Networking Devices and Network Topologies

Sai Pramod Yerubandi

Dept. of Computer Information Sciences

IUPUI

Abstract- To connect a group of computers or any other devices that can be able to share information we need a network. So various protocols and architectures are used to connect the devices with each other and share information in an efficient way. To implement those networks various hardware devices are needed that can communicate with all kinds of networks, those hardware devices are called as networking devices. Another important factor that should be considered for network communication is network topology. This paper provides a succinct study on various networking devices and their underlying topologies.

Keywords- **LANs, WANs, Switch, Router, Network Topology, Firewalls, Hubs, Bridges, Modems, Access Points (APs), NIC's.**

Introduction:

Computer Networking is a process which involves he transportation and exchange of data between two or more machines or nodes across a shared platform. To establish any connection a hardware i.e. a networking device and a software (to manage the network) is needed, understanding the functionality and the connectivity of the used network device is required for any network administrator. To perform the functions in a discrete way networks also need some networking protocols. Networks primarily are of two types:

- Wired networks: In any wired network a physical medium is needed to transport the data across the machines. The physical medium can be anything like an ethernet cable or an optical cable etc.
- Wireless networks: All the wireless networks use radio waves to exchange the data.

Wired networks are considered to be more reliable and faster when compared with the wireless networks [1]. Apart from wired and wireless network can further be categorized into LANs and WANs, where LAN stands for Local Area Network and WAN stands for Wide Area Network, both LAN and WAN can be implemented in both wired and wireless connectivity. LAN uses an ethernet cable to provide by connectivity by means of wired network and Wi-Fi services provided by the router to provide connectivity by means of wireless networks. WAN uses fiber optic cables, telephone lines etc. to provide connectivity by means of wired network and cellular network systems are used to provide the connectivity by means of wireless WAN network [2]. This paper provides a precise description of the devices that are needed to implement any network. In addition to this, a detailed study on various network topologies is also provided in this paper.

Networking Devices:

Hubs

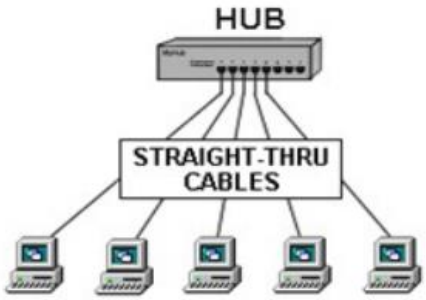
Hubs are networking hardware devices that are used at the end of the network. A network in which devices are connected using twisted pair cables uses hubs. The functionality of hubs is

simple, it just directs the data packets to all the network devices that are connected to the hubs irrespective of the packet destination. Hubs can also be used to create larger networks by joining them together. The functionality of the hub makes it inefficient device on busy networks as they can create a bottleneck [3].

Hubs can be categorized into two types-

- Passive hub – A passive hub just provides a path for the data signals. Except for providing the pathway it does nothing.
- Active hub – An active hub regenerates the electric signal and then forwards the data signal to all the devices that are connected to the hub.

Neither processing of the data nor performing the error check on the data is done by the hub [4].



MSAU

MSAU stands for multi station access unit, it is used in token ring network. In token ring network MSAU is used in place of hub which is implemented on ethernet network [3]. Each MSAU will have a Ring In port and Ring Out port, the Ring In port will be connected to the Ring Out port on the next MSAU, thereby the last MSAU will be connected to first MSAU to complete the ring.

Switches

Switches are similar to hubs, they collect the data from the devices which are connected to them. Devices are connected to a switch by using twisted cables. Unlike hubs, switches are more advanced, and they transfer the data only to one port and that is of the destination device [3]. This is done by using the MAC address, a switch learns the MAC addresses of the devices that are connected to it and then it checks for the destination MAC address from the data received and matches with destination MAC address it receives. Thus, by forwarding the data to only the destination device a switch improves the network performance by –

