

**Project Report**

**On**

**L2 and L3 Protocol And Security Implementation**

COMPLETED AT

HCL(Noida)

Submitted in the partial fulfillment of the requirement for the award of degree of

**Bachelors of Technology**

in

**Computer Science Engineering**

****

Under the guidance of Submitted By:

Dr. R.S Uppal Jaspreet Singh Kalsi

H.O.D Univ. roll no. - 1136365

|  |  |
| --- | --- |
|  |  |

**Certificate**

Certified that Jaspreet Singh Kalsi *(1136365),* student of Computer Science Engineering Department, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib in the partial fulfillment of the requirement for the award of Bachelors of Technology (Electronics & Communication Engineering) Degree of PTU, Jalandhar, is a record of students own study carried under my supervision & guidance.

This report has not been submitted to any other university or institution for the award of any degree.

Name of Project Guide

Miss. Rajan Pra Bohra

Professor

**Acknowledgement**

I wish to express my profound gratitude to the ALMIGHTY with whose grace and blessings, I have been able to complete another chapter of my life.

I would like to extend my appreciation to my industrial supervisor, Miss. Rajan Pra Bohra for their advices and patiently guiding me through while I working here as a trainee. Not forgotten for all the staffs working at (HCL Institue). I very much appreciate for their entire kindness helping and teaching me when I’m working there. I am very lucky to have such a helpful colleagues and I never felt left out in any situation.

I have learnt a lot of valuable things while working here. I realize that learning theoretical is never the same when it comes to practice. There are a lot more to master than just learning from book. For example it is impossible to master the etiquette of communicating with others from the book unless we put it in action. I also learned it is

very important to know how to work as part of the team especially when you are working in a big organization. In order to complete the task given timing is also another crucial thing to take care of. As is it known, the world of working is a completely different phase compared to the time when we are studying; therefore by going for an industrial training it is in hope that the students are well prepared and have high confidence to serve the community.

I am thankful to all the faculty members of CSE Department for the positive and co-operative response with time, energy and valuable suggestions they gave me to fulfill the task.

I find no words to acknowledge the sacrifice, love, help and inspiration rendered by my parents to take up this study.

With thanks to all,

Student name:JaspreetSinghkalsi

Semester – 5th

Branch- CSE

Univ. Roll No. – 1136365

Abstract

I have completed my six week training of Networking in HCL in noida,where I have learnt about Networking Devices(Cisco devices). Firstly our batch have undergone through the basics of Networking.Then we proceed with in depth study of Networking . Then we have started practical for our project i.e. L2 and L3 Protocols and Security Implementation.

We attended 3hrs regularly for just practical session only. We used network stimulator(Cisco Packet Tracer) for designing the network architecture. During designing the network Architecture,we have used networking concepts like subnetting,DHCP ,ISP,Routing protocols(OSPF),VLAN,VTP. Therefore we were ready for our project. My experience ther was realy pleasant, I worked ther with many students came from different universities.. having theoretical knowledge about project was not enough after implementing it on project we got in depth knowledge of controller.

It’s in our fortune to have such an excellent highly qualified trainee faculty which not only taught about networking but also relate it with real time applications. It was unforgettable experience in noida for me during training time.

CONTENT

* Introduction
* OSI Model
* Physical Layer
* Data Link Layer
* Network Layer
* Transport Layer
* Sessional Layer
* Presentation Layer
* Application Layer
* TCP/IP
* Basics of Networking
* Peer to peer
* Client-server
* Structured Cabling
* NIC
* Hub and Switches
* Wireless network
* Network Topologies
* Point-to-point
* Bus
* Star
* Ring or Circular
* Mesh
* Tree
* Hybrid
* Basic Routing Protocols
* Rip
* Ospf
* Eigrp
* DHCP
* PC is getting the I.P through DHCP Server
* Configuration of DHCP in Cisco Packet Tracer
* Configuration of Routing Protocol in Cisco Packet Tracer
* VLAN Configuration

|  |
| --- |
|  |

**L2 AND L3 PROTOCOL AND SECURITY IMPLEMENTATION**

**Introduction**

In the project “ L2 AND L3 PROTOCOL AND SECURITY IMPLEMENTATION ” ,the network architecture of differerent branches of hotel djukra is constructed.There are 6(six) branches of this hotel through out the world (i.e in Singapore,New-York,Florida ,Thailand,Delhi,Mumbai).The Network has made in such a way that any node(computer\laptop) of a particular branch can communicate with the another node of any branch.

