COMSATS University Islamabad Attock Campus

Department Of Electrical And Computer Engineering

June 2022

Network Configuration Using Classless IP Subnetting And RIPv2 Protocol

Data Communication And Computer Networks

Submitted by:

Ammar (FA19-BCE-001)

Shayan Shahid (FA19-BCE-012)

Submitted To

Dr. Shujaat Tanoli

Engr. Ayesha Sadiq

ABSTRACT

Keywords - Data Communication, Routing Protocols, Classless IP Sub-netting

In the age of Internet where everyone loves to work with their computers and smart phones it is impossible to think any work without networking. With advancement of technology use of computer networking is increasing rapidly. In general if we will see, we can feel also how important networking is that may be our day to day social networking or that may be this technical computer networking everything are in a process to make human life better by giving another way of living life by networking.

In small networks, it is easy to overlook minor problems, but in a large network it becomes difficult to identify and face those challenges since it may bring entire network infrastructure down with it. Minor and common computer network problems can be easily identified and dealt with, but there are certain problems that can be tricky to handle, Those computer network challenges. But before going into networking challenges, Let's first give a look this computer network and after that we can analyze challenges involved in computer networks that we face commonly in our day to day life.

We proposed a network with classless IP sub-netting classless addressing decoupled the relationship between network size and IP address and allowed for balanced use across what used to be the Class A, B, and C ranges. Far less wasted addresses. More efficient routing. VLSM and sub-netting make route aggregation and classless routing protocols possible.

Computer Network is basis of communication in Information Technology (IT). It refers to group of computers linked to each other that enables one computer to communicate with another computer to share information and resources. These devices connected to network use a set of network protocols over digital interconnections for purpose of sharing resources located on or provided by network nodes. The interconnections between nodes are formed based on a variety of network topologies.

Contents

List of Figures

Chapter 1

INTRODUCTION

1.1 Objectives

The main goal of the computer network is Resource Sharing. It is to create all the programs, data and hardware accessible to anyone on the network without considering the resource's physical area and the client. So we're creating a network that'll be combination of 3 companies that are interconnected to each other with the following objectives.

- To understand and configure the network using Classless sub-netting that is is to improve the usage of provided IP.
- To understand the concepts of routing and creating the route for data traveling between different networks that are connected by router though RIPv2 Protocol.
- To establish the complete network using provided constrains and connecting the different networks with each other.

1.2 Overview

In this section we'll focus on the basic concepts related to project and discuss the problem statement along side constrains.

1.2.1 Network

In information technology, a network is defined as the connection of at least two computer systems, either by a cable or a wireless connection. The simplest network is a combination of two computers connected by a cable. This type of network is called a peer-to-peer network. There is no hierarchy in this network; both participants have equal privileges. Each computer has access to the data of the other device and can share resources such as disk space, applications or peripheral devices (printers, etc.). Today's networks tend to be a bit more complex and don't just consist of two computers. Systems with more than ten participants usually use client-server networks. In these networks, a central computer (server) provides resources to the other participants in the network (clients).

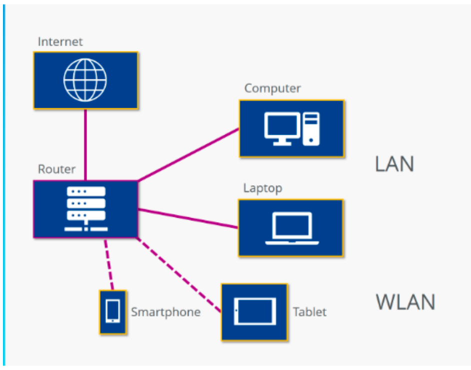


Figure 1.1: Simple Network

1.2.2 Layers: OSI And TCP/IP

The OSI Model is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. The Open System Interconnection (OSI Model) also defines a logical network and effectively describes computer packet transfer by using various layers of protocols.

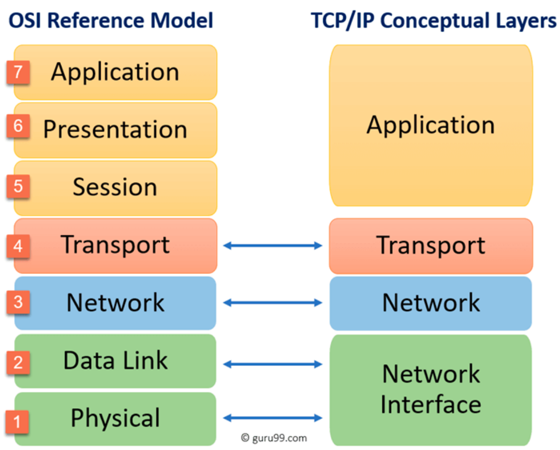


Figure 1.2: TCP/IP Vs OSI Layer Model

TCP/IP helps you to determine how a specific computer should be connected to the internet and how you can transmit data between them. It helps you to create a virtual network when multiple computer networks are connected together. TCP/IP stands for Transmission Control Protocol/ Internet Protocol. It is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

KEY DIFFERENCE

- OSI has 7 layers whereas TCP/IP has 4 layers.
- 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 to determine how a specific computer should be connected to the internet and how you can be transmitted between them.
- OSI header is 5 bytes whereas TCP/IP header size is 20 bytes.
- OSI refers to Open Systems Interconnection whereas TCP/IP refers to Transmission Control Protocol.
- OSI follows a vertical approach whereas TCP/IP follows a horizontal approach.
- OSI model, the 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 to standardize router, switch, motherboard, and other hardware whereas TCP/IP helps you to establish a connection between different types of computers.

1.2.3 Topology

Topology is derived from two Greek words topo and logy, where topo means 'place' and logy means 'study'. In computer networks, a topology is used to explain how a network is physically connected and the logical flow of information in the network. A topology mainly describes how devices are connected and interact with each other using communication links.

In computer networks, there are mainly two types of topologies, they are:

Physical Topology: A physical topology describes the way in which the computers or nodes are connected with each other in a computer network. It is the arrangement of various elements(link, nodes, etc.), including the device location and code installation of a computer network. In other words, we can say that it is the physical layout of nodes, workstations, and cables in the network.

