Volume 2, Issue 11, November 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Networking Devices and Topologies: A Succinct Study

Sushruta Mishra
Dept. of CSE, GEC,BBSR
India

Lamboder Jena
Dept. of CSE, GEC,BBSR
India

Aarti Pradhan
Dept. of CSE, GEC,BBSR
India

Abstract- A network can be defined as a group of computers and other devices connected in some ways so as to be able to exchange data. Now in real life scenario several networks with different protocols and architectures are need to be interconnected for efficient communication. To support this feature there exists many networking relay devices that facilitate communication between heterogeneous networks. Network topology also is a significant factor while considering network communications. This paper presents a precise study of various relay devices with its functionalities and its underlying network topologies.

Keywords- Switches, Gateways, Firewalls, LANS, Network Topology

I. INTRODUCTION

All but the most basic of networks require devices to provide connectivity and functionality.[1] Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and requirements for a Networking candidate. For a LAN to be able to access the backbone network, special devices are required. Using the OSI seven-layer reference model as the basis for comparison, networks can be interlinked at various layers. The layer at which networks are linked will depend on the type or types of networks that need to be connected. The various devices used to link LAN[7][8] segments operate at different layers of the OSI model. Each of the relay devices provides a different type of connectivity, performing different functions. Therefore, most networks will have more than one type of relay device in use. Relay devices support one of two general internal architectures, depending on the type of connectivity they are designed to provide. A local relay device is designed to connect two LANs directly. A remote relay device crosses at least one intermediate network. The implication is that remote relay devices use some form of routing and some conversion process to enable distant LANs to communicate with each other. Here are the complete description of the most widely used relay networking
devices in detail.In addition to this are given a detailed analysis of various networking topologies .

II. NETWORK DEVICES[3][4]

REPEATERS: There are many types of media, and each one has advantages and disadvantages. One of the disadvantages of the type of cable that we primarily use (CAT5 UTP) is cable length. The maximum length for UTP cable in a network is 100 meters (approximately 333 feet). If we need to extend our network beyond that limit, we must add a device to our network. This device is called a repeater. The term repeater comes from the early days of visual communication, when a man situated on a hill would repeat the signal he had just received from the person on the hill to his left, in order to communicate the signal to the person on the hill to his right. It also comes from telegraph, telephone, microwave, and optical communications, all of which use repeaters to strengthen their signals over long distances, or else the signals will eventually fade or die out. The purpose of a repeater is regenerate and retime network signals at the bit level to allow them to travel a longer distance on the media. Repeaters are classified as Layer 1 devices in the OSI model, because they act only on the bit level and look at no other information. As signals travel along a network cable (or any other medium of transmission), they degrade and become distorted in a process that is called attenuation. If a cable is long enough, the attenuation will finally make a signal unrecognizable by the receiver. A Repeater enables signals to travel longer distances over a network. Repeaters work at the OSI's Physical layer. A repeater regenerates the received signals and then retransmits the regenerated (or conditioned) signals on other segments. To pass data through the repeater in a usable fashion from one segment to the next, the packets and the Logical Link Control (LLC) protocols must be the same on the each segment. This means that a repeater will not enable communication, for example, between an 802.3 segment (Ethernet) and an 802.5 segment (Token Ring). That is, they cannot translate an Ethernet packet into a Token Ring packet. In other words, repeaters do not translate anything.

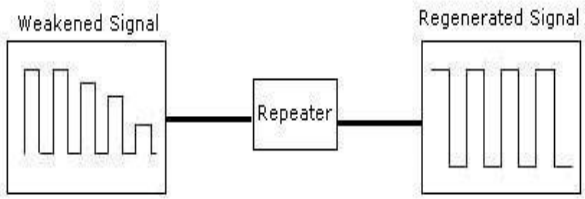

Fig 1 A Repeater

HUBS:

