image] Available from: https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages [Accessed 28 March 2021]

**Pros**

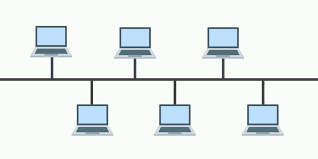
* Data transfer speed between devices is usually the highest of all topologies, since each machine has a separate physical cable connecting it to the other machines on the network.
* If one cable breaks, the link between the two endpoint machines is broken, but the rest of the network integrity remains intact
* As a result, fault finding, and diagnostics is usually simpler with this topology

**Cons**

* Planning and implementation is usually very time consuming
* Devices can only be connected to a small, finite number of other devices (usually limited by the number of available interfaces to be added to the machine)
* Can be quite messy due to the volume of required cables

### Bus

A single, main cable that connects to all the devices to it. Each device then connects directly to the main cable, usually with a coaxial or RJ-45 splitter.



March 2021 | Star Topology. [Online image] Available from: https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages [Accessed 28 March 2021]

**Pros**

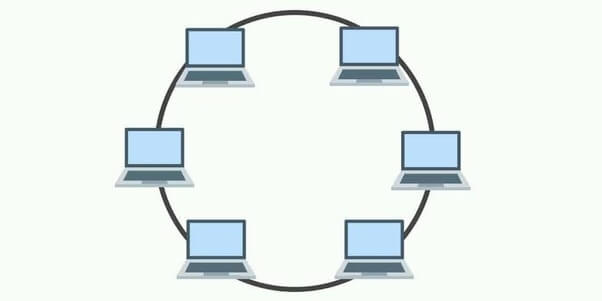
* Easy to install and configure
* Extremely low cost
* Scalability is very high

**Cons**

* If the main cable goes down, then the entire network will drop
* Unidirectional data transfer
* Speed and performance often unreliable, depending on the number of active nodes
* Highly susceptible to traffic collision

### Ring

Like an electronic circuit, each node must be always online, and the data must pass through each one to get to the destination.



March 2021 | Star Topology. [Online image] Available from: https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages [Accessed 28 March 2021]

**Pros**

* Collison unlikely
* Low cost to implement and set up

**Cons**

* All nodes must be available – the network will drop if a single node fails
* Adding nodes needs all other nodes to be shut down and reconfigured
* Speed and performance will drop with each additional node.

Logical Topologies

A logical topology is a networking concept that standardises the way all networked nodes communication with each other using management devices (switches, routers, etc). There are generally two main logical topologies used.

### Bus Topology

The most common logical topology used by far. This topology defines that all devices on the network can broadcast sending data, but only the destination node will reply. DHCP is a good example of this.

### Ring Topology

Single transmission only, in that only one node can send out data at any point. Not practical in most organisations as this would have a detrimental effect on network performance.

# Physical and Logical Addressing

## Physical Address

A physical address, in networking, is the unique Media Access Control identifier that is bound to a network controller and is represented by six groups of two hexadecimal digits. The standard for separating these groups has not been strictly defined, so it is common to see hyphens or colons being used.

There are two primary types of MAC addresses, and these are Unicast and Multicast.

Unicast addresses are bound to a single network interface, whereas a multicast can be bound to multiple address, usually intended for broadcasting to more than one machine on a network.

A MAC address is made up of 48 bits and is commonly split into two groups: Organisational Unique Identifier, and Network Specific Identifier.

An OUI contains information relating to the vendor of that specific hardware, and the NSI contains information relating to the address of the hardware.

## Logical Address

A logical address is the IP address assigned to a device, whether this be dynamic or static. On routers, when a machine in the network first picks up an IP address, it will be stored in an ARP table on the router, which contains mappings of all the logical addresses on the network against the physical address (MAC).

A logical address can change as often as is required, but a MAC address usually remains the same, unless the physical interface is swapped out for any reason. In this event, the router will receive information relating to that IP address and then update the MAC address stored against it in the ARP table.

# Networking Models

## OSI Model

### Application Layer

This is the layer closest to end users and is where the users will enter and receive data. It is responsible for providing services that an application will use to communicate with both users and other applications on the network.

It is often confused as a layer in which actual applications are part of, such as web browsers and application user interfaces but this is not the case. Instead, the application layer simply provides the following functions:

* Presents data to the end users, using visual interfaces to deliver this in a readable manner. (Web browsers, Teams, Discord, etc)
* Enables authentication possibilities where appropriate
* Checks whether required interfaces are present to determine networkable capability

### Presentation Layer

The primary purpose of this layer is to translate data from the application layer. Because there are a plethora of possible data formats it is imperative to ensure the presentation layer is aware of the data formats that are available in order to efficiently manipulate it. This layer is also responsible for:

* Compressing the data
* Encrypting and decrypting of data
* Converting strings to binary/binary to strings
* Preparing and formatting graphic content for use by the Application Layer.

