1. **INTRODUCTION**

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there." The rapid explosion of the internet and existence of high speed wireless and broadband networks have contributed towards depletion of IPv4.The IPv4 protocol created more than three decades ago with approximately an address space of 4 billion cannot cater to the needs of modern internet.

IP Subnetting is a process of dividing a large IP network into smaller IP networks. In Subnetting we create multiple small manageable networks from a single large IP network. Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class. CIDR or Classless Inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller subnetworks which provides better network management capabilities.

Every network address has a valid range of host addresses. All devices attached to the same network will have an IPv4 host address for that network and a common subnet mask or network prefix. Traffic can be forwarded between hosts directly if they are on the same subnet. Traffic cannot be forwarded between subnets without the use of a router. To determine if traffic is local or remote, the router uses the subnet mask. The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address. IPv4 subnets are created by using one or more of the host bits as network bits. Two very important factors that will lead to the determination of the IP address block with the subnet mask are the number of subnets required, and the maximum number of hosts needed per subnet. Subnetting a subnet, or using Variable Length Subnet Mask (VLSM), was designed to avoid wasting addresses

1. **LITERATURE SURVEY**

A network is a collection of computers, servers, network devices, peripherals, or other devices connected to one another to allow the sharing of data. Networks come in all sizes. They can range from simple networks consisting of two computers to networks connecting millions of devices.

**2.1 Network Components**

The network infrastructure contains three categories of network components:

* Devices.
* Network Media.
* Services.

**Devices**

Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices.

1. **End Devices**

The network devices that people are most familiar with are called end devices. An end device is either the source or destination of a message transmitted over the network.



Fig:2.1.a End and Edge Devices

1. **Intermediate Devices**

Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork. These intermediary devices provide connectivity and ensure that data flows across the network.



Fig:2.1.b Intermediary Devices

**Media**

Communication across a network is carried on a medium. The medium provides the channel over which the message travels from source to destination. Modern networks primarily use three types of media to interconnect devices and to provide the pathway over which data can be transmitted. Network media are:

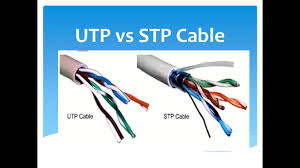
* **Metallic wires within cables** - data is encoded into electrical impulses
* **Glass or plastic fibers (fiber optic cable)** - data is encoded as pulses of light
* **Wireless transmission** - data is encoded using wavelengths from the electromagnetic spectrum

**Copper Media**

There are different Cabling options depending on the access method

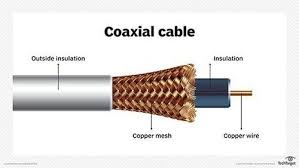
**Twisted pair**

The wires are twisted around each other to minimize interference from other twisted pairs in the cable. Twisted pair cables are available unshielded (UTP) or shielded (STP). UTP is the most common type and uses a RJ-45 Connector. Typical lengths are up to 100m. Twisted pair network uses a star topology.



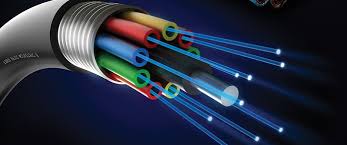
**Coaxial**

Coaxialcable uses BNC connectors. The maximum cable lengths are around 500m. Coaxial networks use a single bus topology

****

**Fiber Optic**

UTP and Co-axial cables are not capable for driving the data signals for long distance i.e. UTP is capable of transmitting up to a distance 100 meters only By using the Fiber cables it is possible to send the data about 10 kilometers. Fiber optic cable uses SC, ST, LC connectors (most common in use is SC connector). In fiber cables the data is converted to light signals and the signal is made to propagate through the fiber cable. There are two types of Fibre optic cable available.



**2.2 Types of Network**

Network infrastructures can vary greatly in terms of:

* Size of the area covered
* Number of users connected
* Number and types of services available

Different types of network are:

1. **Local Area Network**

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization’ offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.

**2. Wide Area Network**

As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone WANs use very expensive network equipment.

**3. Personal Area Network**

A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.

**4. Metropolitan Area Network**

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).

**5. Storage Area Network**

A Storage Area Network (SAN) is a specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols.

**2.3 Network Devices**

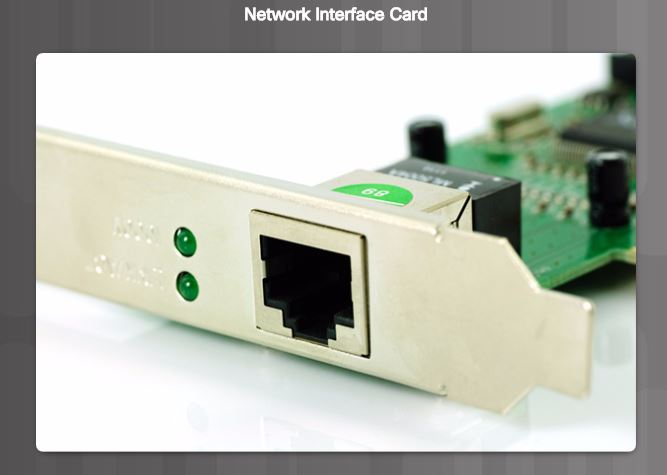
Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called Network Devices. Network devices transfer the data to signals, providing connectivity to different network devices, transfer the data in the form of packets or frames form one device to other. These devices transfer data in a fast, secure and correct way over same or different networks. Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc. Let us explore some of these devices in greater detail.

**Modem**

A modem is a very important piece of network hardware that allows a computer to send and receive data through a telephone line or cable connection. In simple words, it’s the device that connects a computer to the [Internet](https://www.scienceabc.com/innovation/internet-randomly-ceases-work-sometimes.html).



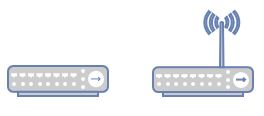
**Network Interface Card (NIC)**

****

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

**Hub**

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.



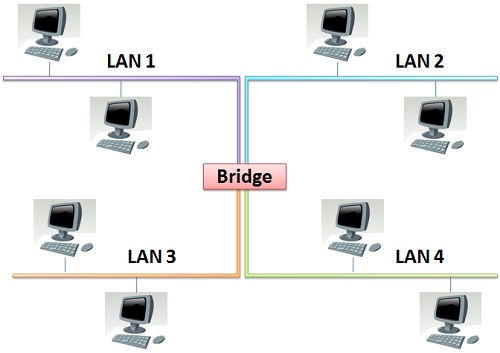
**Repeater**

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length which the signal can be transmitted over the same network.



**Bridge**

A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination.



**Switch**

A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.



**Router**

A router is a device like a switch that routes data packets based on their IP addresses**.** Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.

****

**2.4 Access Methods**

A Cisco IOS switch can be implemented with no configuration and still switch data between connected devices. By connecting two PCs to a switch, those PCs will instantly have connectivity with one another. Even though a Cisco switch will function immediately, configuring initial settings are a recommended best practice. There are several ways to access the CLI environment and configure the device. The most common methods are:

**Console** – This is a physical management port that provides out-of-band access to a Cisco device. Out-of-band access refers to access via a dedicated management channel that is used for device maintenance purposes only.

**Secure Shell (SSH)** – SSH is a method for remotely establishing a secure CLI connection through a virtual interface, over a network. Unlike a console connection, SSH connections require active networking services on the device including an active interface configured with an address.

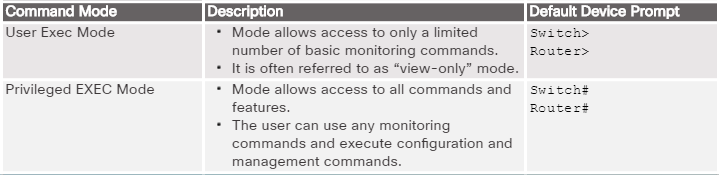
**Telnet** - Telnet is an insecure method of remotely establishing a CLI session through a virtual interface, over a network. Unlike SSH, Telnet does not provide a securely encrypted connection. User authentication, passwords, and commands are sent over the network in plaintext.

**2.5 Primary Command Modes**

As a security feature, the Cisco IOS software separates management access into the following two command modes:

**User EXEC Mode -** This mode has limited capabilities but is useful for basic operations. It allows only a limited number of basic monitoring commands but does not allow the execution of any commands that might change the configuration of the device. The user EXEC mode is identified by the CLI prompt that ends with the > symbol.

**Privileged EXEC Mode -** To execute configuration commands, a network administrator must access privileged EXEC mode. Higher configuration modes, like global configuration mode, can only be reached from privileged EXEC mode. The privileged EXEC mode can be identified by the prompt ending with the # symbol.



The table in the figure summarizes the two modes and displays the default CLI prompts of a Cisco switch and router.

**Configuration Command Modes**

To configure the device, the user must enter Global Configuration Mode, which is commonly called global config mode.

From global config mode, CLI configuration changes are made that affect the operation of the device as a whole. Global configuration mode is identified by a prompt that ends with (config)# after the device name, such as Switch(config)#.

**Global configuration mode** is accessed before other specific configuration modes. From global config mode, the user can enter different sub-configuration modes. Each of these modes allows the configuration of a particular part or function of the IOS device.

Two common sub-configuration modes include:

**Line Configuration Mode -** Used to configure console, SSH, Telnet, or AUX access.

**Interface Configuration Mode -** Used to configure a switch port or router network interface.

When using the CLI, the mode is identified by the command-line prompt that is unique to that mode. By default, every prompt begins with the device name. Following the name, the remainder of the prompt indicates the mode. For example, the default prompt for line configuration mode is **Switch(config-line)#**and the default prompt for interface configuration mode is **Switch(config-if)#**.

**2.6 Navigate Between IOS Modes**

Various commands are used to move in and out of command prompts. To move from user EXEC mode to privileged EXEC mode, use the enable command. Use the disable privileged EXEC mode command to return to user EXEC mode. To move in and out of global configuration mode, use the configure terminal privileged EXEC mode command. To return to the privileged EXEC mode, enter the exit global config mode command. There are many different sub-configuration modes. For example, to enter line sub-configuration mode, you use the line command followed by the management line type and number you wish to access.

**Switch(config)# line console 0**

**Switch(config-line)#**

To move from any sub-configuration mode of the global configuration mode to the mode one step above it in the hierarchy of modes, enter the exit command.

**Switch(config-line)# exit**

**Switch(config)#**

**Switch(config-line)# end**

**Switch#**

**Switch(config-line)# interface FastEthernet 0/1**

**Switch(config-if)#**

**2.7 Network Protocols**

At the human level, some communication rules are formal and others are simply understood based on custom and practice. For devices to successfully communicate, a network protocol suite must describe precise requirements and interactions. Networking protocols define a common format and set of rules for exchanging messages between devices. Some common networking protocols are Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Internet Protocol (IP).

**HTTP -** is an application protocol that governs the way a web server and a web client interact.

**TCP** - is the transport protocol that manages the individual conversations.

**IP -** is responsible for taking the formatted segments from TCP, encapsulating them into packets, assigning them the appropriate addresses, and delivering them to the destination host.

**Ethernet**- is a network access protocol that describes two primary functions: communication over a data link and the physical transmission of data on the network media. Network access protocols are responsible for taking the packets from IP and formatting them to be transmitted over the media.

A set of protocols that work together to provide comprehensive network communication services is called protocol suite. A protocol suite may be specified by a standards organization or developed by a vendor. Standards organizations are usually vendor-neutral, non-profit organizations established to develop and promote the concept of open standards.

**Dynamic Host Configuration Protocol**

The Dynamic Host Configuration Protocol (DHCP) for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters. This is referred to as dynamic addressing. The alternative to dynamic addressing is static addressing. When using static addressing, the network administrator manually enters IP address information on hosts. When a host connects to the network, the DHCP server is contacted, and an address is requested.

**2.8 Network Models**

**Layered Model Concepts and Benefits**

Many benefits can be gained from the process of breaking up the functions or tasks of networking into smaller chunks, called layers, and defining standard interfaces between these layers. The layers break a large, complex set of concepts and protocols into smaller pieces, making it easier to talk about, to implement with hardware and software, and to troubleshoot.

**OSI Reference Model**

The OSI model describes how information makes its way from application programs through a network medium to another application program in other computer. It divides one big problem in to seven smaller problems. Each problem is addressed by one of the seven layers of the OSI model.