Logical Topology: A logical topology describes the way, data flow from one computer to another. It is bound to a network protocol and defines how data is moved throughout the network and which path it takes. In other words, it is the way in which the devices communicate internally. Network topology defines the layout, virtual shape, or structure of the network, not only physically but also logically. A network can have one physical topology and multiple logical topologies at the same time.

1.2.4 Protocols

Network protocols ensure smooth communication between the different components in a network. They control data exchange and determine how communication is established and terminated as well as which data is transmitted. There are usually multiple network protocols that each perform a specific subtask and are hierarchically organized into layers.

Internet Protocol (IP) is a connection free protocol that is an integral part of the Internet protocol suite (a collection of around 500 network protocols) and is responsible for the addressing and fragmentation of data packets in digital networks. Together with the transport layer TCP (Transmission Control Protocol), IP makes up the basis of the internet. To be able to send a packet from sender to addressee, the Internet Protocol creates a packet structure which summarizes the sent information. So, the protocol determines how information about the source and destination of the data is described and separates this information from the informative data in the IP header. This kind of packet format is also known as an IP-Datagram.

In 1974 the Institute of Electrical and Electronics Engineers (IEEE) published a research paper by the American computer scientists Robert Kahn and Vint Cerf, who described a protocol model for a mutual packet network connection based on the internet predecessor ARPANET. In addition to the TCP transmission control protocol, the primary component of this model was the IP protocol which (aside from a special abstraction layer) allowed for communication across different physical networks. After this, more and more research networks were consolidated on the basis of “TCP/IP” protocol combination, which in 1981 was definitively specified as a standard in the RFC 971.

IPv4 and IPv6: What is behind the different version numbers? Today, those who are concerned with the characteristics of a particular IP address e.g., one that would make computers addressable in a local network, will no doubt encounter the two variants IPv4 and IPv6. However, despite undergoing extensive changes in the past, in no way is this the fourth or sixth generation of IP protocol. IPv4 actually is the first official version of the Internet Protocol, whilst the version number relates to the fact that the fourth version of the TCP protocol is used. IPv6 is the direct successor of IPv4 – the development of IPv5 was suspended prematurely for economic reasons.

Even though there have been no further releases since IPv4 and IPv6, the Internet Protocol has been revised since its first mention in 1974 (before this it was just a part of TCP and did not exist independently). The focus was essentially on optimizing connection set-up and addressing. For example, the bit length of host addresses were increased from 16 to 32 bits, therefore extending the address space to approximately four billion possible proxies. The visionary IPv6 has 128-bit address fields and allows for about 340 sextillion (a number with 37 zeroes) different addresses, thus meeting the long term need for Internet addresses.

1.2.5 Routing

Network routing is the process of selecting a path across one or more networks. The principles of routing can apply to any type of network, from telephone networks to public transportation. In packet-switching networks, such as the Internet, routing selects the paths for Internet Protocol (IP) packets to travel from their origin to their destination. These Internet routing decisions are made by specialized pieces of network hardware called routers.
Consider the image below. For a data packet to get from Computer A to Computer B,

should it pass through networks 1, 3, and 5 or networks 2 and 4? The packet will take a shorter path through networks 2 and 4, but networks 1, 3, and 5 might be faster at forwarding packets than 2 and 4. These are the kinds of choices network routers constantly make.

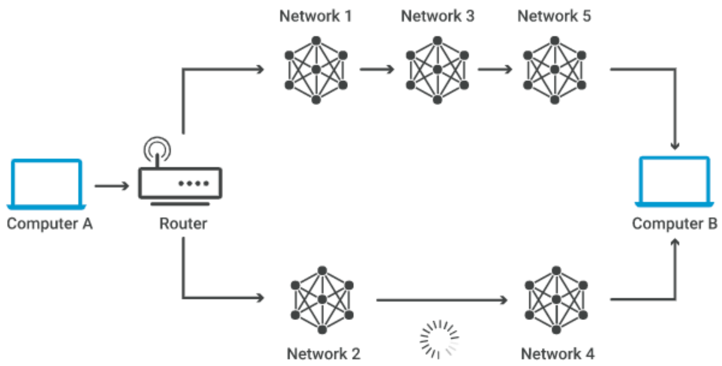


Figure 1.3: Routing Between Networks

What are the main routing protocols? In networking, a protocol is a standardized way of formatting data so that any connected computer can understand the data. A routing protocol is a protocol used for identifying or announcing network paths.
The following protocols help data packets find their way across the Internet:

IP: The Internet Protocol (IP) specifies the origin and destination for each data packet. Routers inspect each packet's IP header to identify where to send them.

BGP: The Border Gateway Protocol (BGP) routing protocol is used to announce which networks control which IP addresses, and which networks connect to each other. (The large networks that make these BGP announcements are called autonomous systems.) BGP is a dynamic routing protocol.

The below protocols route packets within an AS:

OSPF: The Open Shortest Path First (OSPF) protocol is commonly used by network routers to dynamically identify the fastest and shortest available routes for sending packets to their destination.

RIP: The Routing Information Protocol (RIP) uses "hop count" to find the shortest path from one network to another, where "hop count" means number of routers a packet must pass through on the way. (When a packet goes from one network to another, this is known as a "hop.")

Other interior routing protocols include EIGRP (the Enhanced Interior Gateway Routing Protocol, mainly for use with Cisco routers) and IS-IS (Intermediate System to Intermediate System).

1.2.6 Addressing

In addition, it is necessary to ensure that the transmitter and receiver can be correctly identified. Network addresses are used for this purpose. In computer networks, each computer typically has an IP address, similar to a telephone number, that uniquely identifies the computer. This internal IP address is used only for communication between the participants in the local network. For communication on the Internet, external IP addresses are used that are automatically assigned by the Internet provider. A distinction is also made between IPv4 and IPv6 addresses. IPv4 addresses used to be standard, but only a total of around 4.3 billion of these addresses could be assigned before they were exhausted. Due to the massive expansion of the Internet, additional IP addresses were urgently needed. Therefore, the new IPv6 standard was developed, allowing up to 3.4 x 1038 (340 sextillion) addresses. This should be sufficient for the future.