In this project VLSM(Variable Length Subnet Mask) concept is used so that maximum ten thousand users can be connected to this particular network at each branch simultaneously without congestion and delays.

Fast Ethernet cables are used for connecting L2 and L3 Devices(i.e L2 and L3 Switches,Routers which provides excellent connectivity.

The DHCP technique is used at each branch which provides Dynamic I.P Addresses when a node tries to connect to the Internet.

In order to reduce the complexity , maintainence and chances of failures of servers they are place separately(i.e. they are not in directly connected to any branch of this hotel so if any server failes then its fault tracing will be easier).

From Security point of view, VLAN(i.e. Virtual Local Area Network) is implemented at each branch and every branch is divided into three VLAN that is VLAN-5,VLAN-6,VLAN-7 ,so that without Network Administrator’s permission no node of a particular VLAN can communicate with a node which is not at the same VLAN.

To increase the flexibility ,VTP(i.e VIRTUAL TRUNK PROTOCOL) technique is implemented so that any node of any VLAN as well as Branch can communicate with any node of any VLAN as well as Branch.

For implementing overseas communication,Multi-point Casting and Single point-Casting Cloud technique is used and this concept belongs to CCNP.

In order to decrease the hardware cost and efficiency ,the Multilayer –Switches are used.

Also to increase the reliability of the network, double Multilayer switches are implemented so in case if one doesn’t work then another will take its load.

Due to security point of view , main swich(primary Switch) of each branch is kept in SERVER’s mode and secondery Switches are kept in CLIENT’s mode.

**OSI MODEL**

The **Open Systems Interconnection (OSI) model**  is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO).

The model groups similar communication functions into one of seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer.

**DESCRIPTION OF OSI MODEL**

According to recommendation X.200, there are seven layers, labelled 1 to 7, with layer 1 at the bottom. Each layer is generically known as an N layer. An "N+1 entity" (at layer N+1) requests services from an "N entity" (at layer N).

At each level, two entities (N-entity peers) interact by means of the N protocol by transmitting protocol data units (PDU).

A service data unit (SDU) is a specific unit of data that has been passed down from an OSI layer to a lower layer, and which the lower layer has not yet encapsulated into a protocol data unit (PDU). An SDU is a set of data that is sent by a user of the services of a given layer, and is transmitted semantically unchanged to a peer service user.

The PDU at a layer N is the SDU of layer N-1. In effect the SDU is the 'payload' of a given PDU. That is, the process of changing an SDU to a PDU, consists of an encapsulation process, performed by the lower layer. All the data contained in the SDU becomes encapsulated within the PDU. The layer N-1 adds headers or footers, or both, to the SDU, transforming it into a PDU of layer N-1. The added headers or footers are part of the process used to make it possible to get data from a source to a destination.

**Layer 1: Physical Layer**

The physical layer defines electrical and physical specifications for devices. In particular, it defines the relationship between a device and a transmission medium, such as a copper or fiber optical cable.

Establishment and termination connection to a communications medium.

Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.

### Layer 2: Data Link layer

The data link layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer. Originally, this layer was intended for point-to-point and point-to-multipoint media, characteristic of wide area media in the telephone system.

Both WAN and LAN service arrange bits from the physical layer into logical sequences called frames. Not all physical layer bits necessarily go into frames, as some of these bits are purely intended for physical layer functions. For example, every fifth bit of the FDDI bit stream is not used by the layer.

### Layer 3: Network layer

The network layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network (in contrast to the data link layer which connects hosts within the same network), while maintaining the quality of service requested by the transport layer. The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer, sending data throughout the extended network and making the Internet possible. This is a logical addressing scheme values are chosen by the network engineer. The addressing scheme is not hierarchical.

### Layer 4: Transport Layer

The transport layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state- and connection-oriented. This means that the transport layer can keep track of the segments and retransmit those that fail. The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred.

### Layer 5: Session Layer

The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The session layer is commonly implemented explicitly in application environments that use remote procedure calls.

### Layer 6: Presentation Layer

The presentation layer establishes context between application-layer entities, in which the higher-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. If a mapping is available, presentation service data units are encapsulated into session protocol data units, and passed down the stack.

This layer provides independence from data representation (e.g., encryption) by translating between application and network formats. The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer.