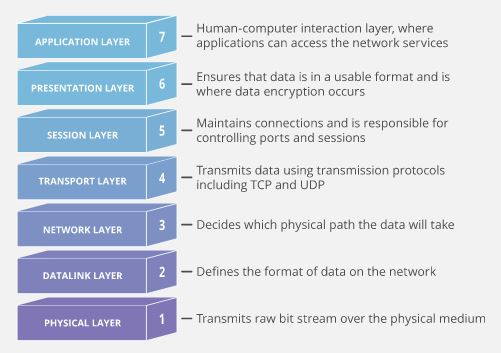


Figure:2.8 OSI Model

**The TCP/IP Protocol Model**

The TCP/IP protocol model for internetwork communications was created in the early 1970s and is sometimes referred to as the Internet model. As shown in the figure, it defines four categories of functions that must occur for communications to be successful. The architecture of the TCP/IP protocol suite follows the structure of this model. Because of this, the Internet model is commonly referred to as the TCP/IP model.

Most protocol models describe a vendor-specific protocol stack. Legacy protocol suites, such as Novell Netware and AppleTalk, are examples of vendor-specific protocol stacks. Because the TCP/IP model is an open standard, one company does not control the definition of the model.

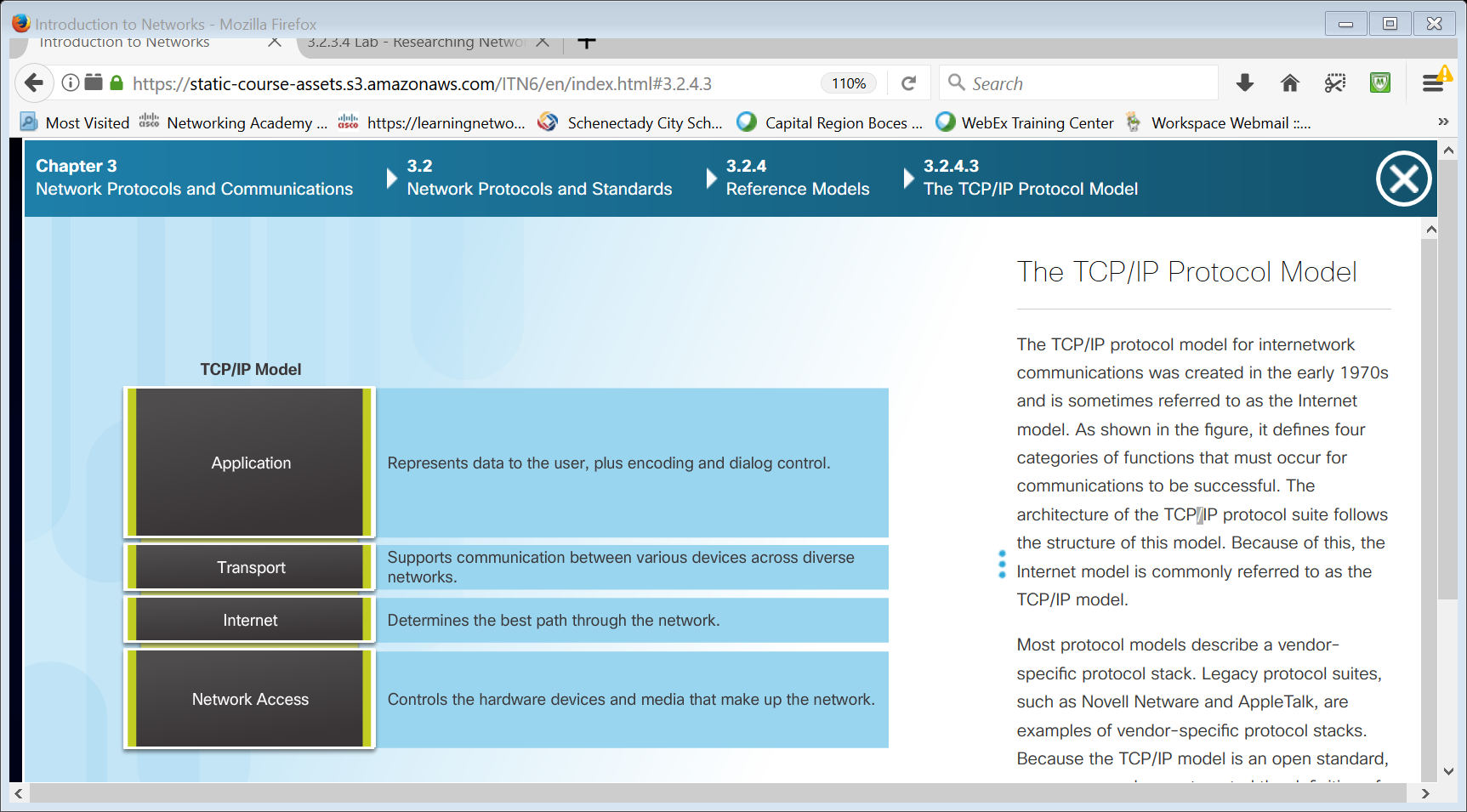
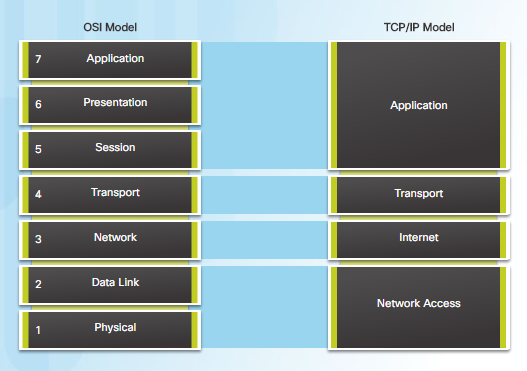
****

Figure:2.8.1: TCP/IP Protocol Model

**Similarities between TCP/IP model and OSI model**

* Both are the logical models.
* Both define standards for networking.
* Both provide a framework for creating and implementing networking standards and devices.
* Both divide the network communication process in layers.
* In both models, a single layer defines a particular functionality and set standards for that functionality only.
* Both models allow a manufacturer to make devices and network components that can coexist and work with the devices and components made by other manufacturers.
* Both models simplify troubleshooting process by dividing complex functions into simpler components.
* Instead of defining the already defined standards and protocols, both models referenced them. OSI Layer model has seven layers while TCP/IP model has four layers.
* OSI Layer model is no longer used while TCP/IP is still used in computer networking.
* To define the functionality of upper layers, OSI uses three separate layers (application, presentation and session) while TCP/IP uses a single layer (application).
* Just like upper layers, OSI uses two separate layers (Physical and Data link) to define the functionality of bottom layers while TCP/IP uses a single layer (Link) for the same.



OSI and TCP/IP model

**2.9 Physical LAN Topologies**

Physical topology defines how the end systems are physically interconnected. In shared media LANs, end devices can be interconnected using the following physical topologies:

**Star** - End devices are connected to a central intermediate device. Early star topologies interconnected end devices using Ethernet hubs. The star topology is easy to install, very scalable and easy to troubleshoot.

**Extended Star** - In an extended star topology, additional Ethernet switches interconnect other star topologies. An extended star is an example of a hybrid topology.

**Bus** - All end systems are chained to each other and terminated in some form on each end. Infrastructure devices such as switches are not required to interconnect the end devices. Bus topologies using coax cables were used in legacy Ethernet networks because it was inexpensive and easy to set up.

**Ring** - End systems are connected to their respective neighbor forming a ring. Unlike the bus topology, the ring does not need to be terminated. Ring topologies were used in legacy Fiber Distributed Data Interface (FDDI) and Token Ring networks.

**2.10 Half and Full Duplex**

Duplex communications refer to the direction of data transmission between two devices. Half-duplex communications restrict the exchange of data to one direction at a time while full-duplex allows the sending and receiving of data to happen simultaneously.

**Half-duplex communication** - Both devices can transmit and receive on the media but cannot do so simultaneously. Half-duplex allows only one device to send or receive at a time on the shared medium and is used with contention-based access methods.

**Full-duplex communication** - Both devices can transmit and receive on the media at the same time. The data link layer assumes that the media is available for transmission for both nodes at any time. Ethernet switches operate in full-duplex mode by default but can operate in half-duplex if connecting to a device such as an Ethernet hub.

**Auto-MDIX**

When the auto-MDIX feature is enabled, the switch detects the type of cable attached to the port and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 port on the switch, regardless of the type of device on the other end of the connection

**2.11 System requirements**

1. Hardware requirements
2. Software requirements

**Hardware requirements**

CPU : Intel Dual core

RAM : 1GB

Hard disk : 256GB

**Software requirements**

Operating system : Windows 7 or 10/Linux

Tool : Cisco Packet Tracer 6 / 7

Terminal Emulation Program : puTTY, TeraTerm

1. **IP ADDRESSING**

Addressing is a critical function of network layer protocols. Addressing enables data communication between hosts, regardless of whether the hosts are on the same network, or on different networks. Both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) provide hierarchical addressing for packets that carry data. The use of IP addresses is the primary means of enabling devices to locate one another and establish end-to-end communication on the Internet. Each end device on a network must be configured with an IP address.

**3.1 IPv4 Addresses**

Every machine on the internet has a unique identifying number, called an IP Address. A typical IP address looks like this: 216.27.61.45. IPv4 Address is a 32-bit number, usually written in dotted decimal form, that uniquely identifies an interface of some computer.

Binary is a numbering system that consists of the numbers 0 and 1 called *bits*. In contrast, the decimal numbering system consists of 10 digits consisting of the numbers 0 – 9. Binary is important for us to understand because hosts, servers, and network devices use binary addressing. The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255. IPv4 addresses are assigned to individual devices connected to a network.

Each address consists of a string of 32 bits, divided into four sections called *octets*. Each octet contains 8 bits (or 1 byte) separated with a dot. For example, PC1 in the figure is assigned IPv4 address 11000000.10101000.00001010.00001010. Its default gateway address would be that of R1 Gigabit Ethernet interface 11000000.10101000.00001010.00000001.

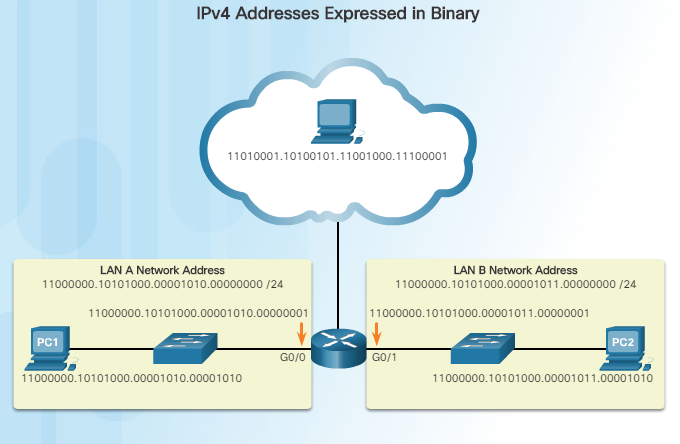


Figure 3.1.1: Doted decimal format representation of IPV4 address

**IPv4 Communication**

A host successfully connected to a network can communicate with other devices in one of three ways:

* **Unicast** - The process of sending a packet from one host to an individual host.
* **Broadcast** - The process of sending a packet from one host to all hosts in the network.
* **Multicast** - The process of sending a packet from one host to a selected group of hosts, possibly in different networks.

**IP Address Classes**

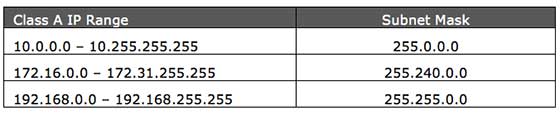
There are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only classes A, B, and C are commonly used. Each class allows for a range of valid IP addresses, shown in the following table.

|  |  |  |
| --- | --- | --- |
| Class | Address range | Supports |
| **Class A** | 1.0.0.1 to 126.255.255.254 | Supports 16 million hosts on each of 127 networks. |
| **Class B** | 128.1.0.1 to 191.255.255.254 | Supports 65,000 hosts on each of 16,000 networks. |
| **Class C** | 192.0.1.1 to 223.255.254.254 | Supports 254 hosts on each of 2 million networks. |
| **Class D** | 224.0.0.0 to 239.255.255.255 | Reserved for [multicast](https://www.computerhope.com/jargon/m/multicast.htm) groups. |
| **Class E** | 240.0.0.0 to 254.255.255.254 | Reserved for future use, or research and development purposes. |

There are a few reserved IPv4 address spaces which cannot be used on the internet. These addresses serve special purpose and cannot be routed outside the Local Area Network.