Fig 2 A Hub

At the bottom of the networking food chain, so to speak, are hubs. Hubs are used in networks that use twisted-pair cabling to connect devices. Hubs can also be joined together to create larger networks. Hubs are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data package is destined for the device. This makes them inefficient devices and can create a performance bottleneck on busy networks. In its most basic form, a hub does nothing except provide a pathway for the electrical signals to travel along. Such a device is called a passive hub. Far more common nowadays is an active hub, which, as well as providing a path for the data signals, regenerates the signal before it forwards it to all of the connected devices. A hub does not perform any processing on the data that it forwards, nor does it perform any error checking. Hubs come in a variety of shapes and sizes. Small hubs with five or eight connection ports are commonly referred to as workgroup hubs. Others can accommodate larger numbers of devices (normally up to 32). These are referred to as high-density devices. Because hubs don't perform any processing, they do little except enable communication between connected devices. For today's high-demand network applications, something with a little more intelligence is required. That's where switches come in. On 10BaseT and 100BaseTX Ethernet networks larger than two computers, each computer or printer (or other networked device) is connected to a hub. The hub is a small box that gathers the signals from each individual device, optionally amplifies each signal, and then sends the signal out to all other connected devices. Amplification helps to ensure that devices on the network receive reliable information. You can think of an Ethernet hub like the hub of a wheel, at the center of the spokes that connect each individual computer or printer. Hubs are also called concentrators or repeaters. Hubs come in various sizes, the most common being 12-port or 24- port (meaning they can connect to 12 or 24 computers/printers/hubs). A simple 10BaseT or 100BaseTX Ethernet network may consist of a few dozen individual computers, printers, or servers connected to a single hub. In a more complex network, many hubs can be interconnected. All of the clients, servers, and peripherals connected to a hub (or to a set of interconnected hubs) share the bandwidth (data delivery capacity) of your network. Technically, they form a single collision domain—an area of an Ethernet network in which data sent to or from a device may potentially collide with the data from other devices. (In Chapter 4, we discussed Ethernet collisions and suggested that a 10% collision rate as reported by your network operating system is normal.) As you add more clients, servers, and peripherals to an Ethernet network, the number of collisions increases and the performance of your network degrades. You can improve performance by isolating network traffic into many smaller collision domains.

Unfortunately, hubs cannot divide a network in this fashion; they simply repeat every signal all to all connected devices. Instead, to divide networks into multiple collision domains you can deploy switches, bridges, or routers. Each switch port, bridge port, or router port forms a new collision domain. That is, devices connected to a single port share the network bandwidth, but they are protected from the interfering signals of devices on other ports. When you purchase a hub, you may wish to keep the following information in mind:

1. Like network interfaces, your hubs must be compatible with your physical and data link level protocols.
2. If you purchase a multiprotocol hub, then make sure that it automatically senses which protocol is being used on each port. Autosensing hubs ensure that you can connect any part of the network to any hub port.
3. Make sure that your hub includes an AUI port (connector). (AUI is an abbreviation for attachment unit interface.) AUI ports are intended to connect with a kind of cabling called thick coaxial cable (like that used for cable TV).
4. Make sure that your hub includes a crossover port. Unlike regular hub ports, which connect hubs to clients, servers, or peripherals, a crossover port connects one hub to another.
5. Purchase hubs from a known manufacturer whose support you trust. Make sure the manufacturer provides a competitive warranty.

SWITCHES:

Fig 3 A 40 port Switch

Like a hub, an Ethernet switch is a device that gathers the signals from devices that are connected to it, and then regenerates a new copy of each signal. Switches on the other hand are more advanced. Instead of broadcasting the frames everywhere, a switch actually checks for the destination MAC address and forward it to the relevant port to reach that computer only. This way, switches reduce traffic and divide the collision domain into segments, this is very sufficient for busy LANs and it also protects frames from being sniffed by other computers sharing the same segment. They build a table of which MAC address belongs to which segment. If a destination MAC address is not in the table it forwards to all segments except the source segment. If the destination is same as the source, frame is discarded. Switches have built-in hardware chips solely designed to perform switching capabilities, therefore they are fast and come with many ports. Sometimes they are referred to as intelligent bridges or multiport bridges.
Different speed levels are supported. They can be 10 Mb/s, 100 Mb/s, 1 Gb/s or more. 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.

