**Network Reference Models Network Topologies** (Huawei, 2022)

It is a schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

|  |  |
| --- | --- |
| * **Star Topology** – in this type of topology, the computers are connected to a single hub through a cable. This hub is the central node while all other nodes are connected to it.   + Advantages: New nodes can be easily added to the network. Communication data must be forwarded by the central node, which facilitates network monitoring.   + Disadvantages: Faults on the central node affect the entire network's   communication. | Icon  Description automatically generated |
| * **Bus Topology** – a network type in which every computer and network device is connected to a single cable. When it has exactly two (2) endpoints, then it is called **Linear Bus Topology**. All nodes are connected through a bus (ex. coaxial cable).   + Advantages: The installation is simple and cable resources are saved. Generally, the failure of a node does not affect the communication of the entire network.   + Disadvantages: A bus fault affects the communication of the entire network. The information sent by a node can be received by all other   nodes, resulting in low security. | Timeline  Description automatically generated |
| * **Ring Topology** – forms a ring as each computer is connected to another computer, with the last one (1) connected to the first—exactly two (2) neighbors for each device.   + Advantages: Cables resources are saved.   + Disadvantages: It is difficult to add new nodes. The original ring must be interrupted before new nodes are inserted to form a new ring. | Shape, polygon  Description automatically generated |
| * **Tree Topology** – has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three (3) levels to the hierarchy.   + Advantages: Multiple star networks can be quickly combined, facilitating network expansion.   + Disadvantages: A fault on a node at a higher layer is more severe. | Icon  Description automatically generated |
| * **Mesh Topology** – a point-to-point connection to other nodes or devices. All the network nodes are connected.   + **Partial Mesh Topology** – in this topology, some systems are connected in the same fashion as mesh topology, but some devices are only connected to two (2) or three (3) devices.     - Advantages: The cost of a partial-mesh network is lower than that of a full-mesh network.     - Disadvantages: The reliability of a partial-mesh network is lower than that of a full-mesh network.   + **Full Mesh Topology** – each node or device is connected.     - Advantages: It has high reliability and high communication efficiency.     - Disadvantages: Each node requires a large number of physical ports and interconnection cables. As a result, the cost is high, and it is difficult to expand. | A picture containing polygon  Description automatically generated  **PARTIAL**  A picture containing icon  Description automatically generated  **FULL** |

|  |  |
| --- | --- |
| * **Hybrid Topology** – it consists of a mix of two (2) different types of topologies merging as one network.   + In actual networking, multiple types of topologies may be combined based on the cost, communication efficiency, and reliability requirements. | Shape  Description automatically generated |

**Common Network Devices** (Huawei, 2022)

|  |  |
| --- | --- |
| **Terminal device**  It is the end-device of the data communication system. *It provides the necessary functions required by the user access protocol operations.*   * This includes **data terminal equipment (DTE)** such as a PC, phone, handsets, printers, and servers. * A **network interface card (NIC)** is a key component that connects directly to a device that allows access to a network such as an internet or a local network. | Graphical user interface, diagram, application  Description automatically generated |
| **Switch**  It is the device closest to end-users, used to access the network and switch data frames.   * Switches belonging at the access layer are usually Layer 2 switches, also known as **Ethernet switches**. * A **broadcast domain** is a set of nodes that can receive broadcast packets from a node. * The Ethernet switch can implement the following functions:   + Data frame switching   + Access to end-user devices   + Basic access security functions   + Layer 2 link redundancy. | Diagram  Description automatically generated |
| **Router**  It is a network-layer device that forwards data packets on the Internet.   * A **modem** is a device that connects a network to the Internet. It takes signals from your **Internet service provider (ISP)** and translates them into signals connected to the local devices. * **Gateway** *is a term for a router that* provides functions such as protocol conversion, route selection, and data exchange when networks using different architectures or protocols   communicate with each other. | Diagram  Description automatically generated |
| **Firewall**  It is a network security device used to ensure secure communication between two networks.   * It monitors, restricts, and modifies data flows passing through it to shield information, structure, and running status of internal networks from the public network * It is located between two (2) networks with different trust levels (for example, between an intranet and the Internet). * It controls the communication between the two networks and forcibly implements unified security policies to prevent unauthorized access to important information resources. | A picture containing text, electronics, jack, screenshot  Description automatically generated |