**Private IP Addresses**

Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses. These IPs can be used within a network, campus, company and are private to it. These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.



**3.2 IPv6 Addresses**

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

**Address Structure**

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols. For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ‘:’ symbol: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

**IPv6 Unicast Addresses**

An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. A packet sent to a unicast address is received by the interface that is assigned that address. Similar to IPv4, a source IPv6 address must be a unicast address. The destination IPv6 address can be either a unicast or a multicast address.

**Global unicast**

A global unicast address is similar to a public IPv4 address. These are globally unique, Internet routable addresses. Global unicast addresses can be configured statically or assigned dynamically.

**Link-local**

Link-local addresses are used to communicate with other devices on the same local link. With IPv6, the term link refers to a subnet. Link-local addresses are confined to a single link. Their uniqueness must only be confirmed on that link because they are not routable beyond the link. In other words, routers will not forward packets with a link-local source or destination address.

**Unique local**

Another type of unicast address is the unique local unicast address. IPv6 unique local addresses have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences. Unique local addresses are used for local addressing within a site or between a limited number of sites. These addresses should not be routable in the global IPv6 and should not be translated to a global IPv6 address. Unique local addresses are in the range of FC00::/7 to FDFF::/7.

**IPv6 Address Types**

There are three types of IPv6 addresses:

**Unicast -** An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. As shown in the figure, a source IPv6 address must be a unicast address.

**Multicast -** An IPv6 multicast address is used to send a single IPv6 packet to multiple destinations.

**Anycast -** An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address. Anycast addresses are beyond the scope of this course.

Unlike IPv4, IPv6 does not have a broadcast address.

1. **IP SUBNETTING**

Designing, implementing and managing an effective IP addressing plan ensures that networks can operate effectively and efficiently. This is especially true as the number of host connections to a network increases. Understanding the hierarchical structure of the IP address and how to modify that hierarchy in order to more efficiently meet routing requirements is an important part of planning an IP addressing scheme. In the original IPv4 address, there are two levels of hierarchy: a network and a host. These two levels of addressing allow for basic network groupings that facilitate in routing packets to a destination network. A router forwards packets based on the network portion of an IP address. When the network is located, the host portion of the address allows for identification of the destination device. However, as networks grow, with many organizations adding hundreds, and even thousands of hosts to their network, the two-level hierarchy is insufficient. A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s.

Subdividing a network adds a level to the network hierarchy, creating, in essence, three levels: a network, a subnetwork, and a host. Introducing an additional level to the hierarchy creates additional sub-groups within an IP network that facilitates faster packet delivery and added filtration, by helping to minimize ‘local’ traffic.

**Reasons for Subnetting**

Subnetting reduces overall network traffic and improves network performance. Subnetting helps you maintain clean separations within a network. It also enables an administrator to implement security policies such as which subnets are allowed or not allowed to communicate together. Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

There are various ways of using subnets to help manage network devices. Network administrators can group devices and services into subnets that are determined by:

* Location, such as floors in a building.
* Organizational unit.
* Device type.

**4.1 Types of Subnetting**

There are two types of Subnetting: FLSM and VLSM.

* FLSM (Fixed-Length Subnet Mask In), all subnets have an equal number of host addresses and use the same Subnet mask. FLSM is easy in implementation and simple in operation but wastes a lot of IP addresses.
* In VLSM (Variable-Length Subnet Mask), subnets have a flexible number of host addresses and use different subnet mask.

**Difference Between FLSM and VLSM**

|  |  |
| --- | --- |
| **FLSM (Fixed Length Subnet Masks)** | **VLSM (Variable Length Subnet Masks)** |
| 1. All subnets are equal in size. | 1. Subnets are variable in size. |
| 1. All subnets have equal number of hosts. | 1. Subnets have variable number of hosts. |
| 1. All subnets use same subnet mask. | 1. Subnets use different subnet masks. |
| 1. It is easy in configuration and administration. | 1. It is complex in configuration and administration. |
| 1. It wastes a lot of IP addresses. | 1. It wastes minimum IP addresses. |
| 1. It is also known as classfull Subnetting. | 1. It is also known as classless Subnetting. |
| 1. It supports both classfull and classless routing protocols. | 1. It supports only classless routing protocols. |

**4.2 VLSM**

VLSM stands for Variable Length Subnet Mask where the subnet design uses more than one mask in the same network which means more than one mask is used for different subnets of a single class A, B, C or a network. It is used to increase the usability of subnets as they can be of variable size. It is also defined as the process of subnetting of a subnet. The biggest advantage of VLSM Subnetting is that, instead of forcing us to use a fixed size for all segments, it allows us to choose the individual size for each segment. This flexibility reduces the IP wastage. We can choose the size of subnet which closely matches with our requirement.

**Basic concepts of VLSM Subnetting**

VLSM Subnetting is the extended version of FLSM Subnetting. In FLSM, all subnets use same block size, thus Subnetting is required only one time. In VLSM, subnets use block size based on requirement, thus Subnetting is required multiple times.

The concept of VLSM Subnetting is relatively simple.

* Select block size for each segment. Block size must be greater than or equal to the actual requirement. Actual requirement is the sum of host addresses, network address and broadcast address.
* Based on block size arrange all segments in descending order.
* Do FLSM Subnetting for the block size of the first segment.
* Assign first subnet from subnetted subnets to the first segment.
* If next segment has similar block size, assign next subnet to it.
* If next segment has lower block size, do FLSM Subnetting again for the block size of this segment.
* From subnetted subnets exclude the occupied subnets. Occupied subnets are the subnets which provide the addresses which are already assigned.
* From available subnets, assign the first available subnet to this segment.
* Repeat above steps till the last segment of the network.

**Classless Subnetting**

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

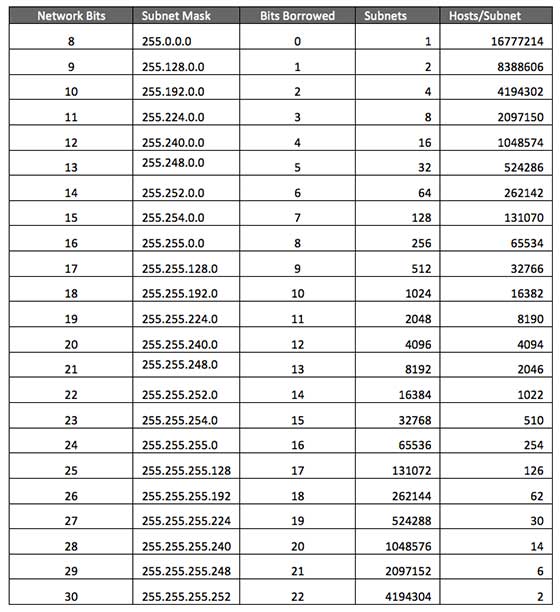
CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

**Class A Subnets**

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (21=2) with (223-2) 8388606 Hosts per Subnet.

The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets −



In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

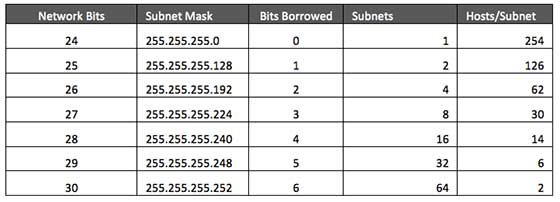
**Class B Subnets**

By default, using Classful Networking, 14 bits are used as Network bits providing (214) 16384 Networks and (216-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting −



**Class C Subnets**

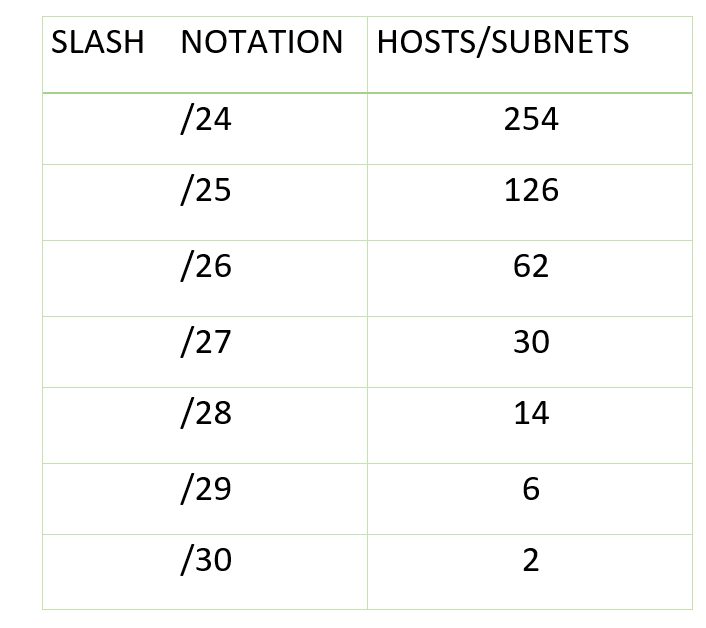
Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address −



**4.3 VLSM Example**

In VLSM, subnets use block size based on requirement so subnetting is required multiple times. Suppose there is an organization that has four departments to manage. These are sales and purchase department with 120 computers, development department with 50 computers, accounts department with 26 computers and management department with 5 computers. If the Network administrator has IP 192.168.1.0/24, department wise IPs can be allocated by following these steps:

1. For each segment select the block size that is greater than or equal to the actual requirement which is the sum of host addresses, broadcast addresses and network addresses. Make a list of subnets possible:

  
 **table –** possible subnets list

1. Arrange all the segments in descending order based on the block size that is from highest to lowest requirement.

Sales and Purchase: 120

Development: 50

Accounts: 26

Management: 5

3. The highest IP available has to be allocated to highest requirement so the sales and purchase department gets 192.168.1.0/25 which has 126 valid addresses that can easily be available for 120 hosts. The subnet mask used is 225.225.225.128

4. The next segment requires an IP to handle 50 hosts. The IP subnet with network number 192.168.1.128/26 is the next highest which can be assigned to 62 hosts thus fulfilling the requirement of development department. The subnet mask used is 255.255.255.192

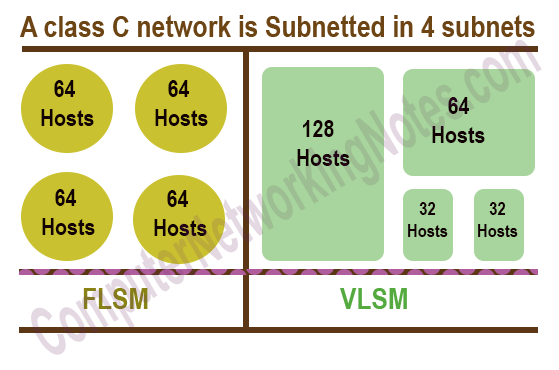
5. Similarly the next IP subnet 192.168.1.192/27 can fulfill the requirements of accounts department as it has 30 valid hosts IP which can be assigned to 26 computers.The mask used is 255.255.255.224

6. The last segment requires 5 valid hosts IP which can be fulfilled by the subnet 192.168.1.224/29 which has the mask as 255.255.255.248 is chosen as per the requirement. The IP with the mask 255.255.255.240 could be chosen but it has 14 valid hosts IPs and the requirement is less in comparison so the one that is comparable with the requirement is chosen.Thus there is less IP wastage in VLSM as compared to FLSM.

**4.4 Advantages of VLSM over FLSM**

* In Fixed length subnet mask subnetting (FLSM), all subnets are of equal size and have equal number of hosts but in VLSM the size is variable and it can have variable number of hosts thus making the IP addressing more efficient by allowing a routed system of different mask length to suit requirements.
* In FLSM there is a wastage of IP addresses but in VLSM there is a minimum wastage of IP addresses.
* FLSM is preferred for private IP addresses while for public IP addresses VLSM is the best option.

**Example**



1. **DESIGN METHODOLOGY**

**Physical topology diagrams** - Identify the physical location of intermediary devices and cable installation.

**Logical topology diagrams -** Identify devices, ports, and addressing scheme.

**5.1 Topology**



Network-1 Network-2 Network-3

Figure 4.1 Topology of Ip

We have designed a network for an organization by using IP Subnetting which consists of three networks: Network-1, Network-2 and Network-3. The requirement for an individual network are 100 systems in Network-1, 50 systems in Network-2 and 20 systems in Network-3. All the three individual networks are connected to a router which acts a default-gateway for ISP. Using a public IP 172.20.0 address we will give IP address by using Subnetting and make them individual networks. We have used a DHCP server in each network which issues an IP address automatically. If a user specifies the range of the IP address in the server then it automatically issues the IP address to each system in the network.