### Session Layer

This layer initiates the opening and closing of sessions between applications. Usually, a session is opened for each piece of information on a separate stream. This allows different streams to provide different piece of information, even from separate sources. The session layer provides the following methods for a stream:

* Saving of the current state (Checkpointing)
* Continuing from checkpoints from (Adjournment)
* Stop the current stream and start again (Restart)
* Stop the current stream and close it (Termination)

### Transport Layer

This layer is responsible for end-to-end communication between two network endpoints (Client-Server). It collects pieces of information from applications and passes them to and from the Network Layer. Error management and correction is also facilitated at this layer. The two main methods of communication at this layer are:

* Transport Control Protocol (TCP) - TCP handshake A three-way communication method that is used to negotiate a reliable connection between two endpoints. When a client sends data using TCP it sends a SYN message which initiates a connection on a specific sequence number. The receiving endpoint then acknowledges this and sends back an ACK message, using the same sequence number. SYN-ACK is the indication that both of these have been sent and received successfully. When information has been sent successfully, a FIN message is finally sent to close the connection
* User Datagram Protocol (UDP) – This is the opposite to TCP, and by extension the TCP handshake. UDP does not facilitate the acknowledgement of packets sent and received, instead just essentially ‘hoping’ for the best. This however allows for a much faster method of communication, as each endpoint does not need to wait for the endpoint to acknowledge that it has received the information

### Network Layer

This is potentially the most important layer of the OSI model. Although each layer works together to send and receive data across the network, this layer is responsible for selecting the best possible route (virtually) between all networked devices.

This layer mediates the connection between the transport layer and the data link layer by responding and issuing requests accordingly.

Routers, Firewalls and often switches all operate at the layer three, providing routing to endpoints by decoding the headers of each packet to view the destination IP addresses and route the information to its intended destination.

### Data-Link Layer

The Data-Link layer is responsible for the organisation and delivery of packet frames between endpoints on the network and consists of two sublayers.

* Media Access Control (MAC) layer, which is used for source and destination physical addresses. Often used in conjunction with an Address Resolution Protocol (ARP) table when only an IP address is known.
* Logical Link Control which manages the flow of data over the network whilst providing simple error checking.

### Physical Layer

This is the lowest level of the OSI model and deals with streams of data bits and how to encode the bits to ensure the correct signals are received at the opposite ends of the physical wire (Ethernet cables as an example).

## TCP/IP Model

### Application Layer

This is the same as the application, presentation, and session layers in the OSI model, but in this layer’s scope in the TCP/IP model it also covers the actual applications that are being used in front of what is displaying the information: Email, RDP, FTP clients, etc.

### Transport Layer

In this model, the Transport Layer is comparable to the Transport Layer of the OSI model, in that it provides functionality to establish connections between endpoints using various protocols.

Again, TCP and UDP are the most common protocols in this layer. This layer does also lend on some of the functionalities that are part of the session layer in the OSI model.

### Internet Layer

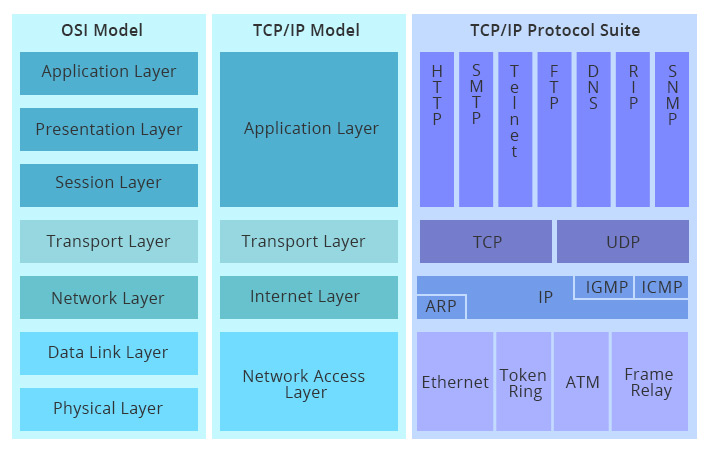
This is essentially a like for like comparison with the Network Layer in the OSI model and does not offer anything more, or anything less that the Network layer.

### Network Access Layer

This is a combination of the Physical Layer and the Data-Link Layer in the OSI model but does have less to offer in that it cannot provide sequencing functionalities provided by layer two of OSI.

## OSI vs TCP

Consider the following image:



Nov 2017 | TCP/IP vs OSI comparison. [Online image] Available from: https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html [Accessed 29 March 2021]

Using the image above we can clearly see that both the OSI model and the TCP/IP model govern the same protocols and suites, but in uniquely different ways.

This is likely since the TCP/IP model, created in the 70s, was created reactively to address networking problems at the time.

In contrast to this, the OSI model is not just a standard for governing how data flows through a network but is also a framework that standardises the creation of networking hardware, whether it be switches, routers, firewalls, or perhaps even hubs to allow them to fit universally into most, if not all networks worldwide, providing they are following the same standard.

From a technical point of view, the OSI model adds more complexity as there are more levels involved. However, in most corporate environments this complexity is quite often an enhancement over the TCP/IP model, as it allows network engineers to diagnose problems more efficiently, due to the granular, module structure it has.

## Common Application Layer Protocols

**FTP**

File Transfer Protocol – A client-server communication protocol used for transferring files and folders to remote endpoints. The FTP protocol provides functionality for user authentication and secure transmission. FTP Servers utilize FTP to host repositories in which users can upload and download resources and usually operate on TCP ports 20, 21, and 22.

**HTTP/HTTPS**

Hypertext Transfer Protocol - A client-server model that facilitates sending and receiving hypermedia content such as images, audio, links, video, and plain text. HTTP was designed explicitly to be used with web servers as a backend, and a web browser as the front end. HTTP does not keep records of any information sent to or from nodes using the service. This is known as a stateless protocol. Web servers usually operate on TCP ports 80 and 443. The latter is used when HTTP is combined with a valid, signed SSL certificate. This is known as HTTPS.

**DNS**

Domain Name System – A hierarchical decentralized system for computers and other networked devices, connected to both private and public networks. At its core it is used to translate networked device hostnames to IP addresses. For example, [www.google.co.uk](http://www.google.co.uk) is a domain name that points to a public IP address for a Google web server. DNS uses both UDP and TCP port 53.