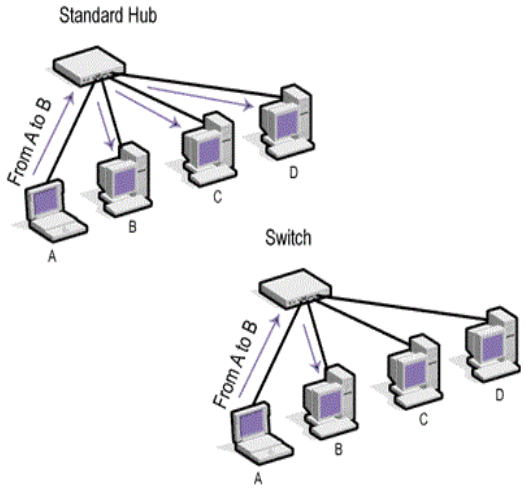
- Establishing a direct link between the switch and the other device connected to it, collision occurrence can be reduced.
- Switches perform in full-duplex (sending and receiving the data simultaneously) mode if there is no collision. In half-duplex mode of switches communication can happen only in one direction.

Thus, switches can perform better when compared with hubs in busy networks. Switches deal with data in the following ways,

- Cut-through – In this function, the packet will be forwarded as soon as it is received by the switch. By using this method there is more possibility of errors as error checking is not done, but this is a very fast approach for forwarding the packet by using a switch.
- Store-and-forward – In this function, the entire packet is received by the switch and the packet will be checked for errors and then it will be forwarded to its destination. The advantage of this method is that network will be error free i.e. errors will not be propagated in the network. Store-and-Forward function is slow as switch takes time for error checking.
- Fragment-Free – This function uses the benefits provided by the Store-and-Forward and transmits the packet faster than the Store-and-Forward function. In this function

switch does not read the entire packet, instead it reads sufficient enough to identify the collision status of the packet. The packet will be forwarded once its collision status is identified, thereby taking less time to forward the packet when compared with Store-and-Forward function.

The following figure differentiates the functionality of switch and hub [5].



Bridges

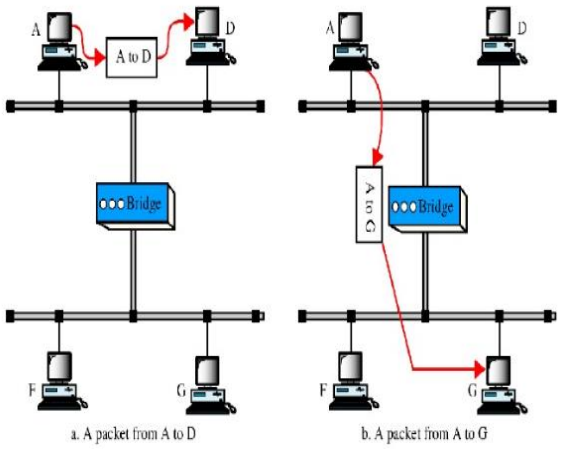
Bridges are the devices that can connect two or more networks to make it into a single large network. Packets that are destined from network to another network only will be forwarded by the bridges [6]. Bridges can combine any two or more different kinds of networks. Bridges can forward the packets from one network to other based on the MAC address of the devices connected in the network segments. Bridges can also block the data if the packet is not destined to the other network. So, in simple words bridges can forward the packet from one network to other and can also block the packets which are trying to passing from one network to other [3]. The issues that might occur when using bridges are:

- Placement – The placement of the bridges in the network should be done based on 80/20 rule i.e. 80% of the data transfer should be within the same network and other 20% of the data transfer should be from one network to another network.
- Bridging loops – When more than one bridge is placed in the network bridging loops occur. When more than one bridge is placed in the network, bridges confuse each other by making each other to believe that a device which is not existing to be existing in a network segment. STP protocol has been introduced to overcome this problem [7].

There are three types of bridges namely,

- Transparent bridge – The devices in the network will be unaware of bridge in the network.
- Source route bridge – In source route bridge networks the packet contains its entire propagation paths embedded in it.
- Translational bridge – These bridges are used to convert the format of the data from one network to another

The following figure shows the functionality of bridge [8].