1. **TESTING AND TROUBLE SHOOTING NETWORK**

**Testing the connectivity using ping and tracert:**

To test connectivity to another host on a network, an echo request is sent to the host address using the ping command. Ping is used to test connectivity between two hosts but does not provide information about the details of devices between the hosts Traceroute (tracert) is a utility that generates a list of hops that were successfully reached along the path.

**6.1 Testing the Connectivity**

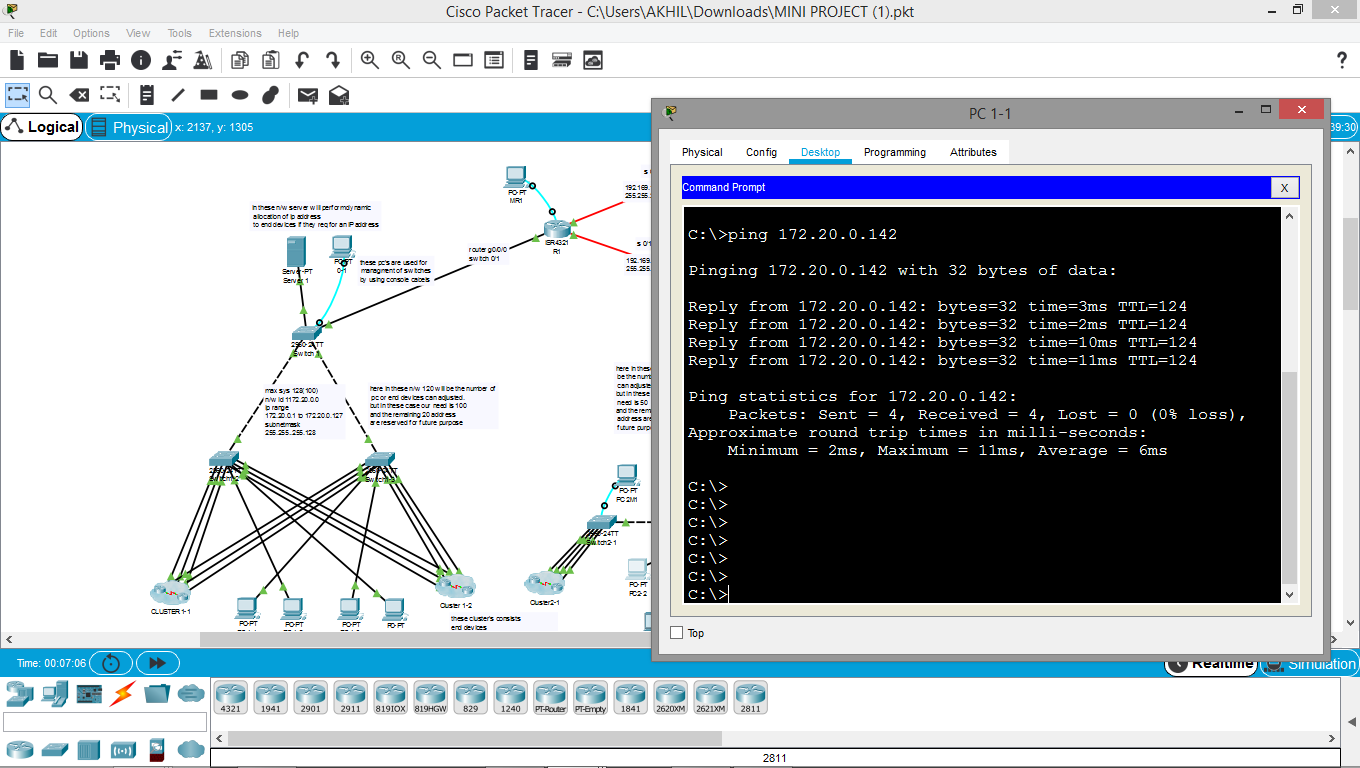


Figure 6.1: Testing the Connectivity