Switches, however, are more powerful than hubs and can substantially increase your network performance. In order to understand how they perform this magic, it is necessary to understand first how they work. Most common switches operate by learning the MAC addresses of all connected clients, servers, and peripherals, and associating each address with one of its ports. When a switch receives an incoming signal, it creates a temporary circuit between the sender and receiver. The temporary circuit provides two important benefits. First, the circuit allows the sender and receiver momentarily to exchange information without intrusion from other devices on the network. Second, the circuit ensures that information travels directly between the communicating computers. Like all network equipment, switches benefit your network only if they are deployed in the proper manner. If your network is congested and if traffic pools in certain areas, then you can improve network performance by replacing hubs with switches, or by connecting hubs to switches in a hierarchical manner. For the pools of heavy traffic, switches increase bandwidth while segregating the traffic from the rest of the network. However, if your network is not congested or if your traffic patterns do not create pools of congestion, then switches may actually cause your network performance to deteriorate. This performance degradation occurs because switches examine the information inside each signal on your network (to determine the addresses of the sender and receiver) and therefore process network information more slowly than hubs. Because switches depend upon MAC addresses, we say in the parlance of the OSI model that they are level 2 devices (level 2 manages the structure and MAC addresses within network signals). Like a hub, a switch is a device that connects individual devices on an Ethernet network so that they can communicate with one another. But a switch also has an additional capability; it momentarily connects the sending and receiving devices so that they can use the entire bandwidth of the network without interference. If you use switches properly, they can improve the performance of your network by reducing network interference. Switches have two benefits: (1) they provide each pair of communicating devices with a fast connection; and (2) they segregate the communication so that it does not enter other portions of the network.

These benefits are particularly useful if your network is congested and traffic pools in particular areas. However, if your network is not congested or if your traffic patterns do not create pools of local traffic, then switches may cause your network performance to deteriorate. This performance degradation occurs because switches examine the information inside each signal on your network (to determine the addresses of the sender and receiver) and therefore process network information more slowly than hubs (which do not examine the signal contents). Most switches operate by examining incoming or outgoing signals for information at OSI level 2, the data link level. When you purchase and install a switch, you should review and apply the following criteria:

1. If you purchase a switch that accommodates more than one protocol, then make sure that it automatically senses which protocol is being used on each port.
2. Purchase switches from a known manufacturer whose support you trust.
3. Install your switches in a room that is cool and free of dust, if possible.

By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways. First, by creating a direct path between two devices and controlling their communication, it can greatly reduce the number of collisions on the network. In addition, the lack of collisions enables switches tocommunicate with devices in full-duplex mode. In a full-duplex configuration, devices can send and receive data from the switch at the same time. Irrespective of whether a connection is at full or half duplex, the method of switching dictates how the switch deals with the data it receives. The following is a brief explanation of each method:[2]

Cut-through In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is very fast, but creates the possibility of errors being propagated through the network, as there is no error checking.

Store-and-forward Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.

FragmentFree To take advantage of the error checking of store-andforward switching, but still offer performance levels nearing that of cutthrough switching, FragmentFree switching can be used. In a FragmentFree-switching environment, enough of the packet is read so that the switch can determine whether the packet has been involved in a collision. As soon as the collision status has been determined, the packet is forwarded.

BRIDGES: A bridge is a device that connects two or more local area networks, or two or more segments of the same network. For example, suppose that your network includes both 10BaseT Ethernet and LocalTalk connections. You can use a bridge to connect these two networks so that they can share information with each other. In addition to connecting networks, bridges perform an additional, important function. possible for bridges to connect networks with different physical and data link level protocols. For example, you can use a bridge to connect a LocalTalk