Routers

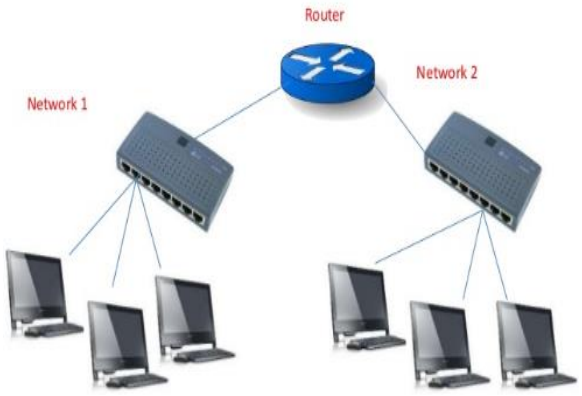
Similar to bridges, routers also combine two or more networks to one large network. A router can be a network hardware or a computer machine which has more than one network interface and a routing software. A router routes the data received by it from one network to

another network. Routers can also be connected to the service providers and act as a gateway to the other networks [10]. After receiving the data packet, router reads the packet header to get the destination address. After getting the destination address it tries to match the destination address with the addresses that are available in its routing table, if the address matches the router forwards the packet to the next hop which can be the end point for the packet or any other router. Thus, the routing table plays a crucial role in routing the packet. Routing table can be populated by the router in two ways:

- Static Routing – When routing information and routes are entered into the routing tables manually then we call it as a static routing environment. In static routing environment errors are more frequent because of manual entry and it is also time-consuming process. If any changes are made in the network, topology etc. even those changes should be made in the routing tables manually. Static routing is suitable only for small networks, in case of large networks dynamic routing is preferred.
- Dynamic Routing - Routing protocols are used to communicate with each other in dynamic routing networks. The functionality of these protocols is to enable all the routers in the network to share their information with each other to populate the routing table of every router [9]. We have two routing protocols namely,
    - Distance Vector Routing
    - Link State Routing

In Distance Vector Routing, each router calculates the distance between itself and neighbors, then the router shares the information about the network to its neighbors and based on the neighbors the router updates its table. Bellman Ford Algorithm is used to make the routing tables. Information sharing with neighbors is done at regular intervals.

In Link State Routing, every router passes the information of its neighbors with each other router in the network. Sharing of information happens only when there are any changes. Dijkstra's Algorithm is used for making routing tables [10].



Gateways

Gateway is hardware device that is used to convert data from one format to another format. Router can be an example of gateway as it converts data from one protocol to other. Similarly, any software application that can convert data from one format to another can also be called as a gateway. Gateway converts the format of the data alone and not the data.

Network Card

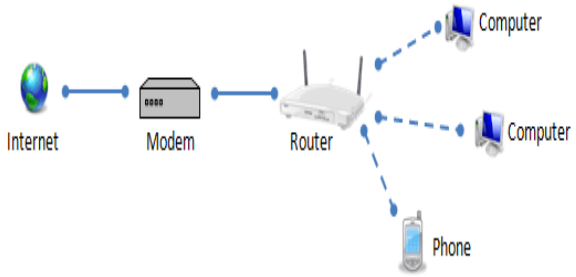
Network cards which are also known as NIC's (Network Interface Cards) is a hardware component which enables a computer or any other device to connect to any network (both wired network and wireless network). All the latest devices will have NIC integrated on their motherboard chipset [11].

Modems

A modem is a network hardware device that enables any device to transfer the data over a wired or wireless connection. The modulating and demodulating of the data is done by modem. During data transmission modem converts the digital data sent by the computer to analog signals so that they can be transmitted through

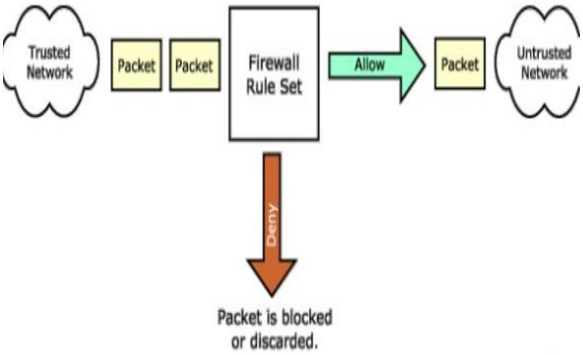
telephone cables and the receiver the modem is used to convert the analog signals to the digital format [12]. Apart from modulating and demodulating the data, modems also perform error check i.e. to identify whether the packet was involved in collision or not, it also performs flow control of data and data compression.