|  |  |
| --- | --- |
| **Wireless Devices**  It is a network that uses radio waves, laser, and infrared signals to replace some or all transmission media in a wired LAN.   * Common Wi-Fi is a WLAN technology based on the **IEEE 802.11 family** of standards.   + **Fat Access Point (Fat AP)** applies to homes. It works independently and needs to be configured separately. It has simple functions and low costs.   + **Fit Access Point (Fat AP)** applies to medium- and large-sized enterprises. It needs to work with the AC and is managed and configured by the AC.   + **Access Controller (AC)** is generally deployed at the aggregation layer of the entire network. The AC provides wireless data control services featuring large capacity, high performance, high reliability, easy installation, and easy maintenance. |  |

# Networking based on Geographical Coverage

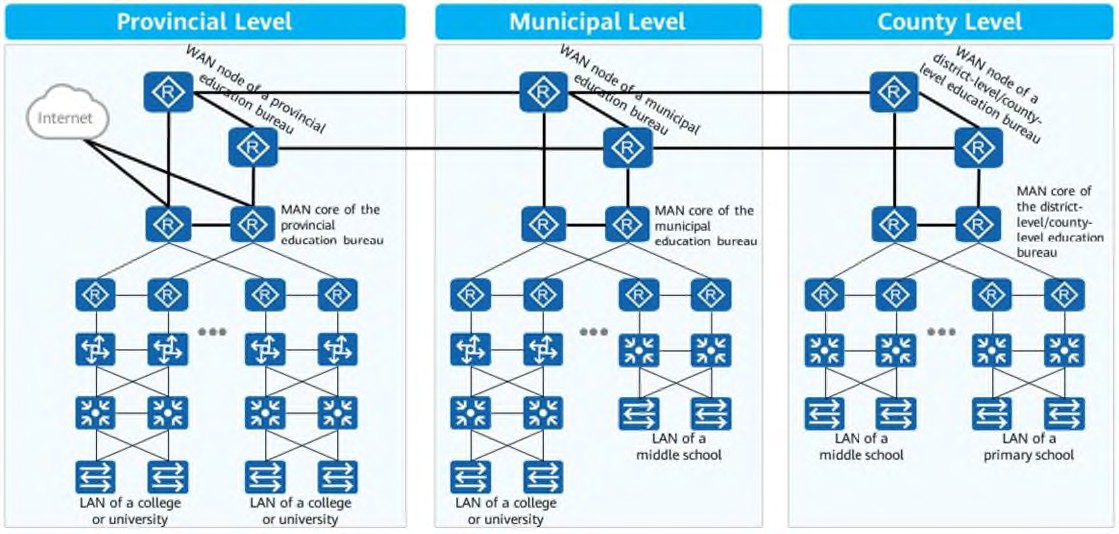
* **Local Area Network (LAN)**
  + A LAN generally covers an area of a few square kilometers.
  + The main function is to connect several terminals that are close to each other (within a family, within one or more buildings, within a campus, for example). Technologies used: Ethernet and Wi-Fi.

# Metropolitan Area Network (MAN)

* + A MAN is a large-sized LAN, requiring high costs but can provide a higher transmission rate. It improves the transmission media in LANs and expands the access scope of LANs (able to cover a university campus or city).
  + The main function is to connect hosts, databases, and LANs at different locations in the same city.
  + Technologies used: Ethernet (10 Gbit/s or 100 Gbit/s) and WiMAX.

# Wide Area Network (WAN)

* + A WAN generally covers an area of several kilometers or larger (thousands of kilometers for example).
  + It is mainly used to connect several LANs or MANs that are far from each other (for example, across cities or countries). Telecom operators' communication lines use HDLC and PPP.



**OSI Reference Model** (Huawei, 2020)

**The Open Systems Interconnection (OSI) model** is a descriptive network scheme. The OSI model describes how information or data makes its way from application programs through a network medium to another application program located on another network.

* **LAYER 7: APPLICATION LAYER** is the OSI layer that is closest to the user. It provides network services to the

user’s applications such as spreadsheet programs, word processing programs, and bank terminal programs.