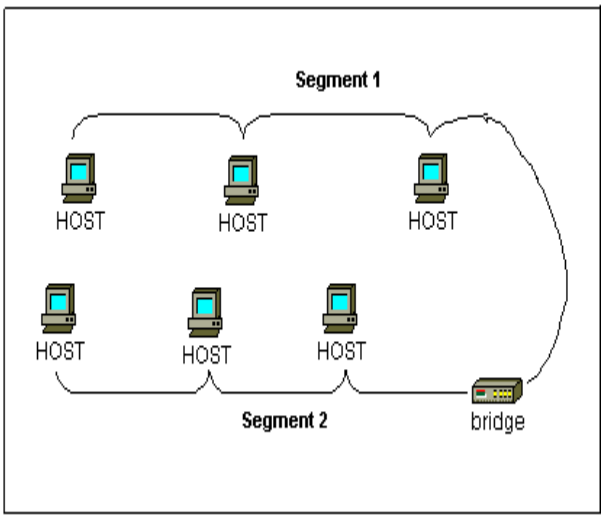

Fig 4 A Bridge connecting two networks

network to a TokenRing network. Traditional bridges connect a single workgroup to another workgroup. More recently, however, manufacturers have produced multiport bridges. Multiport bridges allow network managers to connect more than two network segments to each other. Bridges generally inspect data link level information within a network signal—

information like the Ethernet or LocalTalk (MAC) destination address. They do not attend to network routing or transport protocol information such as that carried within the TCP/IP, IPX/SPX, or AppleTalk portions of the signal. However, bridges can be fitted with custom filters that enable them to read this information—including network routing or transport source address, packet size, or type of protocol—and reject or forward information based on it. A bridge connects two or more networks, or segments of the same network. These networks may use different physical and data link protocols. Bridges filter network traffic. They examine each set of data, transmitting only appropriate data to each connected segment. (Hubs, by contrast, broadcast all information to each connected computer, whether or not that computer is the intended recipient.) In this manner, bridges help reduce overall network traffic. Bridges are relatively simple and efficient traffic regulators. However, in most networks they have been replaced by their less expensive or more powerful cousins—hubs, switches, and routers. There are two issues that you must consider when using bridges. The first is the bridge placement, and the other is the elimination of bridging loops:

Placement Bridges should be positioned in the network using the 80/20 rule. This rule dictates that 80% of the data should be local and that the other 20% should be destined for devices on the other side of the bridge.

Bridging loops Bridging loops can occur when more than one bridge is implemented on the network. In this scenario, the bridges can confuse each other by leading one another to believe that a device is located on a certain segment when it is not. To combat the bridging loop problem, the IEEE 802.1d Spanning Tree protocol enables bridge interfaces to be assigned a value that is then used to control the bridge-learning process.

Types of Bridges

Three types of bridges are used in networks:

Transparent bridge Derives its name from the fact that the devices on the network are unaware of its existence. A transparent bridge does nothing except block or forward data based on the MAC address.

Source route bridge Used in Token Ring networks. The source route bridge derives its name from the fact that the entire path that the packet is to take through the network is embedded within the packet.

Translational bridge Used to convert one networking data format to another; for example, from Token Ring to Ethernet and vice versa.

ROUTERS: In a common configuration, routers are used to create larger networks by joining two network segments. Like bridges, routers are devices whose primary purpose is to connect two or more networks and to filter network signals so that only desired information travels between them. For example, routers are often used to regulate the flow of information between

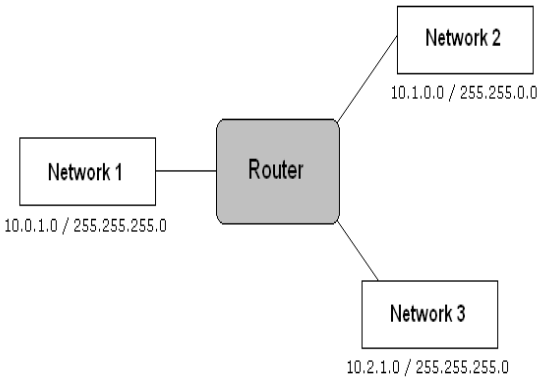

Fig 5 A Router connecting three different networks

information than bridges, and they therefore can regulate network traffic more precisely. They also have another important capability: they are aware of many possible paths across the network and can choose the best one for each data packet to travel. Routers operate primarily by examining incoming data for its network routing and transport information—for example, information carried within the TCP/IP, IPX/SPX, or AppleTalk portions of the network signal. This information includes the source and destination network routing addresses. Based on complex, internal tables of network information that it compiles, a router then determines whether or not it knows how to forward the data packet towards its destination. If the router has been configured with sufficient information to know which of its ports is en route to the destination, it transmits the packet. If the router has not been so configured, it typically drops the packet. Dropping unknown packets provides an