The following diagram shows the functionality of a modem [13].



Firewall

Firewall can be either a simple piece of software or a network hardware device that will filter the information received by the machine or a private network from the internet connection. Firewalls are placed either at entry or exits of a network. Apart from filtering the data coming from public network to private network, firewalls can also control the access between network segments [14]. The software firewalls are implemented in organizations through Windows, Linux or Mac OS servers [3]. The hardware firewalls will be implemented in the network to protect the devices from outside network traffic i.e. the devices that are behind the firewall will be protected from public traffic in the network [15].



Network Topologies:

The logical or physical layout of a network is known as network topology. Apart from describing the places and the mechanism of the devices connected to a network, it also describes the way the data is transferred between the devices [16]. The different categories of network topologies are as follows,

Bus Topology

In this topology a single bus i.e., a wired cable runs across a network and all the nodes i.e. the devices are connected to the bus. This topology is very popular for LAN (local area networks). In bus topology as all the nodes share a common bus the cost will be very cheap as only one single cable will be used to connect all the devices and if any one node is damaged or if there is any fault in any one single node, the nodes in the entire network may get affected [18]. A terminator is used at each end of the bus or cable [17]. In bus topology data transmission between the nodes happen through the shared bus.

Pros:

- Cost efficient.
- Easy to connect new devices.
- Reliable in case of small networks.

Cons:

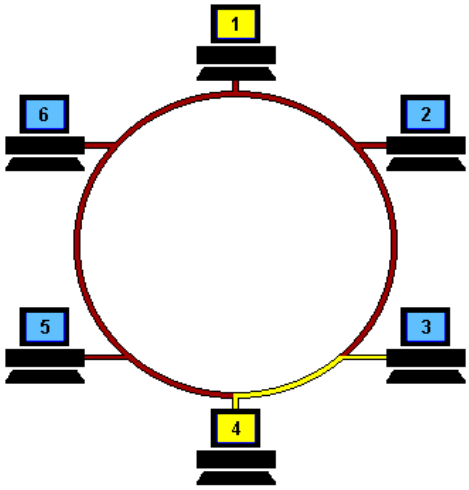
- Entire networks fail if the bus breaks down.
- Increase in number of devices reduces the network speed.
- Not suitable for large networks.

Ring Topology

Ring topology is pretty like bus topology, bus topology is a linear topology and in ring topology each node is connected to its neighboring node and the last node will be connected back to the first node. In ring topology data transmission happens from one node to another. In ring topology network only one node can access the topology at any time [20].

Pros:

- Reliable for large networks.
- All nodes will have equal access to resources.
- Easy to identify the faults in network [19].



Cons:

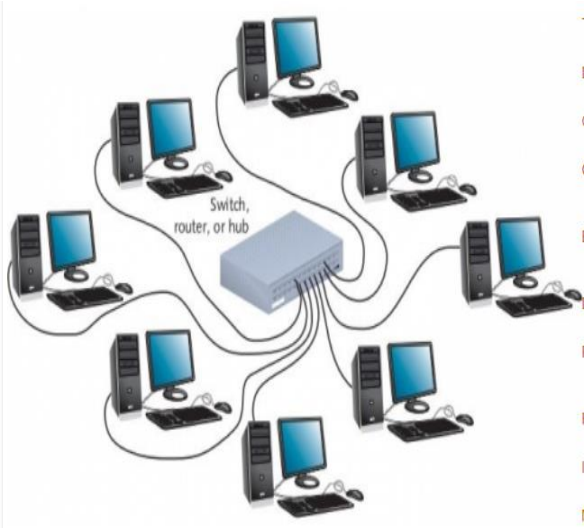
- Moving, changing or adding devices will affect network.
- Failure of any single link between two nodes leads to entire network failure.
- Increase in number of nodes leads in communication delay.