### Layer 7: Application Layer

The Application Layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application-layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network or the requested communication exist. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer.

**TCP\IP**

The **Transmission Control Protocol** (**TCP**) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called *TCP/IP*. TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. It resides at the transport layer.

Web browsers use TCP when they connect to servers on the World Wide Web, and it is used to deliver email and transfer files from one location to another.

Applications that do not require the reliability of a TCP connection may instead use the connectionless User Datagram Protocol(UDP), which emphasizes low-overhead operation and reduced latency rather than error checking and delivery validation.

**NETWORK FUNCTION**

The protocol corresponds to the transport layer of TCP/IP suite. TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP). That is, when an application program desires to send a large chunk of data across the Internet using IP, instead of breaking the data into IP-sized pieces and issuing a series of IP requests, the software can issue a single request to TCP and let TCP handle the IP details.

IP works by exchanging pieces of information called packets. A packet is a sequence of octets and consists of a *header* followed by a *body*. The header describes the packet's source, destination and control information. The body contains the data IP is transmitting.

Due to network congestion, traffic load balancing, or other unpredictable network behavior, IP packets can be lost, duplicated, or delivered out of order. TCP detects these problems, requests retransmission of lost data, rearranges out-of-order data, and even helps minimize network congestion to reduce the occurrence of the other problems. Once the TCP receiver has reassembled the sequence of octets originally transmitted, it passes them to the receiving application. Thus, TCP abstracts the application's communication from the underlying networking details.

TCP is a reliable stream delivery service that guarantees that all bytes received will be identical with bytes sent and in the correct order. Since packet transfer over many networks is not reliable, a technique known as positive acknowledgment with retransmission is used to guarantee reliability of packet transfers. This fundamental technique requires the receiver to respond with an acknowledgment message as it receives the data. The sender keeps a record of each packet it sends. The sender also maintains a timer from when the packet was sent, and retransmits a packet if the timer expires before the message has been acknowledged. The timer is needed in case a packet gets lost or corrupted.

While IP handles actual delivery of the data, TCP keeps track of the individual units of data transmission, called *segments*, that a message is divided into for efficient routing through the network. For example, when an HTML file is sent from a web server, the TCP software layer of that server divides the sequence of octets of the file into segments and forwards them individually to the IP software layer (Internet Layer). The Internet Layer encapsulates each TCP segment into an IP packet by adding a header that includes (among other data) the destination IP address. When the client program on the destination computer receives them, the TCP layer (Transport Layer) reassembles the individual segments and ensures they are correctly ordered and error free as it streams them to an application.

**Basic of Networking**

A computer network consists of a collection of computers, printers and other equipment that is connected together so that they can communicate with each other (see Advice Sheet 17 on the ICT Planning for Corporate Sector or Industry pack). Fig 1 gives an example of a network in a school comprising of a local area network or LAN connecting computers with each other, the internet, and various servers.

Local Area

Network’ (LAN)

Modem or Router

Access to:

Internet content

Cache, Proxy,

Filtering, Firewall

Server

Users

computers

Other users,

computers

File and Print Server

CD or Multimedia Servers

Printers etc.

**Fig 1: Representation of Network in a school.**

Broadly speaking, there are two types of network configuration, peer-to-peer networks and client/server networks.

**Peer-to-peer Networks**

**Peer-to-peer networks** are more commonly implemented where less then ten computers are involved and where strict security is not necessary. All computers have the same status, hence the term 'peer', and they communicate with each other on an equal footing. Files, such as word processing or spreadsheet documents, can be shared across the network and all the computers on the network can share devices, such as printers or scanners, which are connected to any one computer.

Peer to Peer

Network

**Fig 2: Peer to Peer Networking**

**Client/server networks**

**Client/server networks** are more suitable for larger networks. A central computer, or 'server', acts as the storage location for files and applications shared on the network. Usually the server is a higher than average performance computer. The server also controls the network access of the other computers which are referred to as the 'client' computers. Typically, teachers and students in a school will use the client computers for their work and only the network administrator (usually a designated staff member) will have access rights to the server.

File Server

Other equipment

**Fig 3: Client - Server Networking**

**Structured Cabling**

The two most popular types of structured network cabling are **twisted-pair** (also known as **10BaseT**) and **thin coax** (also known as **10Base2**). 10BaseT cabling looks like ordinary telephone wire, except that it has 8 wires inside instead of 4. Thin coax looks like the copper coaxial cabling that's often used to connect a Video Recorder to a TV.