1.2.7 Classless IP Sub-netting

At a high level, classless addressing works by allowing IP addresses to be assigned arbitrary network masks without respect to “class.” That means /8 (255.0. 0.0), /16 (255.255. 0.0), and /24 (255.255. 255.0) network masks can be assigned to any address that would have traditionally been in the Class A, B, or C range. In a word, classless addressing can be summarized as: efficient. Specifically, as we can see in , classless addressing helped solve three major problems and delivers these advantages:

1. **More IP address allocations** Today, we know IPv6 is our long-term IP address solution to the However, IPv6 is not yet widely used. In the early 1990s, it was clear we would rapidly exhaust the IPv4 address space if nothing changed. As a result, classless addressing was used as a medium-term solution to help us stretch the life of IPv4.

2. **More balanced use of IP address ranges** Classless addressing decoupled the relationship between network size and IP address and allowed for balanced use across what used to be the Class A, B, and C ranges. Far less wasted addresses.

3. **More efficient routing** VLSM and subnetting make route aggregation and classless routing protocols possible. With route aggregation (sometimes called route summarization or supernetting), routing tables can be smaller, reducing resource consumption on routers, and saving bandwidth. Additionally, including network masks in routing protocols allows for more specific routes to be advertised. For example, 198.51.100.0/29 tells us more than 198.51.100.0 (with an implicit /24).

   Of course, as anyone who has studied for a networking certification can tell you, there is a significant complexity increase between classful and classless addressing. With classful addressing, you could always infer the subnet from the IP address. With classless addressing and VLSM, network masks must be explicitly defined. Similarly, there are complexities with classless routing that don't exist with classful routing. With classful routing, a routing table can have multiple matches for a single IP address. Overall, it's a lot more to learn and keep straight.

1.2.8 RIP Protocol

Routing Information Protocol (RIP) protocol are the intradomain (interior) routing protocol which is based on distance vector routing and it is used inside an autonomous system.Routers and network links are called node. The first column of routing table is destination address. The cost of metric in this protocol is hop count which is number of networks which need to be passed to reach destination. Here infinity is defined by a fixed number which is 16 it means that using a Rip, network cannot have more than 15 hops.

RIP Version-1: It is an open standard protocol means it works on the various vendor's routers. It works on most of the routers, it is classful routing protocol. Updates are broadcasted. Its administrative distance value is 120, it means it is not reliable, The lesser the administrative distance value the reliability is much more. Its metric is hop count and max hop count is 15. There will be a total of 16 routers in the network. When there will be the same number of hop to reach the destination, Rip starts to perform load balancing. Load balancing means if there are three ways to reach the destination and each way has same number of routers then packets will be sent to each path to reach the destination. This reduces traffic and also the load is balanced. It is used in small companies, in this protocol routing tables are updated in each 30 sec. Whenever link breaks rip trace out another path to reach the destination. It is one of the slowest protocol.

Advantages of RIP v1

1. Easy to configure, static router are complex.
2. Less overhead
3. No complexity.

Disadvantage of RIP v1

1. Bandwidth utilization is very high as broadcast for every 30 seconds.
2. It works only on hop count.
3. It is not scalable as hop count is only 15. If there will be requirement of more routers in the network it would be a problem .
4. Convergence is very slow, wastes a lot of time in finding alternate path.

RIP Version-2: Due to some deficiencies in the original RIP specification, RIP version 2 was developed in 1993. It supports classless Inter-Domain Routing (CIDR) and has the ability to carry subnet information, its metric is also hop count, and max hop count 15 is same as rip version 1. It supports authentication and does subnetting and multicasting. Auto summary can be done on every router. In RIPv2 Subnet masks are included in the routing update. RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast (255.255.255.255).

Advantages of RIP v2

1. It's a standardized protocol.
2. It's VLSM compliant.
3. Provides fast convergence.
4. It sends triggered updates when the network changes.
5. Works with snapshot routing – making it ideal for dial networks.

Disadvantage of RIP v2

1. Max hopcount of 15, due to the 'count-to-infinity' vulnerability.

2. No concept of neighbours.
3. Exchanges entire table with all neighbours every 30 seconds (except in the case of a triggered update).

1.3 Problem Statement

Suppose that you are the CEO of a startup which deals with network configuration for various companies. After 100 days of struggle, you have finally received your first assignment to configure the network for three different companies in such a way that all the PCs in each company must be able to communicate with each other as well as with all the PCs of any other company. The companies are named as CMP X, CMP Y and CMP Z.
CMP X has 5 Rooms with 1 PC in each room.
CMP Y has 3 Rooms with 3 PCs in each room.
CMP Z has 2 Rooms with 4 PCs in each room.
The IP regulating company has assigned the following IP network addresses to each of the company:
CMP Y: 50.152.0.0/15
CMP Z: 210.98.169.64/26
As part of the agreement, all three companies have asked you to bear the expense of all the switches and routers used to interconnect all the computers in a merged network for three companies and further instructed you that all the PCs in a single room must be on the same sub network and all the rooms of a single company must be on a different sub-network which will be assigned after sub-netting the assigned network address only for the relevant company (no outside network or the network of other company will be accepted) e.g, each room for CMP X will be assigned a different sub-network after sub-netting the address of 144.186.96.0/19 only and not any other network address. The companies have further informed you that companies plan to extend the number of their PCs in each room in the future.

You, beign cleverly economical, decide to install old switces (Generic Switches in Cisco Packet Tracer) with only three Ethernet ports working out of four and routers (Generic Routers in Cisco Packet Tracer) to configure the network for three companies in such a way that you use as much less routers and switches as possible.