important service to your network by eliminating restricted, wayward, or damaged information from your network. Bridges lack this capability (they forward unknown packets to all ports), and the misinformation they forward often creates extra network traffic. Routers can be programmed to prevent information from being sent to or received from certain networks or computers based on all or part of their network routing addresses. If you have sensitive student records on a server, for example, you can use a router to filter packets headed for the server so that only authorized personnel—for example, personnel whose network addresses match a specified list—can connect to it. However, routers are much more powerful than bridges. Routers can filter traffic so that only authorized personnel can enter restricted areas. They can permit or deny network communications with a particular Web site. They can recommend the best route for information to travel. As network traffic changes during the day, routers can redirect information to take less congested routes. However, routers are much more powerful than bridges. Routers can filter traffic so that only authorized personnel can enter restricted areas. They can permit or deny network communications with a particular Web site. They can recommend the best route for information to travel. As network traffic changes during the day, routers can redirect information to take less congested routes. Routers quickly become critical components of your network. If they fail, your network services will be significantly impaired. As part of your network plan, you should consider how you might deal with the failure of key routers on your network. Many sites include redundant connections additional routers and network cable connections configured to take over if one router or connection fails. Most routers operate by examining incoming or outgoing signals for information at OSI level 3, the network addressing level. A router derives its name from the fact that it can route data it receives from one network onto another. When a router receives a packet of data, it reads the header of the packet to determine the destination address. Once it has determined the address, it looks in its routing table to determine whether it knows how to reach the destination and, if it does, it forwards the packet to the next hop on the route. The next hop might be the final destination, or it might be another router. Routers do not look at the destination node address; they only look at the network address. Routers will only pass the information if the network address is known. This ability to control the data passing through the router reduces the amount of traffic between networks and allows routers to use these links more efficiently than bridge[5]

GATEWAYS: Gateways make communication possible between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other's environment data. A gateway repackages information to match the requirements of the destination system. Gateways can change the format of a message so that it will conform to the application program at the receiving end of the transfer. A gateway links two systems that do not use the same:

- Communication protocols
- Data formatting structures
- Languages
- Architecture

For example, electronic mail gateways, such as X.400 gateway, receive messages in one format, and then translate it, and forward in X.400 format used by the receiver, and vice versa. Any device that translates one data format to another is called a gateway. Some examples of gateways include a router that translates data from one network protocol to another, a bridge that converts between two networking systems, and a software application that converts between two dissimilar formats. The key point about a gateway is that only the data format is translated, not the data itself. In many cases, the gateway functionality is incorporated into another device. Gateways operate at the network layer and above, but most of them at the application layer.

FIERWALLS:

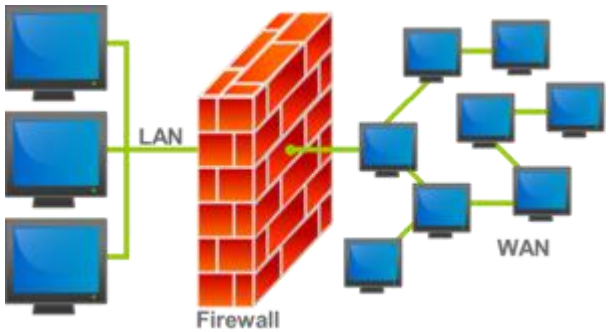

Fig 6 Position of a Firewall

A firewall is a device that prevents unauthorized electronic access to your network. The term firewall is generic, and includes many different kinds of protective hardware and software devices. Routers, discussed in the previous section, comprise one kind of firewall. A different kind of firewall might be created by installing software on a network server that is dedicated to the task of monitoring network activity. Yet another firewall consists of a standalone box (that is, a computer with no keyboard or monitor) which watches all the traffic on your network. All firewalls have one thing in common: they guard your network, examining information inside every network packet. Based on a list of restrictions which you provide, the firewall allows or disables each packet from traveling any further. Firewalls can be divided into three major categories: packet-screening firewalls, proxy servers, and stateful inspection proxies. Packet-screening firewalls. Packet-screening firewalls operate by examining incoming or outgoing signals for information at OSI level 3, the network addressing level. For example, you can configure your firewall to examine incoming packets for their Internet (IP) source address (the place where the information originated); you can deny access to your network if the packet comes from a network(s) that you have identified as unauthorized. Alternatively, your firewall can examine information leaving your network for its Internet (IP) destination address (where theinformation is being sent); you can deny access if users on your network attempt to connect to unauthorized sites. Besides source and destination addresses, firewalls can filter information based on the type of protocol used, the port number to which it is addressed (each Internet service such as electronic mail, TELNET, or FTP has a unique number, called its port number, which it uses to identify itself on the network), or content type (for example, JavaScript, Java, and so forth). You can use firewalls to control the information that enters your local area network from the Internet, leaves your site for the Internet, or travels from one part of your site to another. Packet-screening firewalls have traditionally been implemented as add-on services within routers. On the positive side, they are among the fastest firewalls (because they examine a more restricted set of information than other firewalls). On the negative side, they are limited to examining network address and related information; they cannot implement complex security rules (for example, allowing the use of Web browsers but restricting the use of video). Finally, packetscreening firewalls leave you vulnerable to malicious information in portions of the packet that they don't examine—the data area beyond the packet's network address information.Proxy servers. Proxy servers (also called application-level gateways) operate by examining incoming or outgoing packets not only for their source or destination addresses but also for information carried within the data area (as opposed to the address area) of each network packet. The data area contains information written by the application program that created the packet— for example, your Web browser, FTP, or TELNET program. Because the proxy server knows how to examine this application-specific portion of the packet, you can permit or restrict the behavior of individual programs. For example, you can configure your proxy server to allow Web browsing but to deny requests from FTP programs such as Fetch or WS_FTP. Alternatively, you can configure your proxy to permit FTP requests, but only if they read (not write) information. As a third example, proxies can deny Web browsers access to unauthorized Web sites. You must configure a separate (software) proxy servers for each application you wish to screen. For example, your proxy server (hardware) will include multiple proxy servers (multiple software programs) if you want to screen information based on the common Internet applications—Web browsers, FTP, TELNET, and electronic mail. You should note that not all application programs can be proxied. For example, your accounting system may have no available proxy. For application programs without proxies, you must protect the program through packet-screening firewalls or other network services (passwords, for example). Besides filtering information, proxy servers perform several other useful tasks. First, proxies hide the Internet (IP) addresses used by your organization so that intruders with malicious intent cannot easily determine the addresses to attack. Second, proxies cache information. That is, if the proxy grants permission to retrieve an Internet resource such as a Web page, it keeps a local copy. The next time that someone on your network wants to browse the same page, the proxy server checks its local cache. If the page is there, the proxy server checks with the originating Web server to see if the page has been updated. If not, the proxy delivers its local copy of the Web page to the user. This sequence of events is much faster than retrieving the entire Web page from the original server. In classroom situations where several computers simultaneously browse the same Web pages, this performance improvement can be substantial. The specialized server that runs the proxy software is made as secure as possible by stripping it ofall but essential services. For example, regular network servers may offer login, file- and printer sharing capabilities, but secure proxy servers (and, for that matter, secure firewall servers) allow none of these services; all unnecessary or risk-prone services are turned off. Additionally, operating system updates, which often contain security fixes, are applied religiously. Stripping the proxy server (or firewall server) of extraneous services and keeping its operating system updated makes it more difficult for unauthorized users to gain access. ***Stateful inspection proxies.*** Stateful