**10BaseT Cabling**

When 10BaseT cabling is used, a strand of cabling is inserted between each computer and a hub. If you have 5 computers, you'll need 5 cables. Each cable cannot exceed 325 feet in length. Because the cables from all of the PCs converge at a common point, a 10BaseT network forms a **star configuration**.

[](http://www.cablewarehouse.co.uk/catalog/default.php?cPath=21_33) [](http://www.cablewarehouse.co.uk/catalog/product_info.php?products_id=1268)

Fig 4a: Cat5e Cable and a close up of RJ-45 connector

**Network Interface Card (NIC)**

A NIC (pronounced 'nick') is also known as a network card. It connects the computer to the cabling, which in turn links all of the computers on the network together. Each computer on a network must have a network card. Most modern network cards are 10/100 NICs and can operate at either 10Mbps or 100Mbps.

Only NICs supporting a minimum of 100Mbps should be used in new installations schools.

Computers with a wireless connection to a network also use a network card (see Advice Sheet 20 for more information on wireless networking).

[](http://www.cablewarehouse.co.uk/catalog/default.php?cPath=22_50) [](http://www.linksys.com/products/product.asp?prid=31&scid=30)

Fig 5: Network Interface Cards (NICs)

**Hub and Switch**

A hub is a device used to connect a PC to the network. The function of a hub is to direct information around the network, facilitating communication between all connected devices. However in new installations switches should be used instead of hubs as they are more effective and provide better performance. A switch, which is often termed a 'smart hub'.

Switches and hubs are technologies or ‘boxes’ to which computers, printers, and other networking devices are connected. Switches are the more recent technology and the accepted way of building today's networks. With switching, each connection gets "dedicated bandwidth" and can operate at full speed. In contrast, a hub shares bandwidth across multiple connections such that activity from one PC or server can slow down the effective speed of other connections on the hub.

Now more affordable than ever, Dual-speed 10/100 autosensing switches are recommended for all school networks. Corporate Sector or Industry may want to consider upgrading any hub based networks with switches to improve network performance – ie speed of data on the network.



Fig 6a: An 8 port Hub

 3Com® SuperStack® 3 Switch 4400 SE 24-Port

Fig 6b: 2 Examples of 24 port Switches

**Wireless Networks**

The term 'wireless network' refers to two or more computers communicating using standard network rules or protocols, but without the use of cabling to connect the computers together. Instead, the computers use wireless radio signals to send information from one to the other. A wireless local area network (WLAN) consists of two key components: an access point (also called a base station) and a wireless card. Information can be transmitted between these two components as long as they are fairly close together (up to 100 metres indoors or 350 metres outdoors).



Fig 7a: Wireless Access point or Wireless Basestation

Suppliers would need to visit the Corporate Sector or Industry and conduct a site survey. This will determine the number of base stations you need and the best place(s) to locate them. A site survey will also enable each supplier to provide you with a detailed quote. It is important to contact a number of different suppliers as prices, equipment and opinions may vary. When the term 'wireless network' is used today, it usually refers to a wireless local area network or WLAN. A WLAN can be installed as the sole network in a school or building. However, it can also be used to extend an existing wired network to areas where wiring would be too difficult or too expensive to implement, or to areas located away from the main network or main building. Wireless networks can be configured to provide the same network functionality as wired networks, ranging from simple peer-to-peer configurations to large-scale networks accommodating hundreds of users.

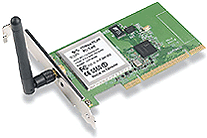
 

Fig 7b : Desktop PC Wireless LAN card Fig 7c : Laptop PC Wireless LAN card

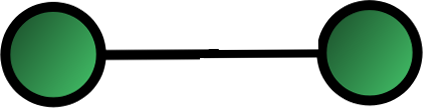
**Network topology**

It is the arrangement of the various elements (links, nodes, etc.) of a computer or biological network. Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