You have also bought the folliwng IP network address for the serial communication between different routers which will be connecting different Inter-Company and Intra-Company subnets. You plan to form the subnets of the following address in order to cater the serial communication between all the routers: Routers Serial Communication: 199.210.121.160/28

1.3.1 Constrains

You, being very cautious, decide to simulate the topology on Cisco Packet Tracer in order to optimally design the network considering the number of devices (switches, routers etc.) used to maximize the profit margins of your company. However, you must simulate the topology strictly following rules and regulations described below:

1. Use Straight Through wires, Cross Over cables or Serial DCE wires where necessary and applicable.
2. Use Generic Router and Generic PCs for your design
3. Use Generic Switches such that you attach only 3 of the 4 available Ethernet Interfaces for a single switch, however, you can attach as many switches considering optimal design.
4. You have to assign IPs to the PCs using Static IP allocation.
5. Although you have to use GUI of the router to configure its interfaces but you must use CLI of the router to configure the RIPv2 Protocol for Classless Subnet Addressing.

1.4 Requirements

This section explain the basic requirements needed to design the proposed methodology.

1.4.1 Routers

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same

Internet connection. There are several types of routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router. A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches*. ”A network switch forwards data packets between groups of devices in the same network, whereas a router forwards data between different networks”

1.4.2 Switches

A switch, in the context of networking, is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN). A LAN switch operates at the data link layer (Layer 2) or the network layer of the OSI Model and, as such it can support all types of packet protocols. The layer 2 switch is also sometimes called a bridge: its function is to send frames containing data packets between nodes or segments of a network. Essentially, switches are the traffic cops of a simple local area network. Switching establishes the trajectory for the frames as the data units, and how the data moves from one area of a network to another. By contrast, routing takes place at layer 3, there data gets sent between networks or from one network to another.

1.4.3 PC(End-Points)

An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Endpoints represent key vulnerable points of entry for cybercriminals. Endpoints are where attackers execute code and exploit vulnerabilities, as well as where there are assets to be encrypted, exfiltrated or leveraged. With organizational workforces becoming more mobile and users connecting to internal resources from off-premises endpoints all over the world, endpoints are increasingly susceptible to cyberattacks.

1.4.4 Cisco Packet Tracer

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Cisco Networking Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

1.5 Applications

Following are some business applications of computer networks:

Resource Sharing: The goal is to make all programs, equipments(like printers etc), and especially data, available to anyone on the network without regard to the physical location of the resource and the user.

Server-Client model: One can imagine a company's information system as consisting of one or more databases and some employees who need to access it remotely. In this model, the data is stored on powerful computers called Servers. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simple machines, called Clients, on their desks, using which they access remote data.

Communication Medium: A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication.

eCommerce: A goal that is starting to become more important in businesses is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future.

Chapter 2

METHODOLOGY

As in previous chapter we have seen the basic overview of our project. In this chapter we'll work on adopted methodology to create a required network. The first basic step in creating a network is address allocation for which we're using classless sub-netting and all the IP calculation are been mentioned in respective section called mathematical model. After mathematical model there is configuration of computers has been shown afterwards there is completed topology diagram and at end there is final demonstration in paper figure format to show the successfully transmission of data from one end to the other.

2.1 Mathematical Model

This section include the mathematical model for the proposed network with their respective company titles.

2.1.1 For Company CMP-X

5 Rooms – 5 Subnets

1 PC Each Room

Assigned IP: 144.186.96.0/19

Binary Form Of IP: 10010000.10111010.01100000.00000000

Network Mask:11111111.11111111.11100000.00000000

As we need to have 5 subnets, we will use 3 additional bits for subnetting that will be 20,21,22

Subnet Mask = 19+3 = /22

For Subnet No #01

Subnet IP: 10010000.10111010.01100000.00000000

144.186.96.0

First IP:

10010000.10111010.01100000.00000000

11111111.11111111.11111100.00000000

AND

144.186.96.0/22

Last IP:

10010000.10111010.01100000.00000000

00000000.00000000.00000011.11111111

OR

144.186.99.255/22

Difference: 0.0.3.255

Total Address:

- 2^32-22 = 1024
- By IP Difference: 4*256 = 1024

For Subnet No #05

Subnet IP: Subnet IP: 10010000.10111010.01110000.00000000

First IP:

Subnet IP: 10010000.10111010.01110000.00000000

11111111.11111111.11111100.00000000

AND

144.186.112.0/22

Last IP:

Subnet IP: 10010000.10111010.01110000.00000000

00000000.00000000.00000011.11111111

OR

144.186.115.255/22

Difference: 0.0.3.255

Total Address:

- 2^32-22 = 1024
- By IP Difference: 4*256 = 1024

2.1.2 For Company CMP-Y

3 Rooms – 3 Subnets

3 PC Each Room

Assigned IP: 50.152.0.0/15

Binary Form Of IP: 00110010.10011000.00000000.00000000

Network Mask:11111111.11111111.10000000.00000000

As we need to have 5 subnets, we will use 2 additional bits for subnetting that will be 16,17

Subnet Mask = 15+2 = /17

For Subnet No #01

Subnet IP: 00110010.10011000.00000000.00000000

50.152.0.0

First IP:

00110010.10011000.00000000.00000000

11111111.11111111.10000000.00000000

AND

50.152.0.0/17

Last IP:

00110010.10011000.00000000.00000000

00000000.00000000.01111111.11111111

OR

50.152.127.255/17

Difference: 0.0.127.255

Total Addresses:

- 2^32-17 = 32768
- By IP Difference: 128*256 = 32768

For Subnet No #03

Subnet IP: 00110010.10011001.00000000.00000000

50.153.0.0

First IP:

00110010.10011001.00000000.00000000

11111111.11111111.10000000.00000000

AND

50.153.0.0/17

Last IP:

00110010.10011001.00000000.00000000

00000000.00000000.01111111.11111111

OR

50.153.127.255/17

Difference: 0.0.127.255

Total Addresses:

- 2^32-17 = 32768
- By IP Difference: 128*256 = 32768

2.1.3 For Company CMP-Z

2 Rooms – 2 Subnets

4 PC Each Room

Assigned IP: 210.98.169.64/26

Binary Form Of IP: 11010010.01100010.10101001.01000000

Network Mask:11111111.11111111.11111111.11000000

As we need to have 2 subnets, we will use 1 additional bit for subnetting that will be 27

Subnet Mask = 26+1 = /27

For Subnet No #01

Subnet IP: 11010010.01100010.10101001.01000000

210.98.169.64

First IP:

11010010.01100010.10101001.01000000

11111111.11111111.11111111.11100000

AND

210.98.169.64/27

Last IP:

11010010.01100010.10101001.01000000

00000000.00000000.00000000.00011111

OR

210.98.169.95/27

Difference: 0.0.0.31

Total Addresses:

- 2^32-27 = 32
- By IP Difference: 1*32 = 32

For Subnet No #02

Subnet IP: 11010010.01100010.10101001.01100000

210.98.169.95

First IP:

11010010.01100010.10101001.01100000

11111111.11111111.11111111.11100000

AND

210.98.169.95/27

Last IP:

11010010.01100010.10101001.01100000

00000000.00000000.00000000.00011111

OR

210.98.169.127/27

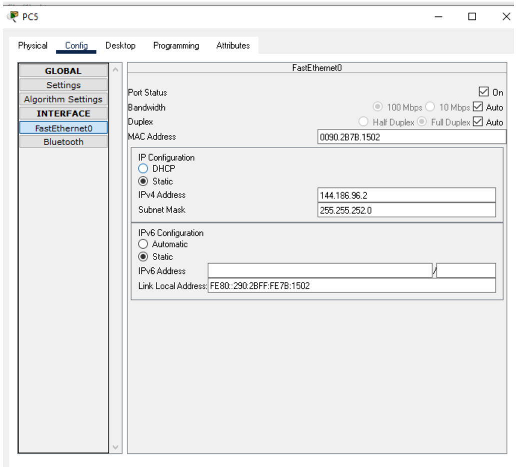
Difference: 0.0.0.31
Total Addresses:

- 2ˆ32-27 = 32

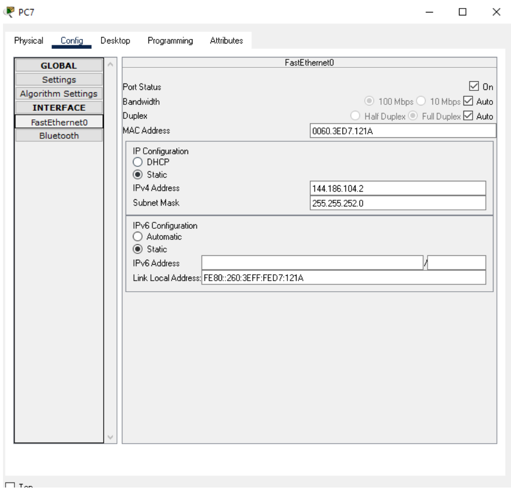
- By IP Difference: 1*32 = 32

2.2 Configuration

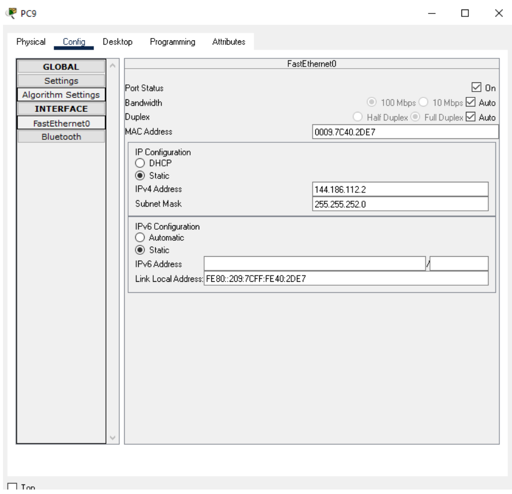
The goal of a computer network is to improve accessibility and the performance of the system. A system's performance can be improved by inserting one or more processors into it as its workload grows. In this section there is configuration of network end points is shown via images as there are almost of 25 endpoint but for the report only 9 PC end point with there respective IP addresses is shown.
For Company X :



(a)



(b)

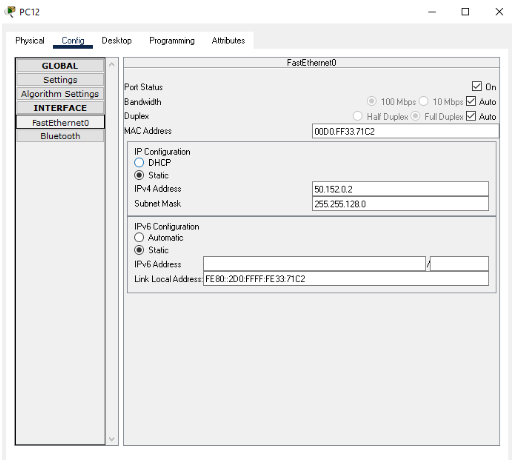


(c)

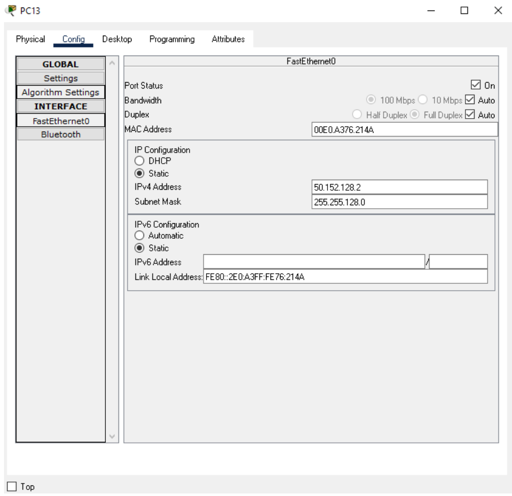
Figure 2.1: Configuration Of End-Points For Company X

In Fig.2.1 configuration of Company X where there are five sub-nets and one PC in each sub-net is installed. These images show the IP configuration of PC by classless sub-netting.