inspection proxies examine the data within network packets to ensure that they are a legitimate part of a sensible, ongoing conversation between computers rather than a random insertion of (possibly malicious) material. Stateful inspection proxies fall midway between packet-filters and proxy servers in terms of security, but they offer relative ease of use and high performance. Like proxy servers, stateful inspection servers hide your internal Internet (IP) addresses from would-be intruders. sharing capabilities, but secure proxy servers (and, for that matter, secure firewall servers) allow none of these services; all unnecessary or risk-prone services are turned off. Additionally, operating system updates, which often contain security fixes, are applied religiously. Stripping the proxy server (or firewall server) of extraneous services and keeping its operating system updated makes it more difficult for unauthorized users to gain access. As mentioned, firewalls can be implemented through software or through a dedicated hardware device. Organizations implement software firewalls through network operating systems (NOS) such as Linux/UNIX, Windows servers, and Mac OS servers. The firewall is configured on the server to allow or permit certain types of network traffic. In small offices and for regular home use, a firewall is commonly installed on the local system and configured to control traffic. Many third-party firewalls are available. Hardware firewalls are used in networks of all sizes today. Hardware firewalls are often dedicated network devices that can be implemented with very little configuration and protect all systems behind the firewall from outside sources. Hardware firewalls are readily available and often combined with other devices today. For example, many broadband routers and wireless access points have firewall functionality built in.

III. NETWORK TOPOLOGIES[6]

TOPOLOGY – defines the structure of the network. There are two parts to the topology definition: the physical topology which is the actual layout of the wire (media) and the logical topology which defines how the media is accessed by the hosts. It refers also to how computers are being connected with each other. Network topologies may be physical or logical. Physical topology refers to the physical design of a network including the devices, location and cable installation. Logical topology refers to how data is actually transferred in a network as opposed to its physical design. In general physical topology relates to a core network whereas logical topology relates to basic network. Topology can be understood as the shape or structure of a network. This shape does not necessarily correspond to the actual physical design of the devices on the computer network. The computers on a home network can be arranged in a circle but it does not necessarily mean that it represents a ring topology. Any particular network topology is determined only by the graphical mapping of the configuration of physical and/or logical connections between nodes. The study of network topology uses graph theory. Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ in two networks and yet their topologies may be identical.

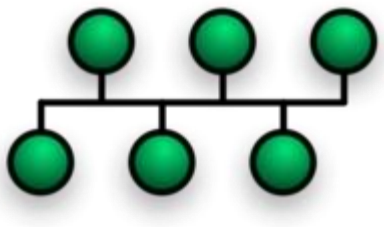

Fig 7 A Bus network

BUS TOPOLOGY uses a single backbone segment (length of cable) that all the hosts connect to directly. The idea is that is just like riding a bus. It has only one driver and many passengers who are riding. Bus networks (not to be confused with the system bus of a computer) use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. Ethernet bus topologies are relatively easy to install and don't require

much cabling compared to the alternatives. 10Base-2 ("ThinNet") and 10Base-5 ("ThickNet") both were popular Ethernet cabling options many years ago for bus topologies. However, bus networks work best with a limited number of devices. If more than a few dozen computers are added to a network bus, performance problems will likely result. In addition, if the backbone cable fails, the entire network effectively becomes unusable

Linear bus The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints. all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

RING TOPOLOGY connects one host to the next and the last host to the first. This creates a physical ring of cable. In a ring network, every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). A failure in any cable or device breaks the loop and can take down the entire network. To implement a ring network, one typically uses FDDI, SONET, or Token Ring technology. Ring topologies are found in some office buildings or school campuses.

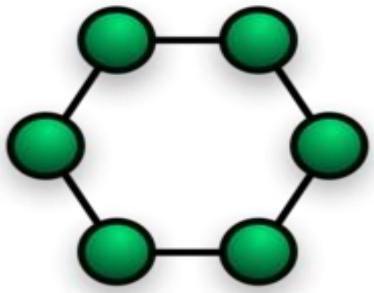

Fig 8 Ring topology

STAR TOPOLGY connects all cables to a central point of concentration. This point is usually a hub or switch. It has a focal point where all the resources are there. Many home networks use the star topology. A star network features a central connection point called a "hub node" that may be a network hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet. Compared to the bus topology, a star network generally requires more cable, but a failure in any star network cable will only take down one computer's network access and not the entire LAN.