Star Topology

In star topology also known as star network, all the nodes in the network connect to a network device at the center. The device in the center will act as a server and the other devices will act as clients. Data communication happens through the central network device. In star topology failure of one node doesn't affect the other nodes in the network [18].

Pros:

- More reliable than ring topology.
- It is easy to add or remove devices from the network.
- Multiple cable types can be used in the same network [21].



Cons:

- Cost is high.
- Failure of central device leads to failure of network.
- The performance of the network is determined by the central device [22].

Mesh Topology

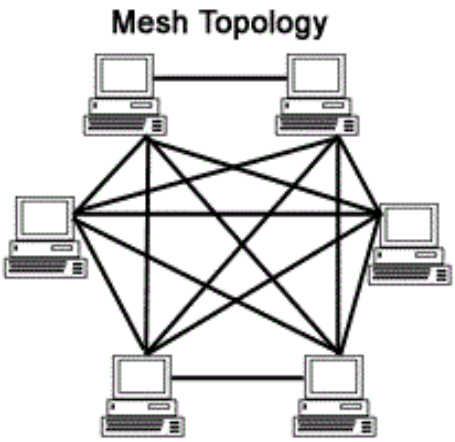
In mesh network topology each device is connected to most of the other nodes in the network. Data communication happens between the nodes, no centralized device is needed for communication. Mesh network topology can be categorized into two,

- Full mesh network topology, in full connected mesh network all the nodes in the network are connected to each other.

- Partial mesh network topology, in partial mesh network topology all the nodes are not connected to each other [23].

Pros:

- Data load can be different for each connection.
- Diagnosing a fault in any node is easy.
- Secured network [24].



Cons:

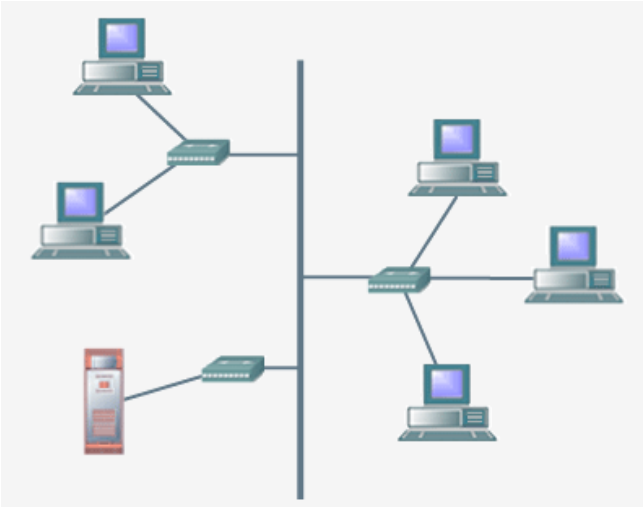
- Installation will be difficult in case of large networks.
- More wiring will be required.
- Cost will be more and higher in case of large network.

Tree Topology

Combination of bus topology and star topology network is called as tree network topology. In tree network topology hub devices connect to the bus. Tree topology is effective when communication happens between two networks [25].

Pros:

- More nodes can be accommodated in hierarchical chain.
- Fault finding is easy and easy to maintain.
- If one hierarchical network goes down other networks will not be affected [24].



Cons:

- Maintenance cost will be high.
- Bus breakdown results in network failure.

Appendix:

AP	Access Point
NIC	Network Interface Card
LAN	Local Area Network
WAN	Wireless Area Network
MSAU	Multi Station Access Unit
STP	Spanning Tree Protocol
MAC address	Medium Access Control address

Conclusion:

In this paper, important traditional devices are introduced that help build the networks and it also presents a precise information on functionality of these traditional networking hardware devices and network topologies used to build any network. Advantages and disadvantages of network topologies have also been described. Few approaches that help to deal with network related problems are also mentioned.