**6.2 Simulation**

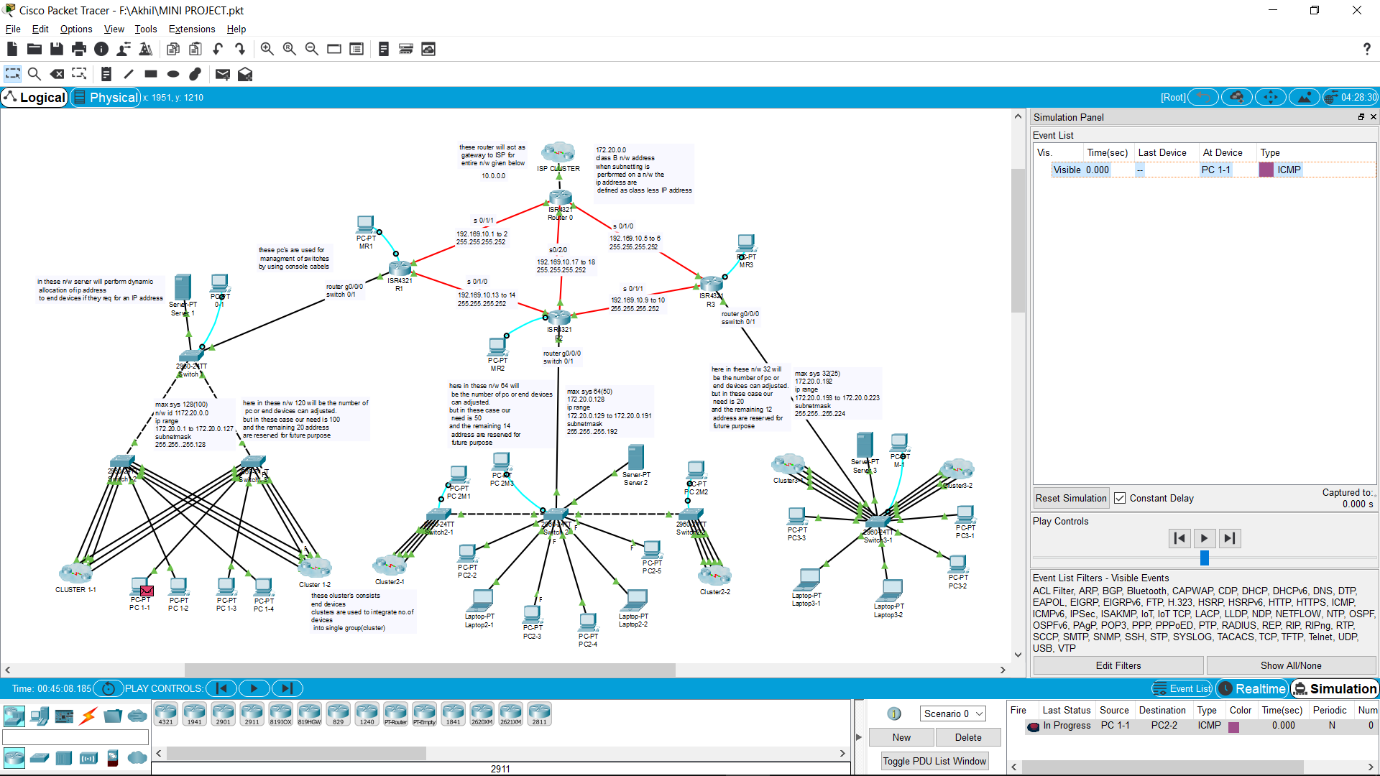


Figure 6.2.1: Simulation of ICMP Packet Moving from PC1-1

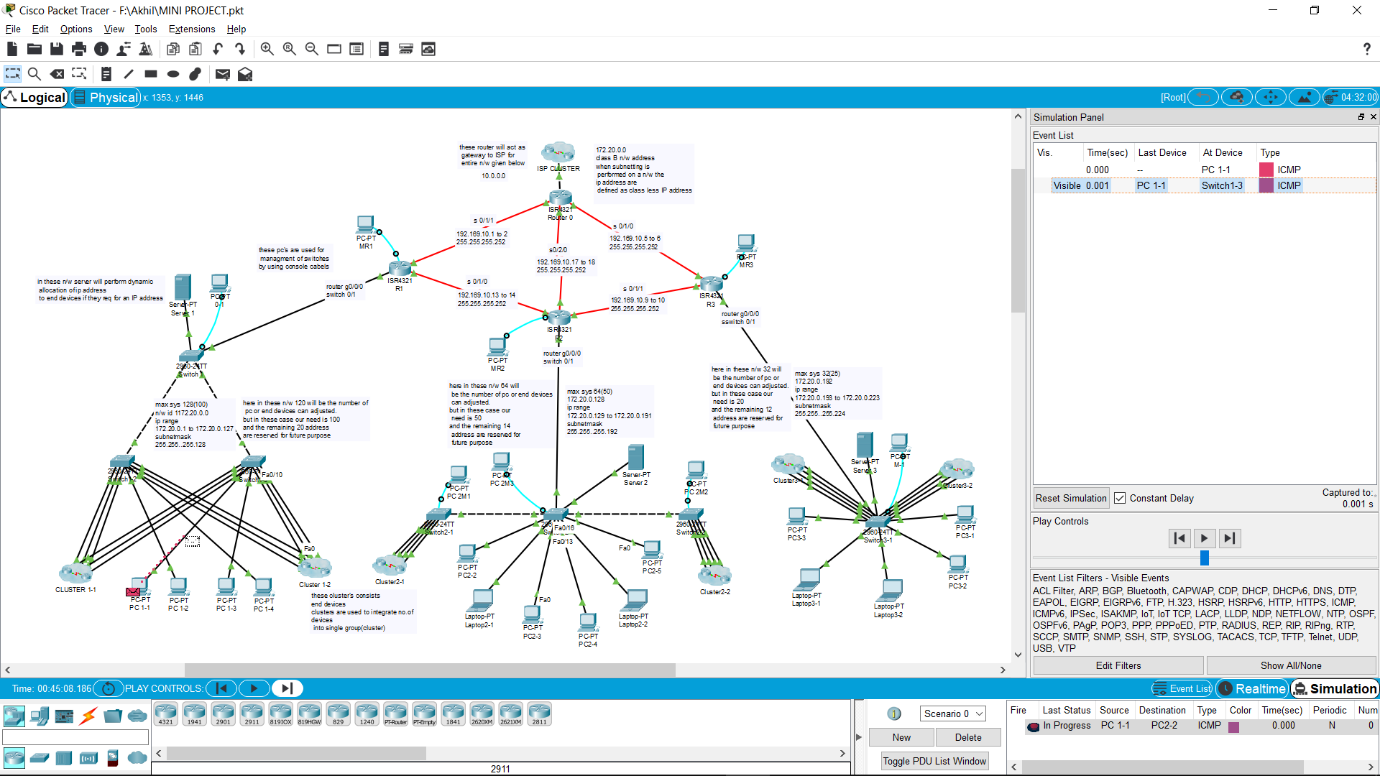


Figure 6.2.2: Simulation of ICMP Packet Moving from PC1-1 TO Switch 1-3

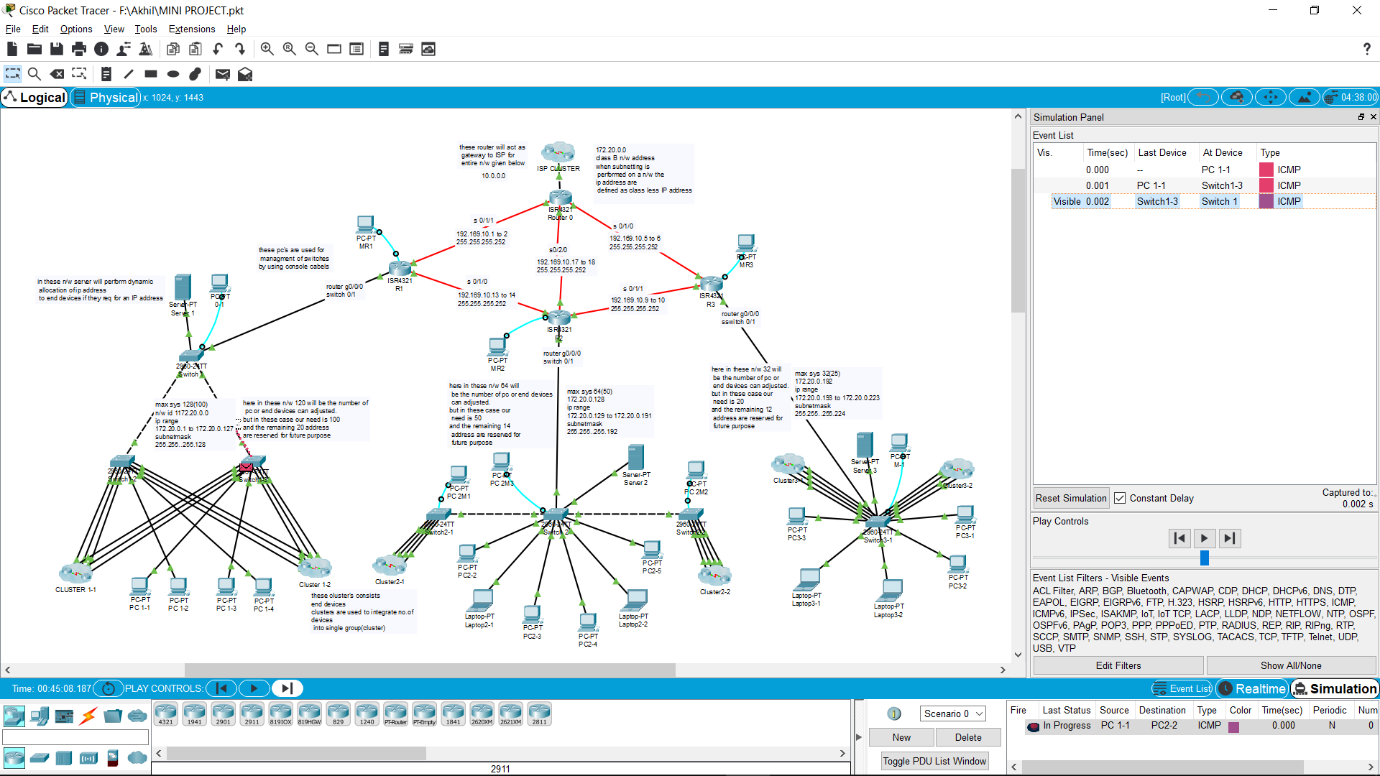


Figure 6.2.3: Simulation of ICMP Packet Moving from Switch 1-3 to Switch 1-1

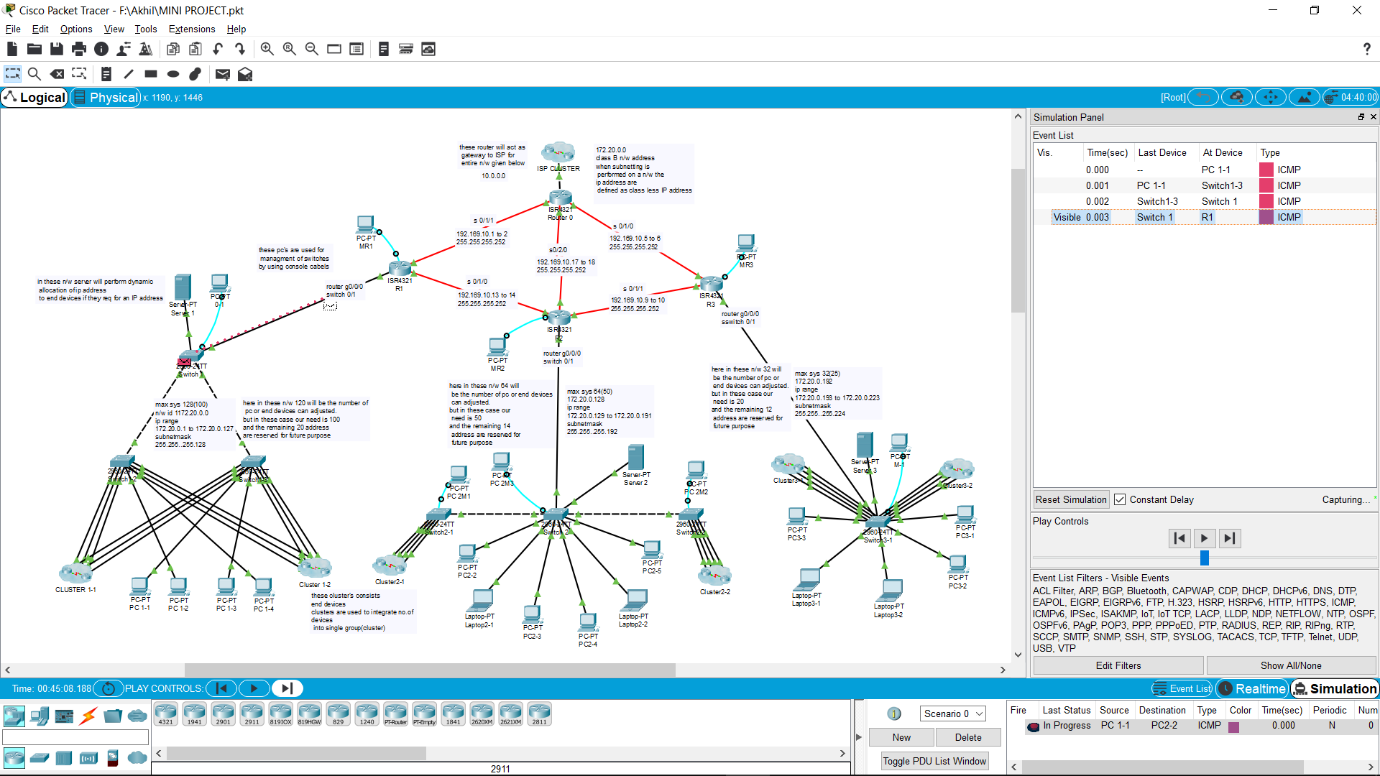


Figure 6.2.4: Simulation of ICMP Packet Moving from Switch 1-3 to Router R1

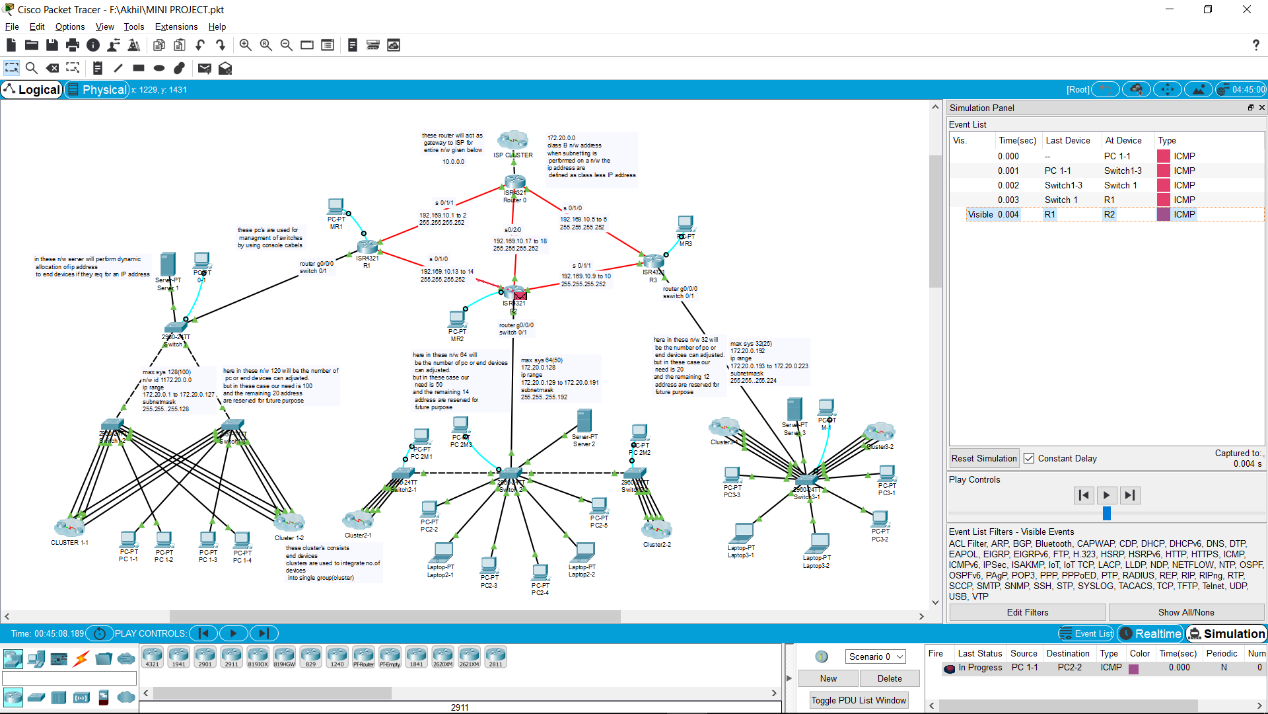


Figure 6.2.5: Simulation of ICMP Packet Moving from Router R1 TO R2

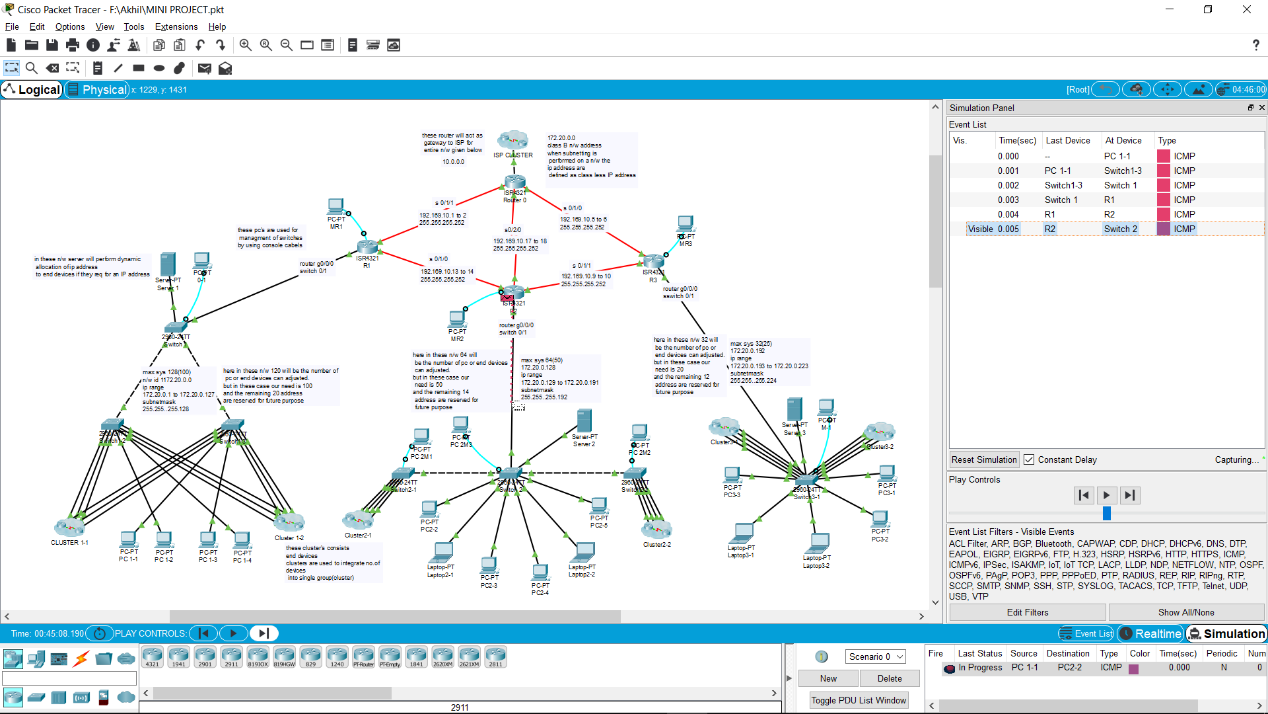


