|  |
| --- |
| Newtown Department |
| Network Principles |
| Newtown Fire Department |
|  |
| **K.P.I. Shenesh Perera: IDM** |
| **9/11/2018** |

Contents

[Introduction 2](#_Toc532303458)

[Physical & Virtual addressing 3](#_Toc532303459)

[Role of a physical address, functionality and limitations 3](#_Toc532303460)

[Role of a virtual address, functionality and limitations 3](#_Toc532303461)

[Relationship & differences between IP and MAC addresses 3](#_Toc532303462)

[Physical and logical topologies 4](#_Toc532303463)

[Physical Topologies 4](#_Toc532303464)

[1. Bus Topology 4](#_Toc532303465)

[2. Star Topology 4](#_Toc532303466)

[3. Hybrid Topology 4](#_Toc532303467)

[Logical topologies 5](#_Toc532303468)

[Virtual Local Area Network 5](#_Toc532303469)

[Network Models 6](#_Toc532303470)

# Introduction

This report is a comprehensive and structured gathering of information and analytics revolving the new fire department in New town. It will not include any direct implications on the design or the structure of the network, however most of the techniques, standards and procedures used in the network will be explained in simple terms.

# Physical & Virtual addressing

## Role of a physical address, functionality and limitations C:\Users\PC\AppData\Local\Microsoft\Windows\INetCache\Content.Word\mac-addresse-numbers-800x400.jpg

Figure 1.0, porunnuevopais.org, Jason, 01/23/2017

In general IT, a physical address refers to either some memory location, identified as a series of a binary number or a media access control address. However for the scope of this report, a physical address refers to the Media Access Control address (MAC) of a computer which is a unique identification associated with the network adapter (Network Interface Card) that is used to identify a computer in a network.

This address is used both by hardware and software for accessing data. For software, however, there is no direct use of the physical address; instead it uses a virtual address to access memory. A hardware unit inside the computer system known as the Memory Management Unit (MMU) is solely responsible for translating virtual address to physical address and vice versa. A protocol called Address Resolution Protocol (ARP) is responsible for converting these addresses in a network.

## Role of a virtual address, functionality and limitations

A virtual address generally refers to a memory pointer to a particular memory that a operating system has allowed a process to use. However in networking a virtual address generally refers to the IP address, short for the Internet protocol address that the computer system will use to communicate with other members of the network, IP addresses are crucial in a network as when there is a necessity to transfer or send data from one place to another, you need a source and destination address. The IP address is used to define these 2 addresses.

IP addresses achieve many tasks that a computer system just cannot with a MAC address, it allows networks to communicate with other networks, retrieve and send data to and from devices that are not computers etc. One of the biggest achievements of the existence of IP addresses is the Internet.

## Relationship & differences between IP and MAC addresses

|  |  |
| --- | --- |
| Internet Protocol Address | Media Access Control Address |
| * Identifies the connection to a network. * Has 2 versions called IPv4 and IPv6 * IPv4 is 32 bits, IPv4 is a 128 bit address. * An IP address is assigned by the ISP or the network administrator in the network. * RARP can retrieve information about the IP address of a system. * Is unique in a network. * Allows communication between computer systems and networks at high levels. | * Identifies as the physical address of a computer system. * Has only 1 version * It’s a 48 bit hexadecimal address * It is hard-written into the ROM of the NIC by the manufacturer. * ARP can retrieve information about the MAC address of a system. * Is unique in a network. * Allows communication between computer systems at the lower level. |

# Physical and logical topologies

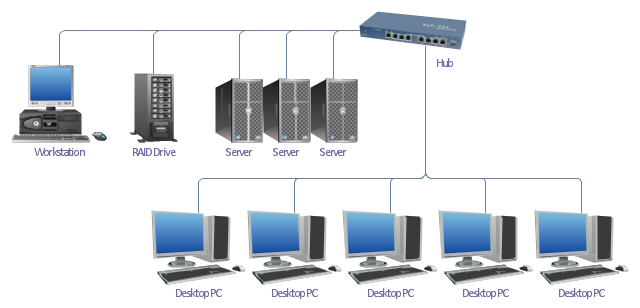
Briefly, the physical topology of a network defines how wires of the network are connected while the logical topology defines how the network behaves and inter-operates. Logical topologies focus mainly on traffic flow, routing domains, roter peering, control points, IP address schemas etc. while the physical topology is concerned with type, length and arrangement of networking cables, how likely they are to be met with interference etc.

# Physical Topologies

There are a plenty of physical topologies but only 3 of the topologies are still technically used in the industry the bus, star and hybrid topologies.

Figure 1.1, conceptdraw.com, David23, 21/09/2016

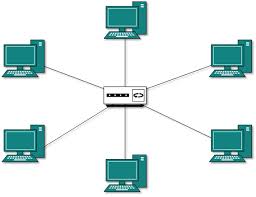
## Bus Topology



Bus topology is a type of network in which every client of the network and network device is connected to a single cable. When the cable stretches straight and has only 2 endpoints, it’s called a linear bus topology. It transmits only in traffic in only one direction. It is very cost effective and requires the least cable length, used in smaller networks and is easy to understand, however it is slower than the ring topology, if the cable fails the whole network becomes usable and the performance of the network decreases with the increase of traffic.