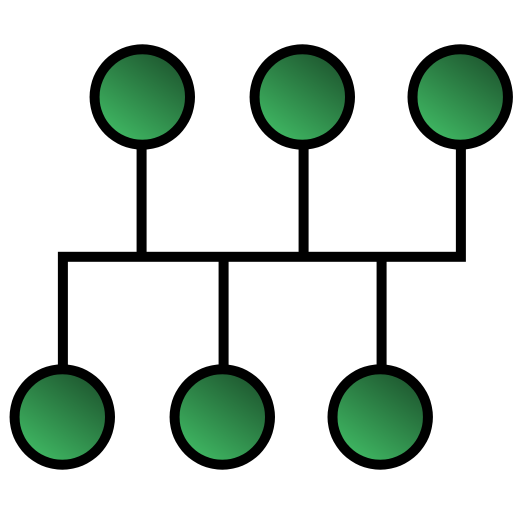
There are eight basic topologies:

1. Point-to-point
2. Bus
3. Star
4. Ring or circular
5. Mesh
6. Tree
7. Hybrid
8. **Point-to-point**

The simplest topology is a permanent link between two endpoints. Switched point-to-point topologies are the basic model of conventional telephony. The value of a permanent point-to-point network is unimpeded communications between the two endpoints. The value of an on-demand point-to-point connection is proportional to the number of potential pairs of subscribers, and has been expressed as Metcalfe's Law.



1. **Bus**



In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.

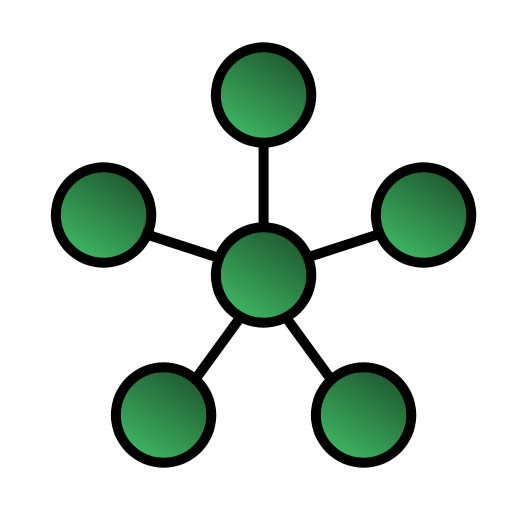
* **Linear bus**

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

* **Distributed bus**

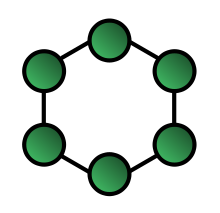
The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same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

1. **Star**

****

In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch. The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device. All traffic that traverses the network passes through the central hub. The hub acts as a signal repeater. The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the hub represents a single point of failure.

1. **Ring**

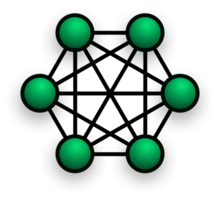


A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the right acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring. The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link.

**5.MESH**

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

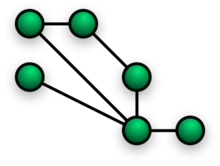
**Fully connected**

[](http://en.wikipedia.org/wiki/File:NetworkTopology-FullyConnected.png)

The number of connections in a full mesh = n(n - 1) / 2.

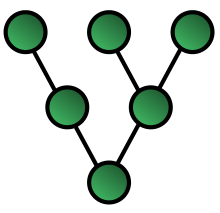
The physical fully connected mesh topology is generally too costly and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected (see Combinatorial explosion).

**Partially connected**

[](http://en.wikipedia.org/wiki/File:NetworkTopology-Mesh.png)

The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

**6. Tree**



The type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy (The hierarchy of the tree is symmetrical.) Each node in the network having a specific fixed number, of nodes connected to it at the next lower level in the hierarchy, the number, being referred to as the 'branching factor' of the hierarchical tree. This tree has individual peripheral nodes.