Figure 6.2.6: Simulation of ICMP Packet Moving from Router R2 to Switch 2-0

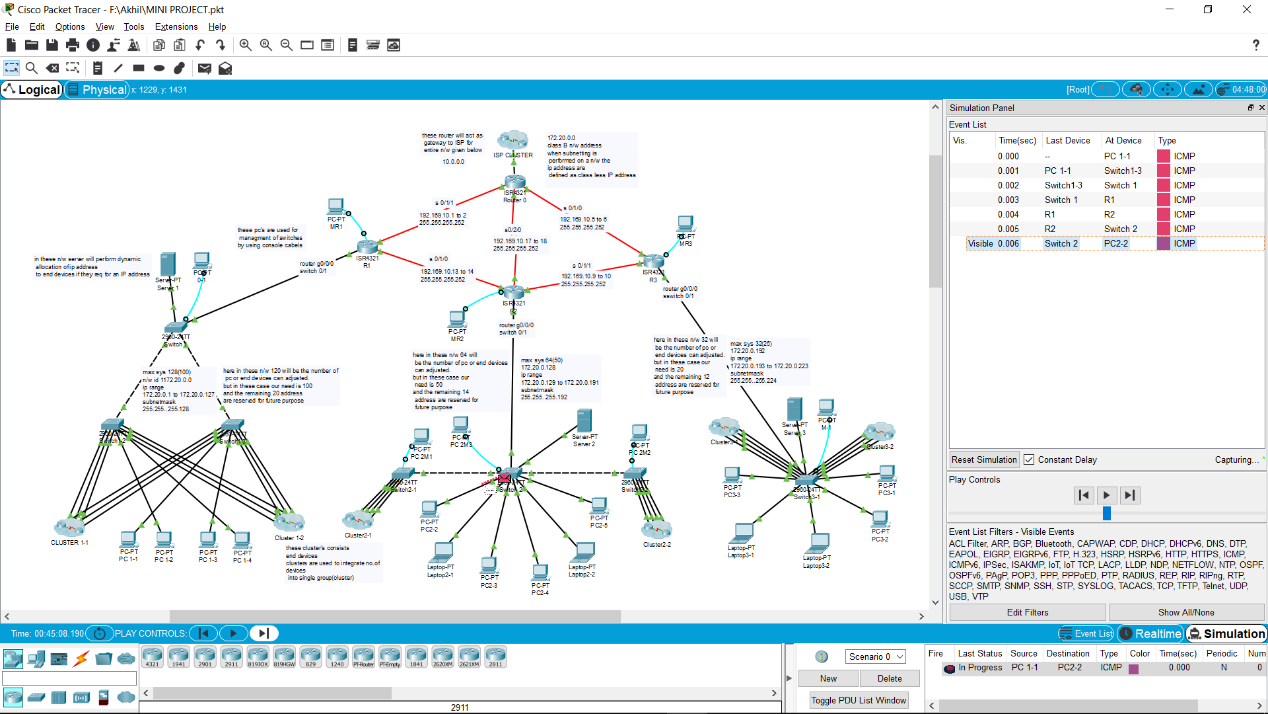


Figure 6.2.7: Simulation of ICMP Packet Moving from Switch 2-0 to PC-2

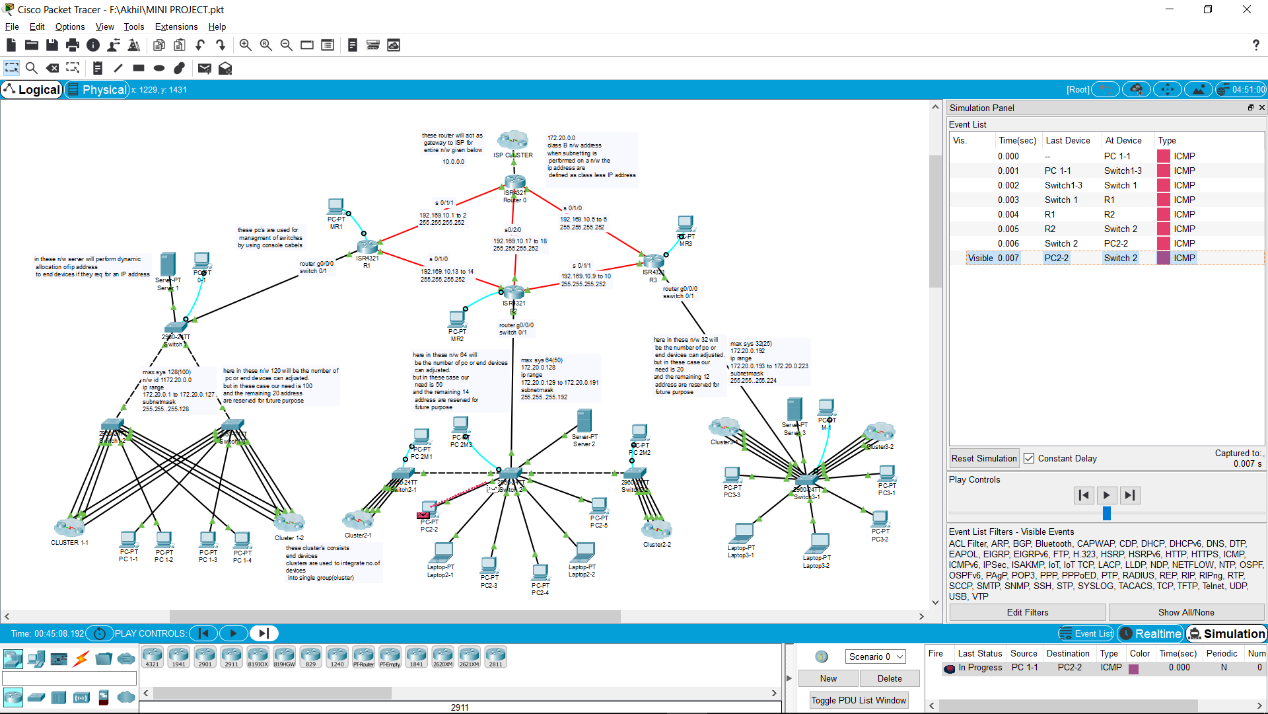


Figure 6.2.8: Acknowledgement from PC-2 to Switch 2-0

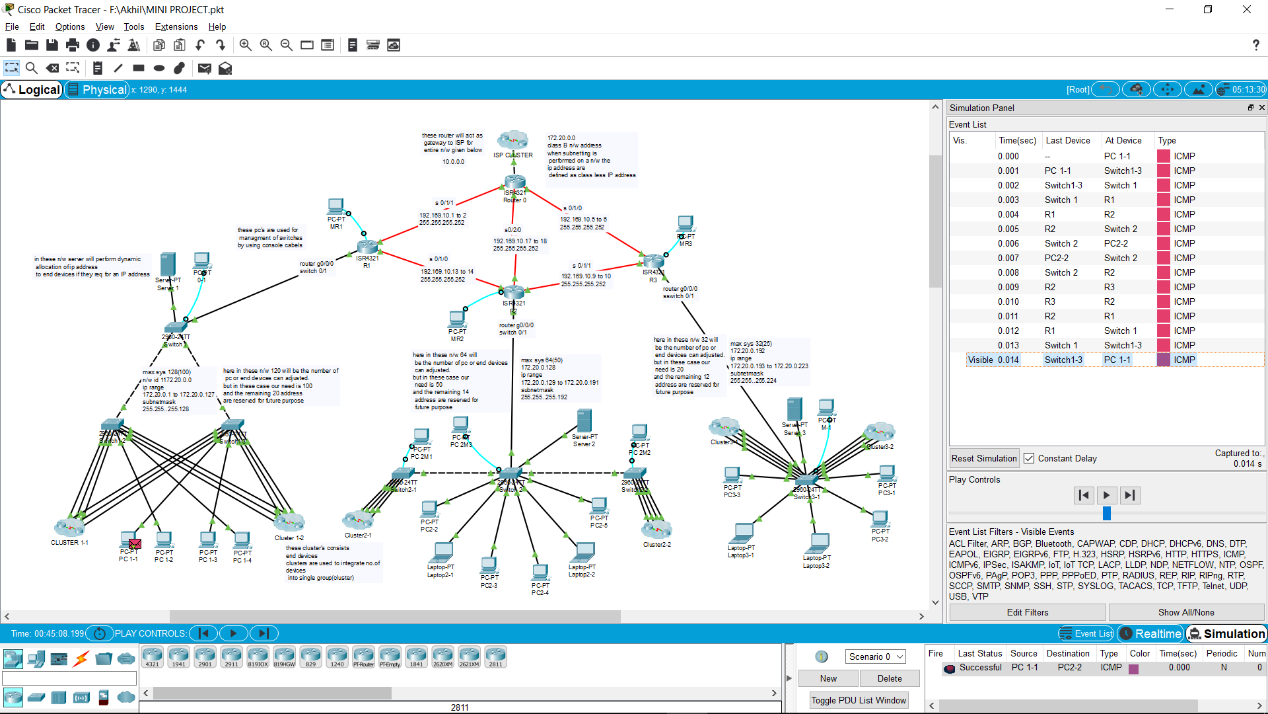


Figure 6.2.9: Acknowledgement By7 PC 1-1

**6.3 Tracing the route (tracert)**

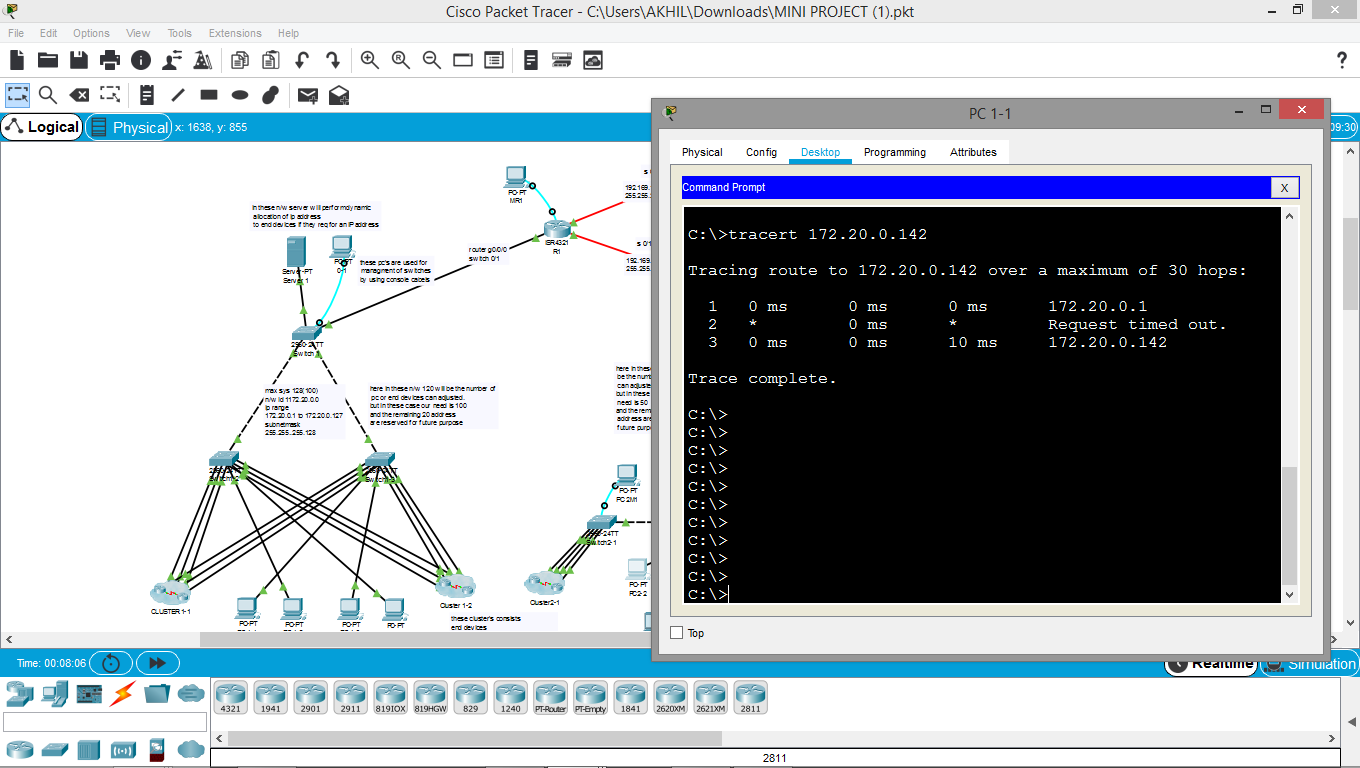


Figure 6.3: Tracing the route

**6.4 Trouble Shooting**

By using the show commands we can do the trouble shoot using packet tracer.