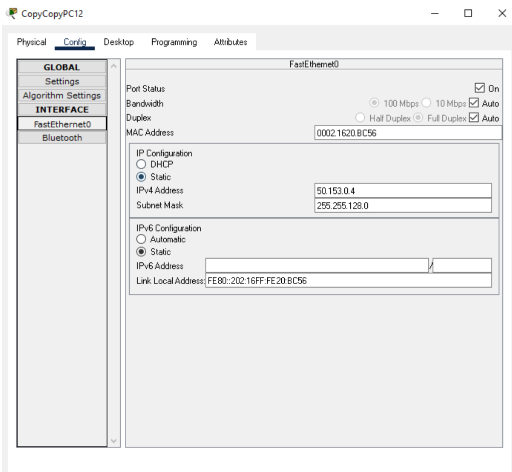
For Company Y :



(a)



(b)



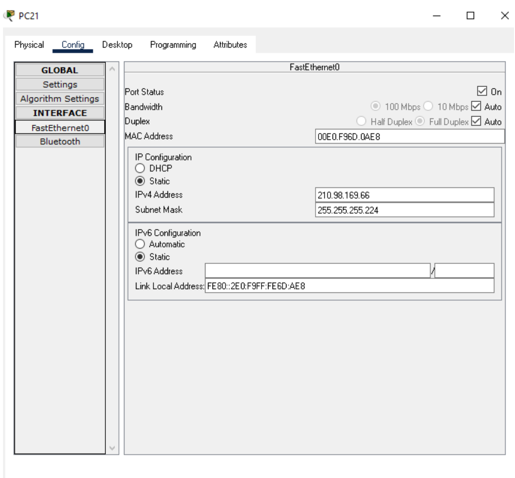
(c)

Figure 2.2: Configuration Of End-Points For Company Y

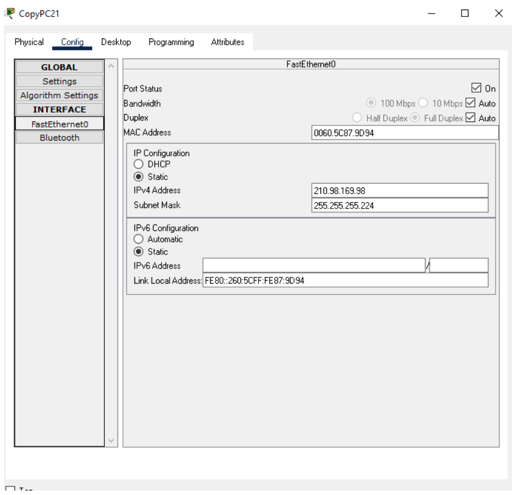
In Fig.2.2 configuration of Company Y where there are three sub-nets and two PC in each sub-net is installed. These images show the IP configuration of PC by classless sub-netting.

For Company Z :

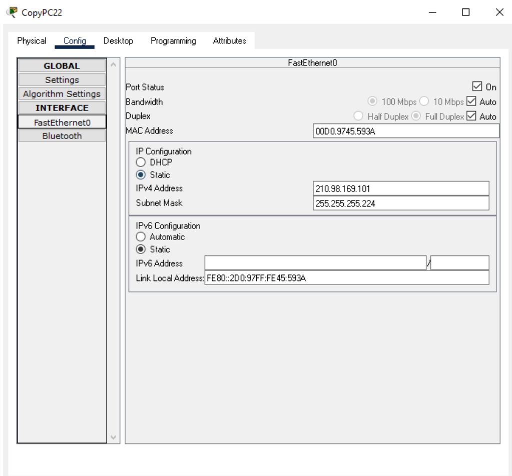
In Fig.2.3 configuration of Company Z where there are two sub-nets and three PC in each sub-net is installed. These images show the IP configuration of PC by classless sub-netting.



(a)



(b)



(c)

Figure 2.3: Configuration Of End-Points For Company Z

2.3 Topology Diagram

In Fig. 2.4 finalized topology network is shown where we have configured the network using provided constrains and IPs. There are total of 5 routers to interact with different network and 15 switches to attach the PC to the network. All the three companies are inter connected to each other and all the twenty two end points are using IP provided by classless sub-netting and for routing RIPv2 protocol is used.

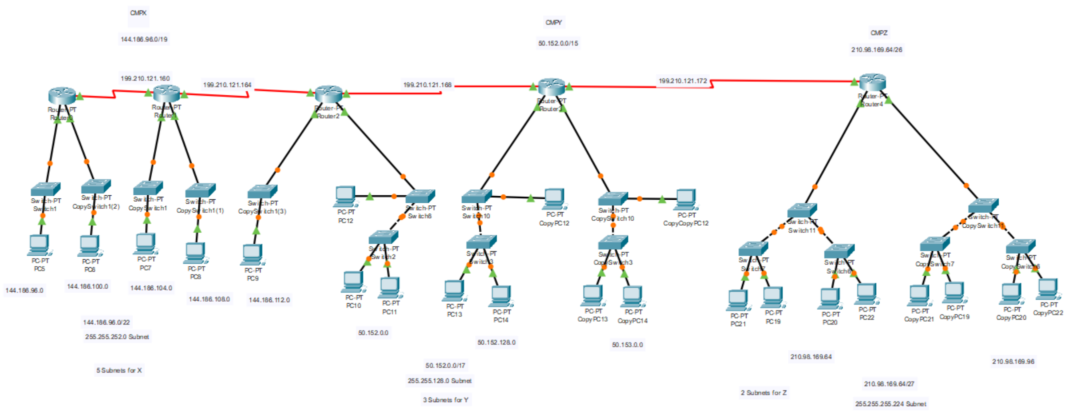


Figure 2.4: Final Network Configuration

2.4 Data Transmission

When sending data from software to actual physical transmission link (medium), there are several layers. Each layer provides certain services. The Open System Interconnection (OSI) layer model is the international standard, and it has 7 layers.