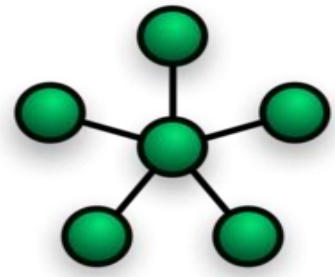

Fig 9 Star topology

Extended star A type of network topology in which a network that is based upon the physical star topology has one or more repeaters between the central node (the 'hub' of the star) and the peripheral or 'spoke' nodes, the repeaters being used to extend the maximum transmission distance of the point-to-point links between the central node and the peripheral nodes beyond that which is supported by the transmitter power of the central node or beyond that which is supported by the standard upon which the physical layer of the physical star network is based.

Distributed Star A type of network topology that is composed of individual networks that are based upon the physical star topology connected in a linear fashion – i.e., 'daisy-chained' – with no central or top level connection point (e.g., two or more 'stacked' hubs, along with their associated star connected nodes or 'spokes').

HYBRID TOPOLOGY Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network connected to a tree network is still a tree network topology. A hybrid topology is always produced when two different basic network topologies are connected. Two common examples for Hybrid network are: star ring network and star bus network

A Star ring network consists of two or more star topologies connected using a multistation access unit (MAU) as a centralized hub.

A Star Bus network consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network's backbone).

While grid and torus networks have found popularity in **high-performance computing** applications, some systems have used **genetic algorithms** to design custom networks that have the fewest possible hops in between different nodes. Some of the resulting layouts are nearly incomprehensible, although they function quite well A Snowflake topology is really a "Star of Stars" network, so it exhibits characteristics of a hybrid network topology but is not composed of two different basic network topologies being connected. Definition : Hybrid topology is a combination of Bus,Star and ring topology.

MESH TOPOLOGY is used when there can be absolutely no break in communications. So as you can see in the graphic, each host has its connections to all other hosts. This also reflects the design of the internet which has multiple paths to any one location. Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that even in a ring, although two cable paths exist, messages can only travel in one direction.) Some WANs, most notably the Internet, employ mesh routing. A mesh network in which every device connects to every other is called a full mesh. As shown in the illustration below, partial mesh networks also exist in which some devices connect only indirectly to others.

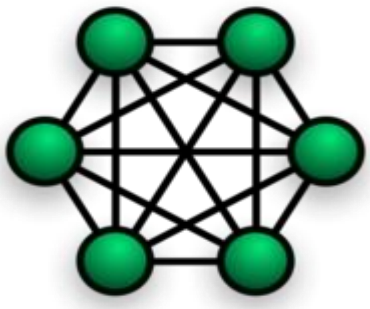

Fig 10 Mesh topology

TREE TOPOLOGY Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the root of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.

IV. CONCLUSION

We have been introduced so far are the main traditional devices used to build networks, understanding how they work helps to understand the logic behind networks designing, however, now that technology advance quickly, it is possible to find new products in the market combining two or more of these devices into one. Thus this paper presents a precise survey of network devices and its functionalities along with different network topologies that form the base for ant network architecture.

REFERENCES

[1] Kraemer, R., "Bluetooth Based Wireless Internet Applications for Indoor Hot Spots: Experience of a Successful Experiment During CeBIT 2001," Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 41 , Issue 3, February 2003, pp. 303 – 312.
[2] Introduction to data communication and networking, Behrouz Forouzan, TMH.

[3] O'Hara, B. and Petrick, A., IEEE 802.11 Handbook: A Designer's Companion, Standards Information Network, IEEE Press, New York, New York, 1999.

[4] "IEEE 802.11a White Paper." http://www.vocal.com/data_sheets/ieee802.11a.html

[5] James F. Kurose, Keith W. Ross, 2004, Computer Networking – A top down approach featuring the Internet

[6] Lowekamp, B., O'Hallaron, D., and Gross, T. 2001. Topology discovery for large ethernet networks. In Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications (San Diego, California, United States). SIGCOMM '01. ACM Press, New York, NY, 237-248.

[7] IEEE Std 802.1D TM 2004 - IEEE Standard for Local and Metropolitan Area Networks: Media Access Control Bridges

[8] Bruce Lowekamp, 2000, Discovery and Application of Network Information

