LAB 1

Overview of Networks and layered communication, understanding of networking equipment.

Protocols:

A Protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulates the following characteristics of a network:

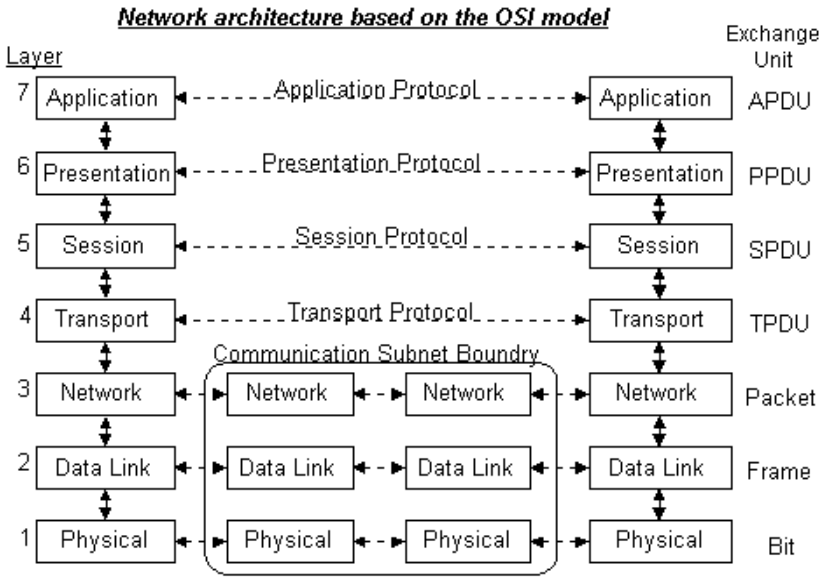
- Access method
- Allowed physical topologies
- Types of cabling
- Speed of data transfer

Layered Communication:

Computers communicate using a layered set of protocols. Layers provide a division of the work done by a network. Networks are set up with a protocol hierarchy that divides the communication task into several layers. The main example of layered communication is OSI reference model.

OSI Layer:

The OSI reference model organizes a network into seven layers (a **protocol stack**). These layers define how networking hardware and software are to hand data and transfer it across a network. Interoperability, the purpose for defining a standard protocol model, exists when there is compatibility between the protocol stack of one workstation or peripheral device and that of another. Each layer is able to communicate with the corresponding layer of a receiving station.



- **Physical Layer** – consists of rules for dealing with hardware, such as voltages, bit-rates, frequencies, etc. The medium is below this and not given an actual layer assignment. For example: Network Interface Cards (NICs), Repeaters and Hubs.
- **Data-Link Layer** - this layer communicates using chunks of data called frames. The data-link layer can perform error checking and control the rate of flow of information. The data link layer is for a wire with just two ends, one sender and one receiver. For example: Bridges and Switches manipulate data in the Data-Link Layer.
- **Network Layer** - The network layer deals with addresses and provides message or **packet routing**. (Note: packets are like frames, but in the network layer.) Because not all devices are directly connected to each other, some packets may have to take several **hops** to get from source to destination. Finding a route for packets in a potentially large and changing network is the job of the network layer. **IP** is a network layer protocol, and **IP address** is what IP uses to determine where a packet should go. **Logical network addressing and routing occur in the Network Layer. Routers and Layer 3 switches are devices that operate at the Network layer.**
- **Transport Layer** - The transport layer provides reliable, transparent transfer of data between commputers on a network. The transport layer is the lowest layer to provide and end-to-end view of the communication. The transport layer may have to break the data into packets for the network layer. It is then the transport layer's job to make sure they are reassembled in the right order. The interaction between the end-to-end view of this layer and the machine-to-machine view of the network layer is probably the most critical one in the hierarchy. **TCP** is a transport protocol. Actually, both **TCP** and **IP** are part of the **TCP/IP model** instead of the OSI model. The TCP/IP model owes its success (and its name) to these two hardworking protocols, despite definitions in other layers in the TCP/IP model that are weaker than those in the OSI model. **TCP/IP and IPX/SPX Protocols are active at the Transport Layer.**
- **Session Layer** - The session layer provides remote logons and some other things. May software developers have considered this layer fairly useless and simply absorb any needed functions into their application programs. Different network operating systems (Novell,WindowsNT) utilize this layer for different purposes.
- **Presentation Layer** - The presentation layer is also frequently bypassed, but it can provide translation of data transferred between applications. If data from a spreadsheet needs to be converted to data for a database, this happens at the presentation layer.
- **Application Layer** - The application layer contains communication services that include file transfer and message handling like Telnet, FTP, and email. These services then interact with other applications such as word processing, databases, and World Wide Web browsers.

Network Hardware:

Network hardware is a set of physical or network devices that are essential for interaction and communication between hardware units operational on a computer network. These are dedicated hardware components that connect to each other and enable a network to function effectively and efficiently.

Repeater:

Repeaters are simple devices that work at the physical layer of the OSI. It regenerates the signals.

Hub:

A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices. Network hubs are best suited for small, simple local area network (LAN) environments.

There are mainly two types of hubs:

1. **Passive:** The signal is forwarded as it is.
2. **Active:** The signal is amplified, so they work as repeaters.

Switch:

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s). It supports unicast, multicast as well as broadcast communications.

Most common switching methods are:

1. **Cut-through:** Directly forward what the switch gets.
2. **Store and forward:** receive the full frame before retransmitting it.

Normal Switches are on the data link layer (just above physical layer), that's why they deal with frames instead of bits and filter them based on MAC addresses. Switches are known to be used for their filtering capabilities. Intelligent switches work as a router.

Virtual LANs:

VLANs (Virtual LANs) and broadcast domains: Switches do not control broadcast domains by default, however, if a VLAN is configured in a switch it shall have its own broadcast domain.

VLAN is a logical group of network devices located on different LAN physical segments. However, they are logically treated as if they were located on a single segment.

Bridges:

Bridges are used to extend networks by maintaining signals and traffic. Bridges are on the data link layer so in principle they are capable to do what switches do like data filtering and separating the collision domain, but they are less advanced. They are known to be used to extend distance capabilities of networks.

In a comparison with switches, bridges are slower because they use software to perform switching. They do not control broadcast domains and usually come with a smaller number of ports. Multiport bridges are generally termed as switch.

Routers:

Routers are used to connect different LANs or a LAN with a WAN (e.g. the internet). Routers control both collision domains and broadcast domains. If the packet's destination is on a different network, a router is used to pass it the right way, so without routers, the internet could not functions. Routers use NAT (Network Address Translation) in conjunction with IP Masquerading to provide the internet to multiple nodes in the LAN under a single IP address. Routers work on the network layer so they can filter data based on IP addresses. They have routing tables to store network addresses and forward packets to the right port.

Gateway:

Gateways are very intelligent devices or else can be a computer running the appropriate software to connect and translate data between networks with different protocols or architecture, so their work is much more complex than a normal router. For instance, allowing communication between TCP/IP clients and IPX/SPX or AppleTalk. Gateways operate at the network layer and above, but most of them at the application layer.