## Star Topology

Figure 1.2, http://spiroprojects.com, Admin on



Within the star topology all computers are connected to a single hub through a cable, this hub is the central node and all the other clients are connected to it. This topology can be used with any type of cable, the hub can act like a repeater for data flow, it’s easy to troubleshoot and setup but the cost of implementing it is high and just like the bus topology if the hub fails the whole network dies.

## Hybrid Topology

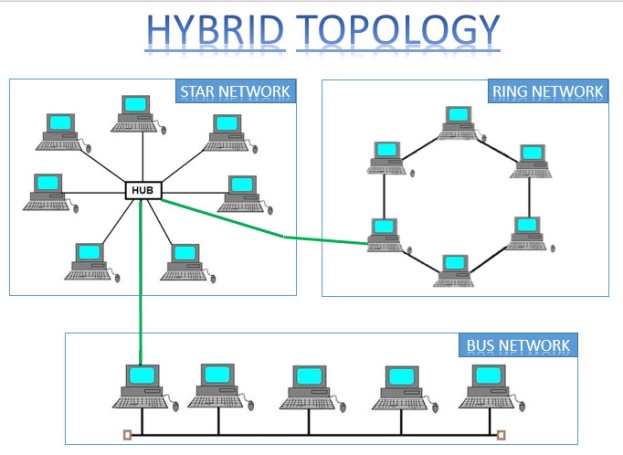
This topology is just the combination of multiple other topologies, if you combine a star and a bus topology together then it becomes a hybrid topology. This type of topology inherits the advantages of all the involved topologies but also inherits their disadvantages; it’s very complex and difficult to troubleshoot.

Figure 1.3, http://swissen.in, Suyash Srivastava, 19/05/2012

With all this said regardless, physical topologies are barely ever seen in the industry in the modern world. As you may now understand they have severe problems and rely on technology that has far become obsolete. Logical topologies do not replace physical topologies but help counter these problems without physical structure making advantage of modern technology.

# Logical topologies

## Virtual Local Area Network

A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution.

A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.

In addition, VLANs are created to provide segmentation and assist in issues like security, network management and scalability. Traffic patterns can also easily be controlled by using VLANs.

|  |  |
| --- | --- |
| Pros | Cons |
| * Allows network administrators to apply additional security to network communication * Makes expansion and relocation of a network or a network device easier * Provides flexibility because administrators are able to configure in a centralized environment while the devices might be located in different geographical locations * Decreases the latency and traffic load on the network and the network devices, offering increased performance | * Higher risk of virus issues because one infected system may spread a virus through the whole network * Equipment limitations exist in very large networks because additional routers might be needed to control the workload * Effective at controlling latency than a WAN, but less efficient than a LAN |

# Network Models

The most known and common network principles known to networking are the OSI model and the TCP/IP model. Below in the table a full comparison of the protocols, networking concepts and solutions have been described.

|  |  |
| --- | --- |
| Open Systems Interconnection Model | Transmission Control Protocol/Internet Protocol Model |
| * It is a theoretical model primarily used for computer systems. * Consists of 7 main layers. * Developed by International Standard Organization. * Usage is pretty low. * Follows a vertical approach * The transport layer in the OSI model guarantees the successful delivery of packets. * The OSI model has separate presentation and session layers. * Transport and network layers are compulsorily connection oriented. * OSI is mostly a guidance tool for learners in the networking field. * The OSI model is vague in terms of including protocols into the model as at times 1 protocol functions in multiple layers. * Protocols are easily changed in the OSI model as technology advances. * The OSI model defines interfaces, services and protocols used clearly and are also protocol independent. * The physical layer that performs media, signal and binary transmission uses 802.11, DSL, SDH, V.34, RJ45 and RS-232 protocols. * The data link layer that performs physical addressing uses Ethernet, 802.11, MAC/LLC, HDP, Fiber Channel, Frame relay, HDLC, PPP, Q.921 and Token ring protocols. * The network layer that performs path determination and logical addressing uses IP, ARP, IPsec, ICMP, IGMP and OSPF protocols. * The transport layer that performs end to end connections and reliability uses TCP, UDP, SCTP, SSL and TLS protocols. * The session layer that performs inter-host communication uses TCP, SIP, RTP and RPC-named pipes. * The presentation layer that performs data representation and encryption uses HTML, DOC, JPEG, MP3, AVI and sockets. * The application layer that performs network process to application procedures uses DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet and FTP protocols. | * It is a client to server based model for transmission of data over the internet. * Consists of 4 main layers. * Developed by Department of defense. * Usage and implementation is frequent. * Follows a horizontal approach * The TCP/IP model there is no guarantee that packets will be delivered successfully but it is more reliable than OSI. * TCP/IP model does not have such separate layers. * Transport layer and network layers are both connection & connection less oriented. * The TCP/IP model could be called the implementation of the OSI model. * The TCP/IP model does not have such a problem. * Replacing or introducing a new protocol is not easy. * TCP/IP is protocol dependent and there is no clear differentiation between interfaces and protocols. * Have a combined layer for data link and physical called network access layer that uses Ethernet, token ring, ATM or frame relay protocols. * Network layer is called internet layer, and performs the function uses ARP, IP, IGMP and ICMP protocols. * Transport layer uses TCP and UDP protocols. * Application, presentation and session layer are combined and are called the application layer, and uses HTTP, SMTP, Telnet, FTP, DNS, RIP, SNMP etc. protocols. |

From the above as you notice, the OSI model is conceptual and therefore cannot be implemented in the real world. Therefore I wish to implement the TCP/IP model while basing my network per the OSI model’s standards and layered architecture.