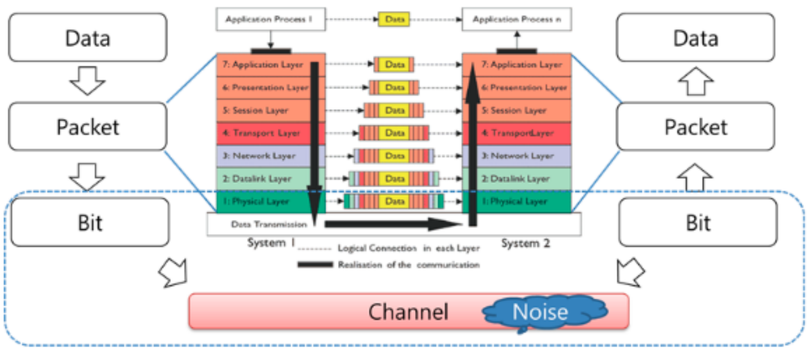
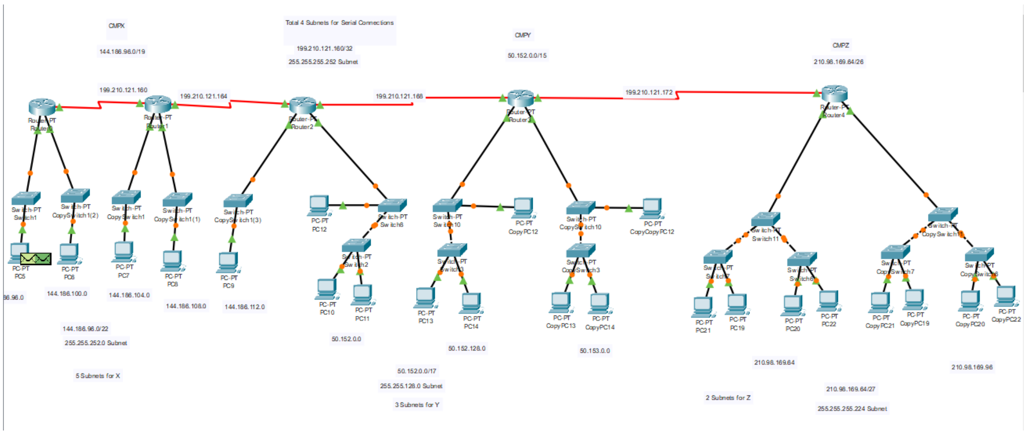
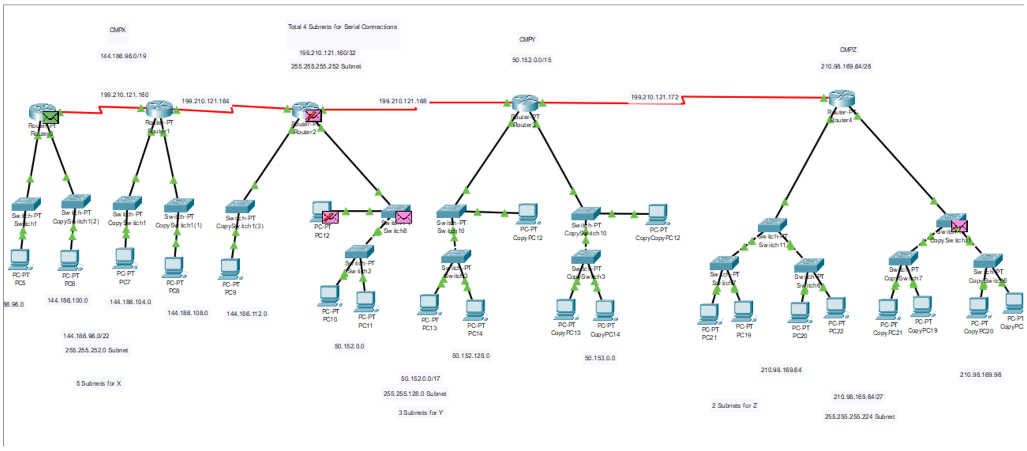


Figure 2.5: General digital control system

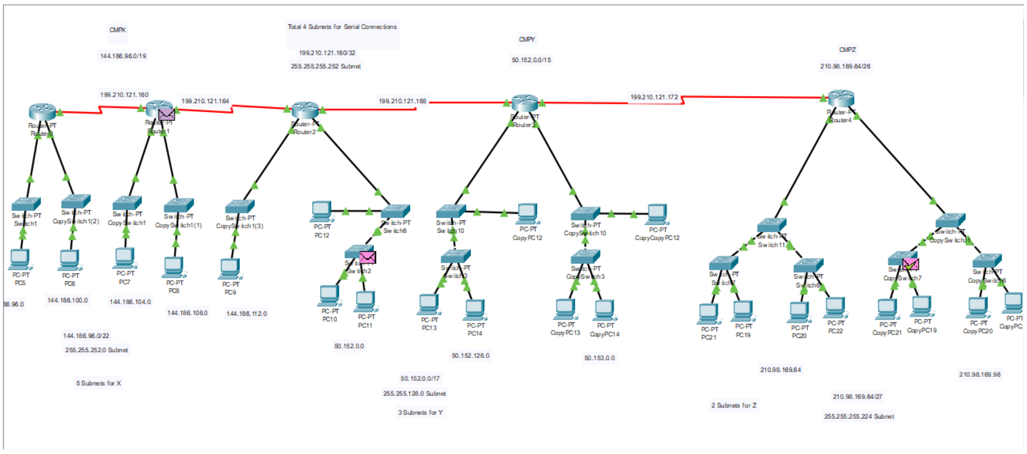
In Fig.2.7, 2.7 the transmission of data packet is shown. As one of the requirement for the network was to interconnect all the companies together so that the data from one company can easily travel to the other. To find best possible route for the transmission RIPv2 protocol is used that is hop count base routing system. We transmitted the packet from PC5 of CMP-X to the PC22 of CMP-Z. In attached images it can clearly be seen that packet reached its destination hop by hop that is from one router to the other router.