References:

1. Networking Devices and Topologies: A Succinct Study. (n.d.). Retrieved from https://pdfs.semanticscholar.org/9aea/0d3998cfdf9d95480410c71fa70a08d5bc7c.pdf
2. WAN vs LAN. (n.d.). Retrieved from https://business.cableone.net/business-resources/business-internet/wan-vs-lan
3. Networking Devices. (n.d.). Retrieved from https://www.pearsonhighered.com/assets/samplechapter/0/7/8/9/0789732548.pdf
4. Networking Components Quick Guide. Hubs Device that splits a network connection into multiple computers Data is transmitted to all devices attached Computers. - ppt download. (n.d.). Retrieved from https://slideplayer.com/slide/9918293/
5. Hussain, S. F. (n.d.). Network Switch VS Hub: Which One Is Better? Retrieved from https://www.networking-basics.net/network-switch-vs-hub/
6. Projects, C. T. (2018, November 29). Switches, Routers, Bridges and LANs/Bridges. Retrieved from https://en.wikibooks.org/wiki/Switches,_Routers,_Bridges_and_LANs/Bridges#Bridge
7. Bridge Placement and Bridging Loops. (n.d.). Retrieved from https://www.brainbell.com/tutorials/Networking/Types_Of_Bridges.html
8. Rupinderj Follow. (2012, May 05). Networking devices. Retrieved from https://www.slideshare.net/rupinderj/networking-devices-12807479
9. Exploring the Functions of Routing. (2012, November 28). Retrieved from http://www.learncisco.net/courses/icnd-1/lan-connections/functions-of-routing.html
10. AmzadKhn Follow. (2015, May 01). Router & functionality. Retrieved from https://www.slideshare.net/AmzadKhn/router-functionality
11. What is a Network Interface Card (NIC)? - Definition from Techopedia. (n.d.). Retrieved from https://www.techopedia.com/definition/5306/network-interface-card-nic
12. What is the Function of a Modem. (n.d.). Retrieved from https://techspirited.com/what-is-function-of-modem
13. Modem vs Router. (n.d.). Retrieved from https://www.diffen.com/difference/Modem_vs_Router
14. Tyson, J. (2000, October 24). How Firewalls Work. Retrieved from https://computer.howstuffworks.com/firewall1.htm
15. Amin, N. (2017, January 16). Firewall and its types and function. Retrieved from https://www.slideshare.net/nisargamin6236/firewall-and-its-types-and-function
16. What is Network Topology? - Definition from Techopedia. (n.d.). Retrieved from https://www.techopedia.com/definition/5538/network-topology
17. What is Bus Topology? Advantages and Disadvantages. (n.d.). Retrieved from https://www.orosk.com/bus-topology/
18. K. (n.d.). Network Structure or Topology. Retrieved from http://www.ijarcsms.com/docs/paper/volume1/issue2/v1i2-0006.pdf
19. ... (n.d.). Network Troubleshooting and Resource Site for School IT Staff. Retrieved from http://webpage.pace.edu/ms16182p/networking/ring.html
20. What is Ring topology ? Advantages and Disadvantages. (n.d.). Retrieved from https://www.orosk.com/ring-topology/
21. Solutions, S. (1970, January 01). FINAL YEAR NS2 PROJECTS. Retrieved from http://finalyearns2projects.blogspot.com/2015/11/what-is-star-topology.html
22. What is Star Topology? (2018, January 24). Retrieved from https://www.computerhope.com/jargon/s/startopo.htm

23. Shekhar, A. (2017, March 06). What Is Mesh Topology? Advantages And Disadvantages Of Mesh Topology. Retrieved from https://fossbytes.com/what-is-mesh-topology-advantages-and-disadvantages-of-mesh-topology/
24. (n.d.). Retrieved from http://units.folder101.com/cisco/sem1/Notes/ch2-topologies/toplogies.htm
25. Shekhar, A. (2017, December 14). What Is Tree Topology? Advantages And Disadvantages Of Tree Topology. Retrieved from https://fossbytes.com/tree-topology-advantage-disadvantage/
26. Network Protocols Handbook. (n.d.). Retrieved from http://bkarak.wizhut.com/www/lectures/networks-07/NetworkProtocolsHandbook.pdf
27. What is Networking (computer)? - Definition from WhatIs.com. (n.d.). Retrieved from https://searchnetworking.techtarget.com/definition/networking