* + The application layer establishes the availability of intended communication partners, synchronizes, and establishes agreement on procedures for error recovery and control of data integrity.
* **LAYER 6: PRESENTATION LAYER** ensures that the information that the application layer of one (1) system sends out is readable by the application layer of another system.
  + If necessary, the presentation layer translates between multiple data formats by using a common format. Provides encryption and compression of data. Examples: JPEG, MPEG, ASCII, HTML.
* **LAYER 5: SESSION LAYER** defines how to start, control and end conversations (called **sessions**) between applications. It also synchronizes dialogue between two (2) hosts’ presentation layers and manages their data exchange.
* **LAYER 4: TRANSPORT LAYER** regulates information flow to ensure end-to-end connectivity between host applications reliably and accurately. This layer segments data from the sending host’s system and reassembles the data into a data stream on the receiving host’s system.
* **LAYER 3: NETWORK LAYER** defines end-to-end delivery of packets. It defines how routing works (identifying endpoints) and how routes are learned so that the packets can be delivered.
  + The network layer defines how to fragment a packet into smaller packets to accommodate different media. Examples: Routers operate at Layer 3 - IP, IPX, AppleTalk.
* **LAYER 2: DATA LINK LAYER** provides access to the networking media and physical transmission across the media and this enables the data to locate its intended destination on a network.
  + The data link layer provides reliable transit of data across a physical link by using the **Media Access Control (MAC) addresses**.
  + This layer is concerned with network topology, network access, error notification, ordered delivery of frames, and flow control. Examples: Ethernet, Frame Relay, FDDI.
* **LAYER 1: PHYSICAL LAYER** deals with the physical characteristics of the transmission medium. It defines the electrical, mechanical, procedural, and functional specifications for achieving, maintaining, and deactivating the physical link between end systems.
  + Such characteristics as voltage levels, the timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications. Examples: EIR/TIA-232, RJ45, NRZ.

# TCP/IP Model

It is a networking model with a set of communication protocols for the Internet and similar networks. It is commonly known as TCP/IP because its Transmission Control Protocol and Internet Protocol (IP) were the first networking protocols defined in this model. **Internet Protocol (IP)** provides basic communication. **Transmission Control Protocol (TCP)** provides key functions that applications need.

* **APPLICATION LAYER** represents an interface through a variety of protocols that enable services to be applied to end-user application processes. These services include handling high-level protocols, issuing of representation, encoding, and dialog control.
* **TRANSPORT LAYER** is responsible for reliable end-to-end data delivery from the source host to the destination host.
* **INTERNET LAYER** (Network) is responsible for the delivery of service requests that respond from the transport layer and have them arrive at their destination through the “virtual network” image of the Internet.
* **NETWORK ACCESS LAYER** is also called the host-to-network layer, which is concerned with all of the issues that an IP packet requires to make a physical link to the network media. The network interface layer functions include mapping the IP addresses to physical hardware addresses and encapsulation of IP packets.

**Comparison of OSI Reference Model to TCP/IP Model** (Williams, 2021)

|  |  |
| --- | --- |
| * The OSI Model is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. On the other hand, TCP/IP helps you determine how a specific computer should be connected to the Internet and how you can be transmitted between them. * OSI follows a vertical approach, whereas TCP/IP follows a horizontal approach. * The OSI model’s, transport layer is only connection-oriented, whereas the TCP/IP model is both connection-oriented and connectionless. * OSI model is developed by ISO (International Standard Organization), whereas TCP Model is developed by ARPANET (Advanced Research Project Agency Network). * OSI model helps you standardize router, switch, motherboard, and other hardware whereas TCP/IP helps you establish a connection between different types of computers. | Diagram  Description automatically generated |

# References:

Comer, D. (2019). *The internet book: Everything you need to know about computer networking and how the Internet works*. CRC Press.

Huawei. (2020). *HCIA-Datacom V1.0 Training Material*.

Karumanchi, N., Damodaram, A., & Rao, S. (2020). *Elements of computer networking: An integrated approach.* Career Monk.

Kurose, T & Ross, K. (2021). *Computer networking: A top-down approach.* Pearson. Robertazzi, T. (2017). *Introduction to computer networking.* Springer International.

Williams, L. (2021). TCP/IP vs OSI model: What’s the difference? [Web Article]. Retrieved on January 21, 2020, from https://[www.guru99.com/difference-tcp-ip-vs-osi-model.html](http://www.guru99.com/difference-tcp-ip-vs-osi-model.html)