(a)

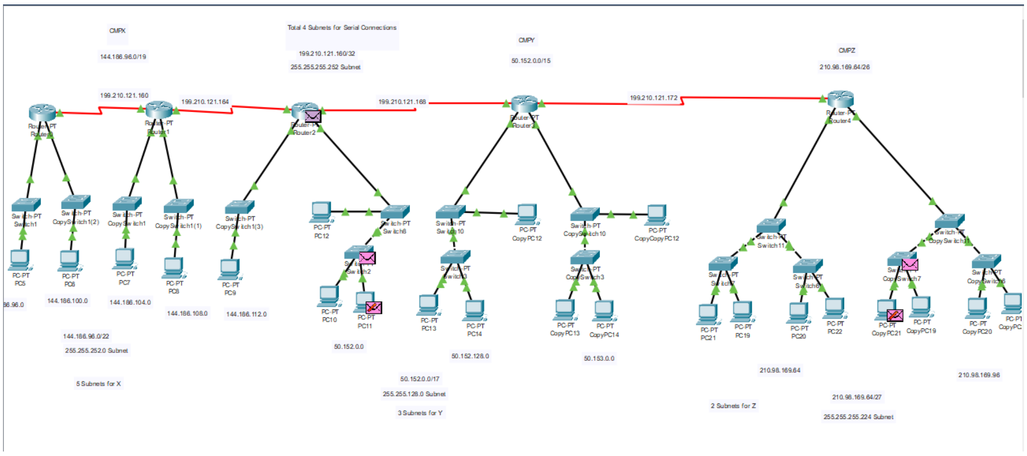


(b)

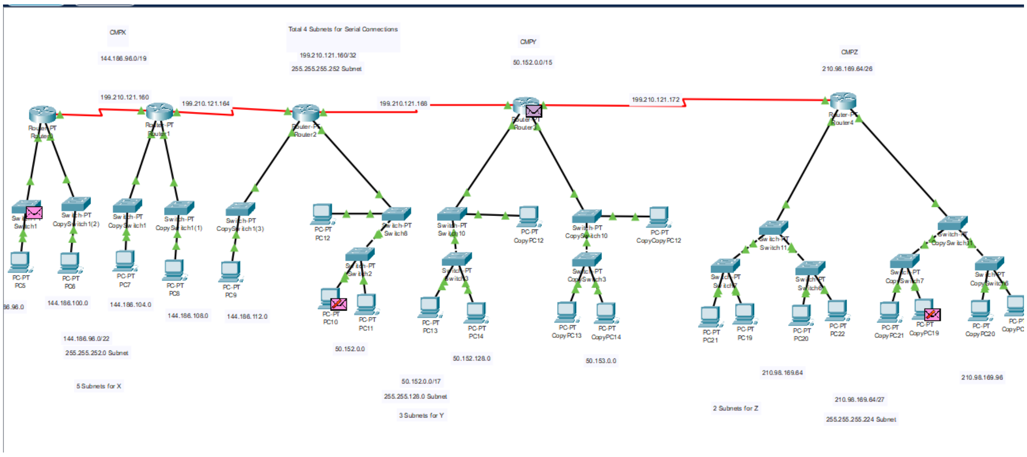


(c)

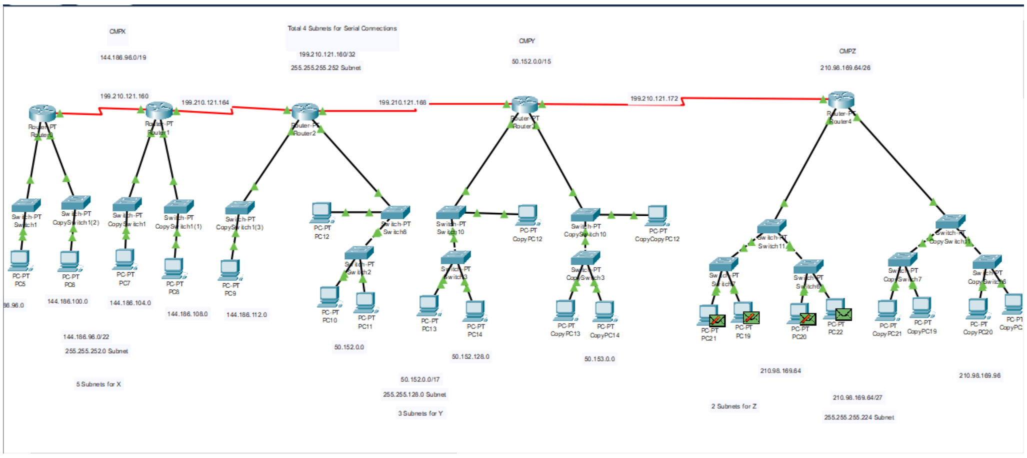
Figure 2.6: Transmission From CMP-X PC5 To CMP-Z PC22 A



(a)



(b)



(c)

Figure 2.7: Transmission From CMP-X PC5 To CMP-Z PC22 B

Chapter 3

CONCLUSIONS

As in previous chapters we have seen the introduction to the proposed model and adopted methodology of the system along side all IP configuration and data transmission from one end to the other. In this last chapter of the report we'll focus on the conclusion to all our approaches through out the project. We'll start form discussing the results of previous sections and general comparisons and at the end we'll show the designed system meet the initial project objectives.

3.1 Results And Discussions

The main objective of data communication and networking is to enable seamless exchange of data between any two points in the world. This exchange of data takes place over a computer network. Data refers to the raw facts that are collected while information refers to processed data that enables us to take decisions. As we have seen in previous chapter that how the sub-netting and routing protocol improve the quality of any network as well as we have demonstrated how the data is traveling form hop to hop.

3.2 Conclusions

At the completion of this project we have observed that Computer Network means an interconnection of autonomous (standalone) computers for information exchange. The connecting media could be a copper wire, optical fiber, microwave, or satellite. The network will be considered by following criteria:

Performance – It is measured in terms of transit time and response time.

Reliability – It is measured in terms of Frequency of failure ,Recovery from failures ,Robustness during catastrophe
Security – It means protecting data from unauthorized access.

- As were initial objective were to understand the classes less addressing that is completed by assigning properly derived IPs to each PC.
- We have used the RIPv2 protocol that is routing protocol to define the path for data from source to destination.
- At the end we have established the complete topology with different PCs, Routers and Switches that is shown in above section along side explanation.

Bibliography

[1] https://www.geeksforgeeks.org/goals-of-networks/

[2] https://ecomputernotes.com/computernetworkingnotes/communication-networks/what-is-data-communication

[3] https://www.techtarget.com/searchnetworking.

[4] https://community.cisco.com/t5/networking-documents/ripv2-routing-information-protocol/ta-p/3117425.

[5] https://www.geeksforgeeks.org/differences-between-ripv1-and-ripv2/