* Show commands
* Show version
* Show ipconfig
* Show ip interface brief
* Show running-config
* Show ip protocol

1. **RESULTS**

**7.1 Running Configuration of Router**

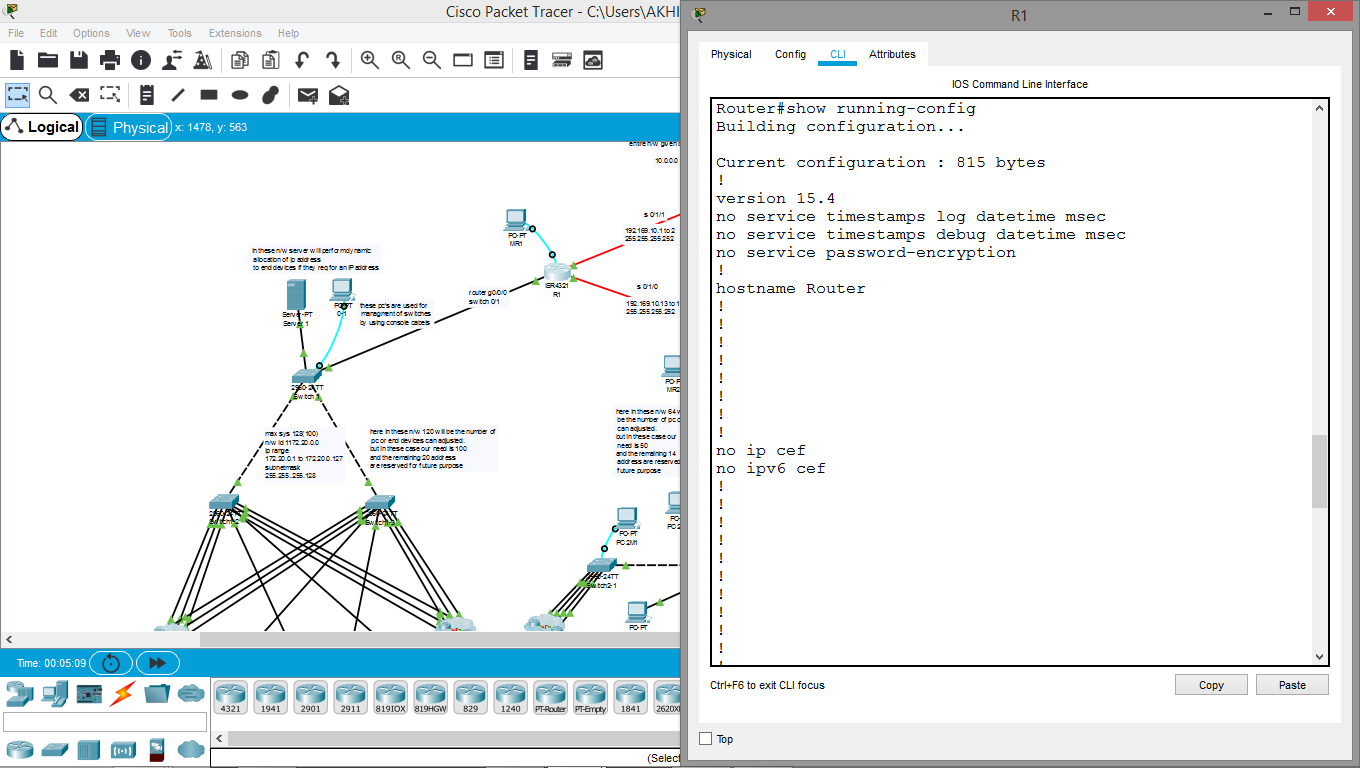


Figure 7.1.1: Running Configuration of Router1

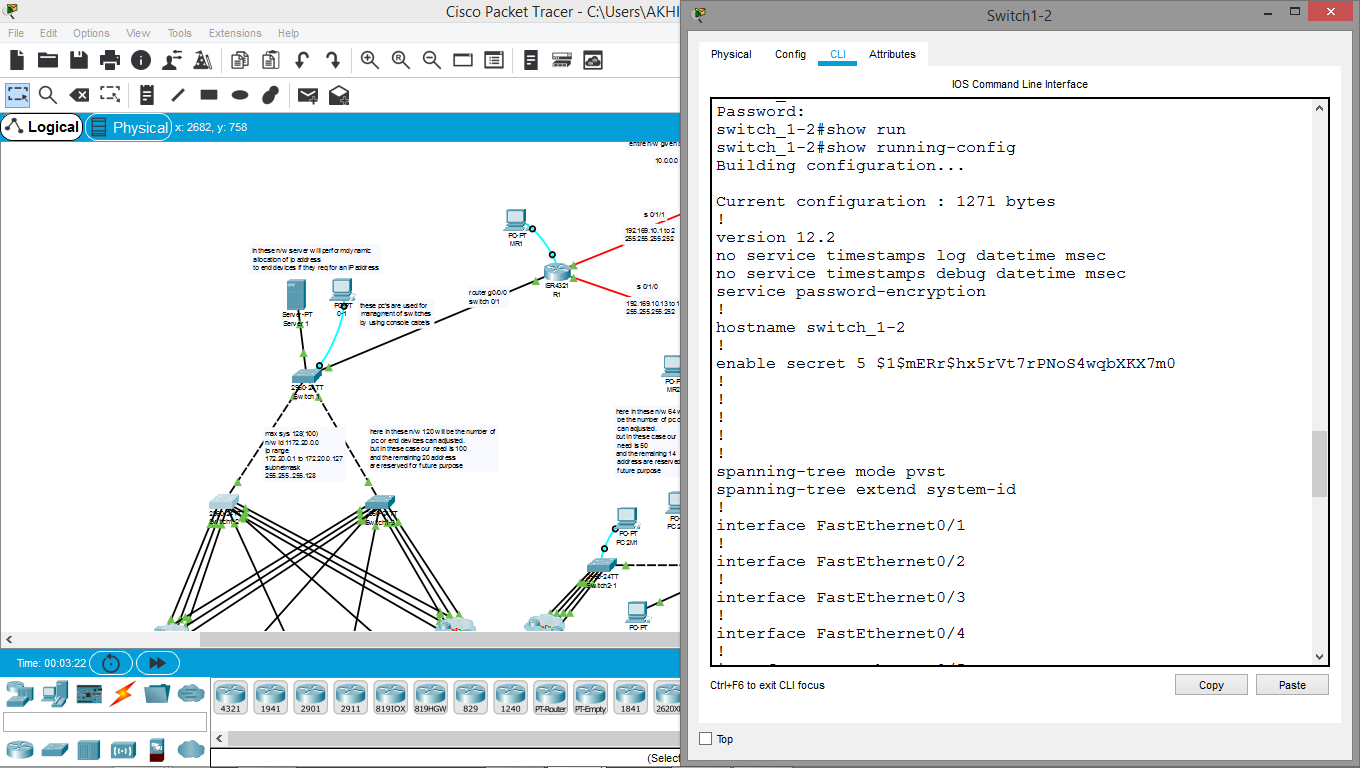


Figure 7.1.2: Running Configuration of switch\_1-2

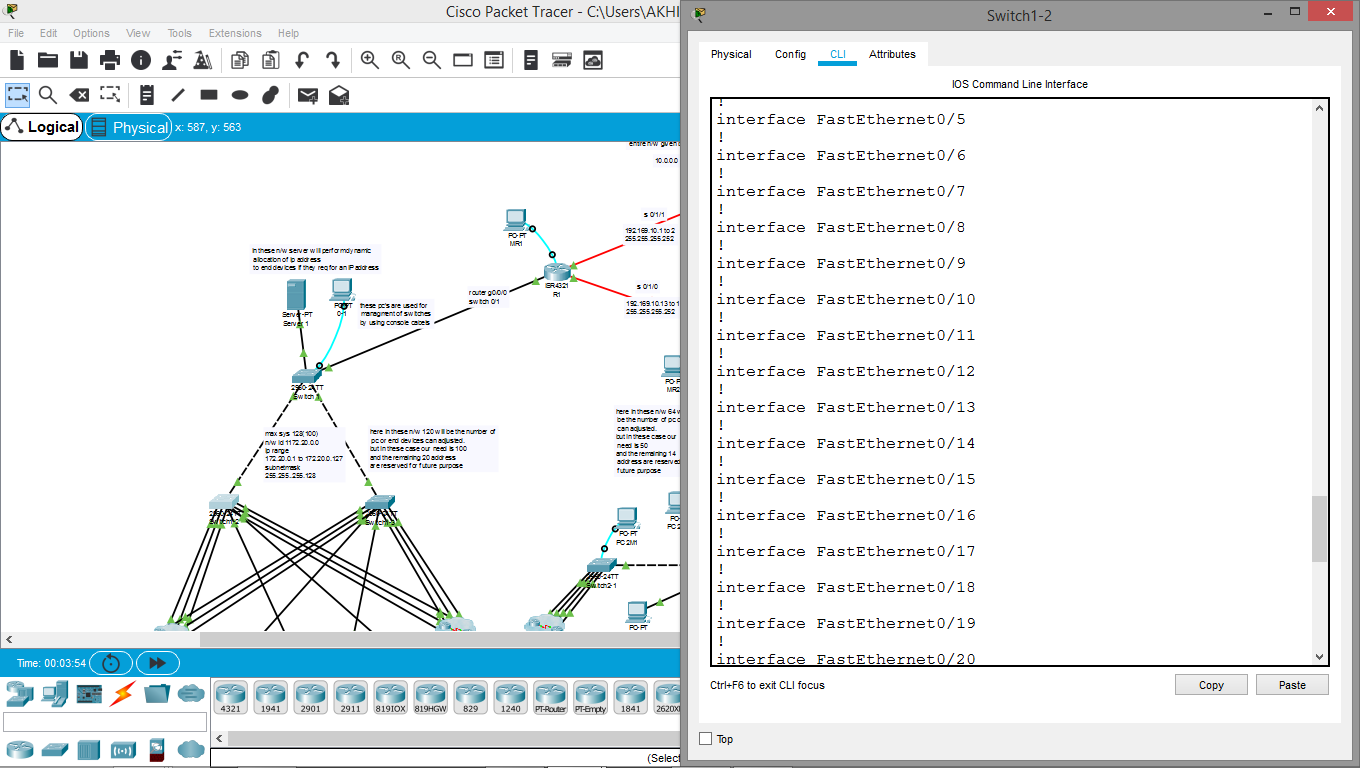


Figure 7.1.3: Running Configuration of 2switch 1\_2 interface

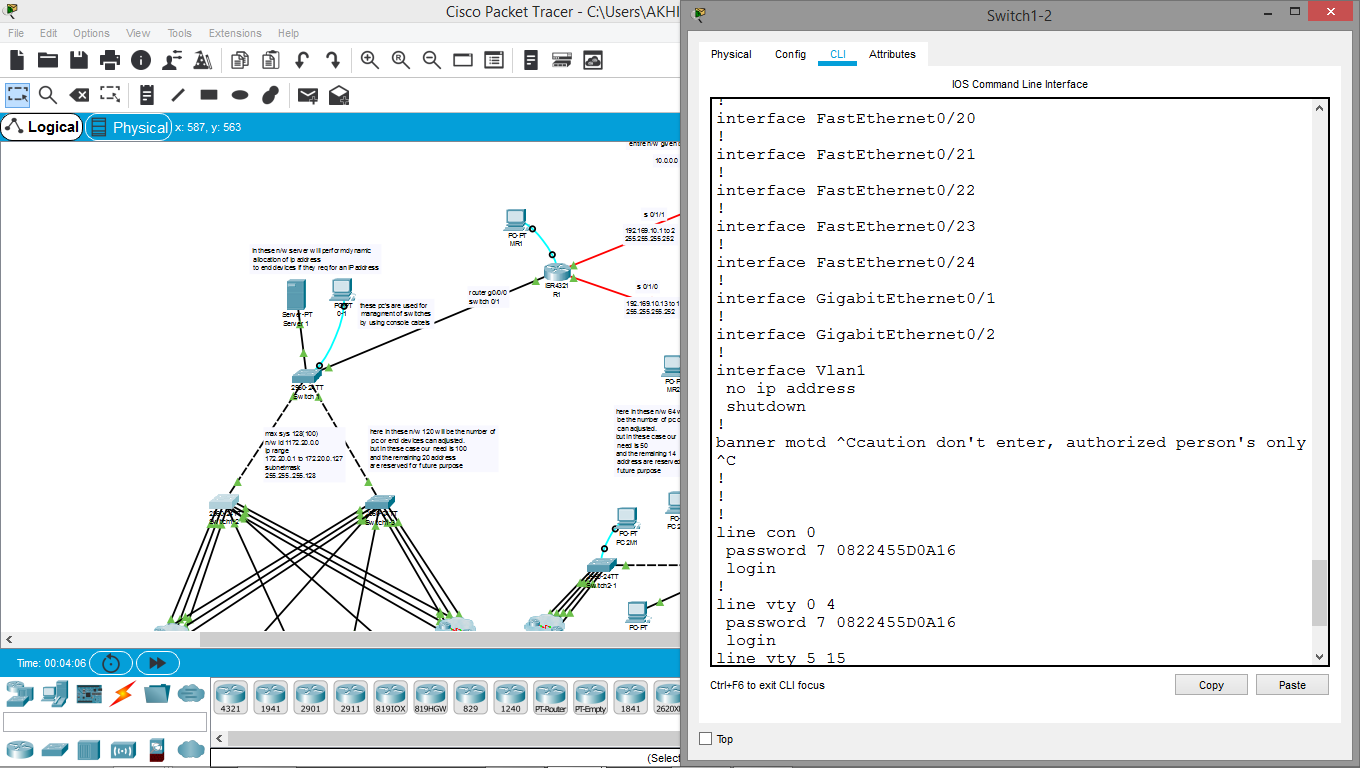


Figure 7.1.4: Running Configuration of 3switch 1\_2

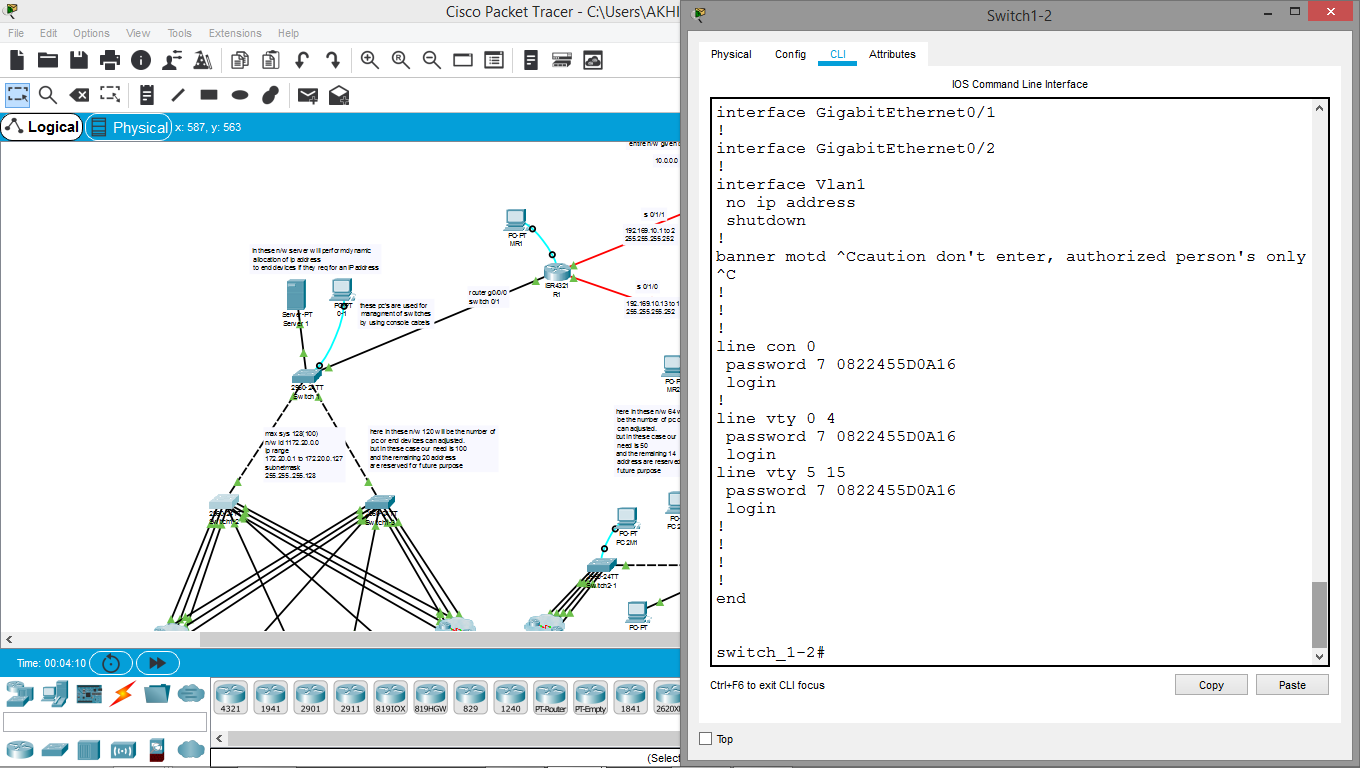


Figure 7.1.5: Running Configuration of 4switch 1\_2

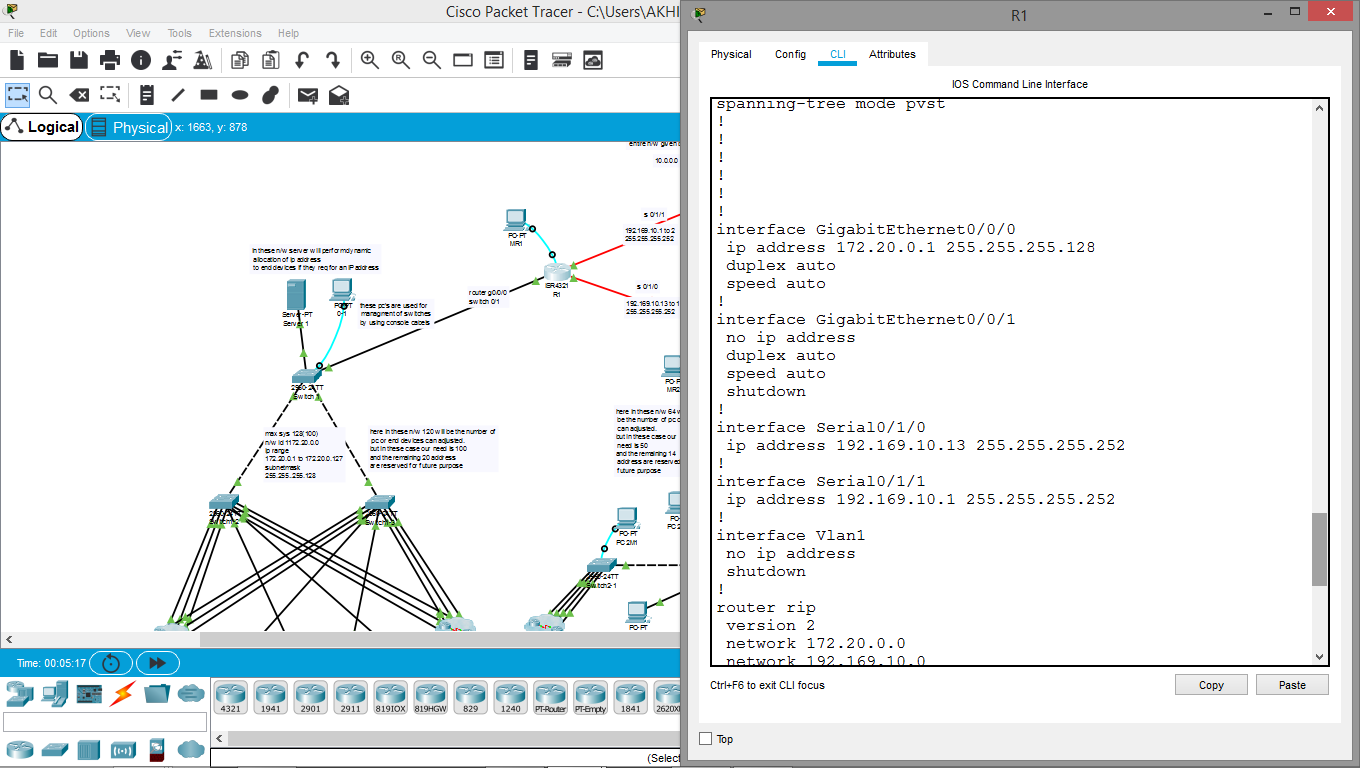


Figure 7.1.6: Running Configuration of 2 R1

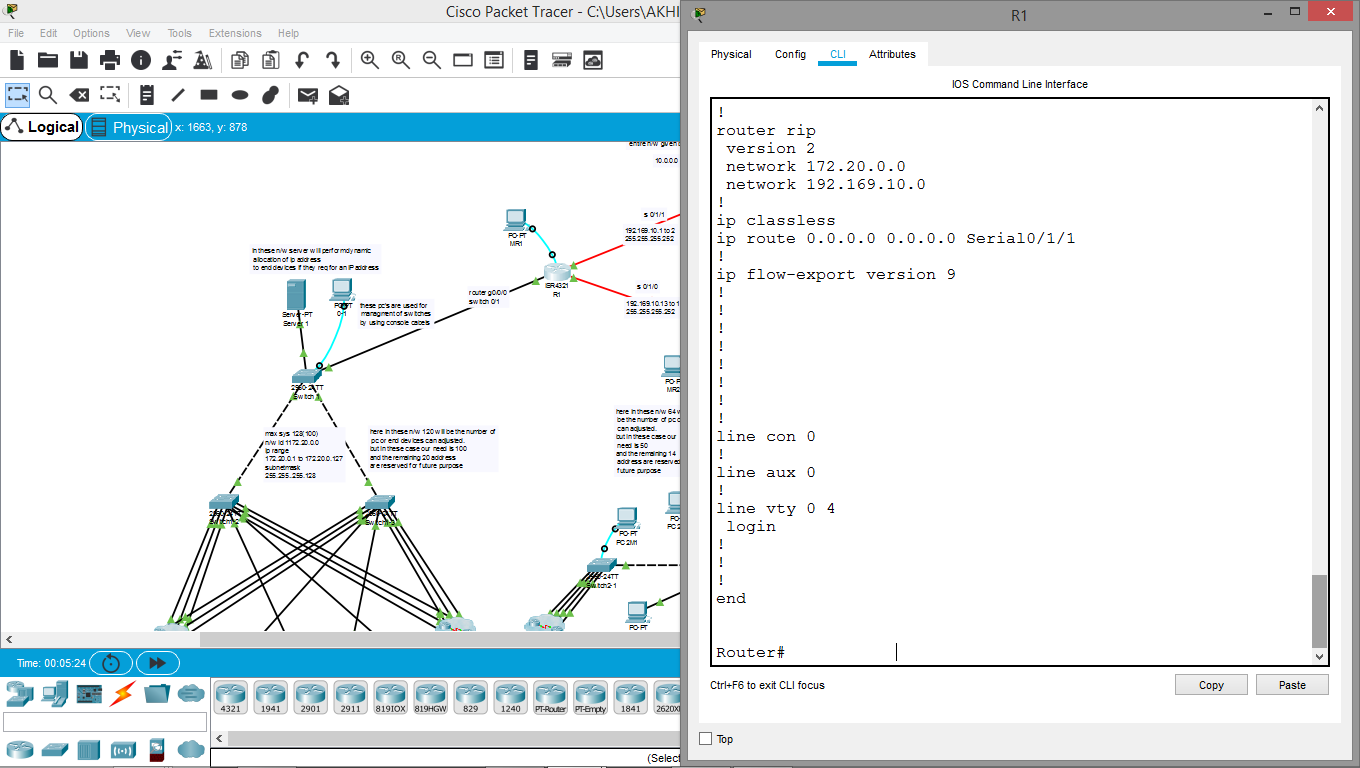


Figure 7.1.7: Running Configuration of 3 R1

1. **CONCLUSION**

The process of segmenting a network by dividing it into to multiple smaller network spaces is called subnetting. Every network address has a valid range of host addresses. All devices attached to the same network will have an IPv4 host address for that network and a common subnet mask or network prefix. Traffic can be forwarded between hosts directly if they are on the same subnet. Traffic cannot be forwarded between subnets without the use of a router. To determine if traffic is local or remote, the router uses the subnet mask. The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

IPv4 subnets are created by using one or more of the host bits as network bits. Two very important factors that will lead to the determination of the IP address block with the subnet mask are the number of subnets required, and the maximum number of hosts needed per subnet. Subnetting a subnet, or using Variable Length Subnet Mask (VLSM), was designed to avoid wasting addresses. in VLSM the size is variable and it can have variable number of hosts thus making the IP addressing more efficient by allowing a routed system of different mask length to suit requirements. In FLSM there is a wastage of IP addresses but in VLSM there is a minimum wastage of IP addresses.

**BIBILOGRAPHY**

1. Cisco Certified Network Associate Study Guide fifth edition by Todd Lammle

2. Data Communication and Computer Networks by Beroz Forozan.

3. www.netacad.com

4.www.cisco.com

5.www.google.com