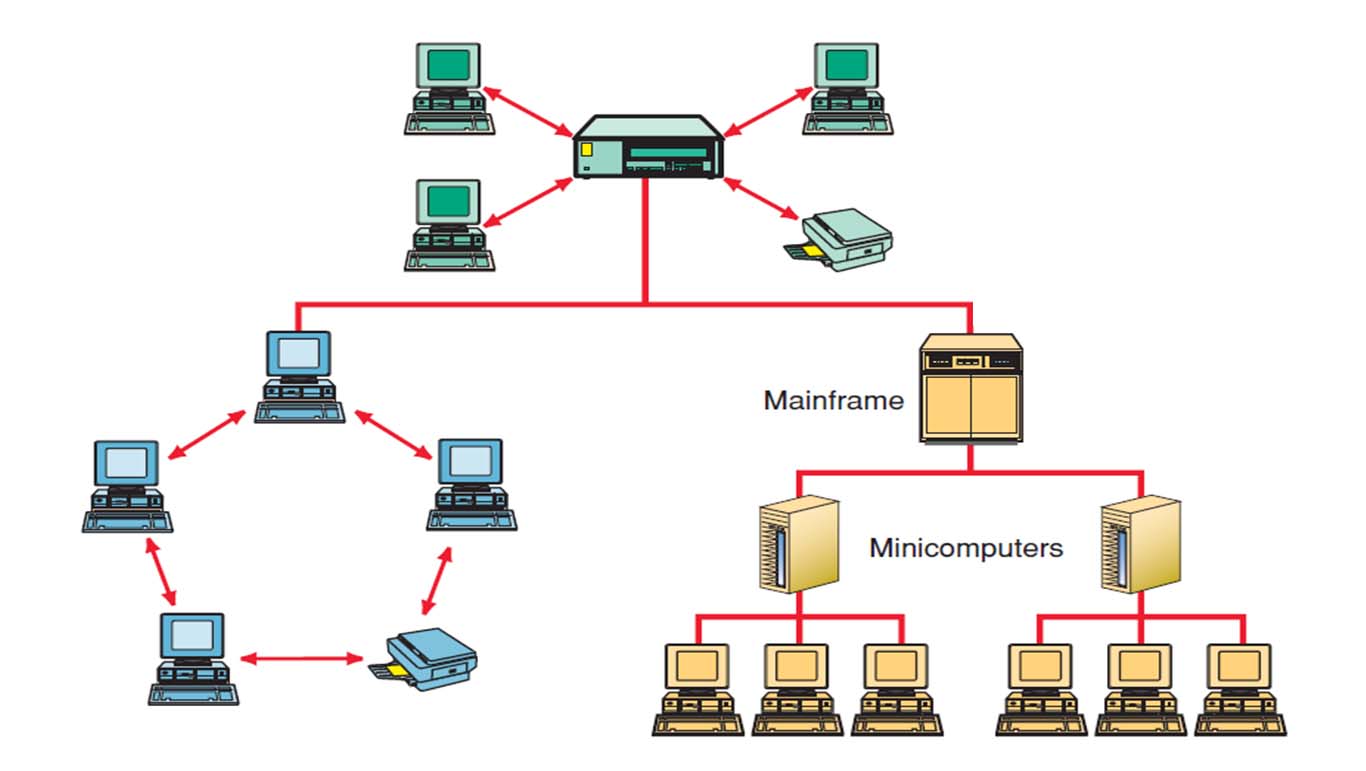
1. A network that is based upon the physical hierarchical topology must have at least three levels in the hierarchy of the tree, since a network with a central 'root' node and only one hierarchical level below it would exhibit the physical topology of a star.
2. The branching factor, f, is independent of the total number of nodes in the network and, therefore, if the nodes in the network require ports for connection to other nodes the total number of ports per node may be kept low even though the total number of nodes is large – this makes the effect of the cost of adding ports to each node totally dependent upon the branching factor and may therefore be kept as low as required without any effect upon the total number of nodes that are possible.
3. If the nodes in a network that is based upon the physical hierarchical topology are required to perform any processing upon the data that is transmitted between nodes in the network, the nodes that are at higher levels in the hierarchy will be required to perform more processing operations on behalf of other nodes than the nodes that are lower in the hierarchy. Such a type of network topology is very useful and highly recommended.

**6.Hybrid**

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

* A Star-ring network consists of two or more star topologies connected using a multi-station access unit (MAU) as a centralized hub.
* A Star Bus network consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network's backbone).

**Hybrid Network**



**Introduction to Routing Protocols**

**Routing** is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks.

In packet switching networks, routing directs packet forwarding (the transit of logically addressed packets from their source toward their ultimate destination) through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

In case of overlapping/equal routes, the following elements are considered in order to decide which routes get installed into the routing table (sorted by priority):

1. **Prefix-Length**: where longer subnet masks are preferred (independent if it is within a routing protocol or over different routing protocol)
2. **Metric**: where a lower metric/cost is preferred (only valid within one and the same routing protocol)
3. **Administrative distance**: where a lower distance is preferred (only valid between different routing protocols.

## Basic Routing Protocol families

### Distance vector routing protocols

In distance vector routing protocols, every host maintains a routing table containing the distance from itself to possible destinations. Each routing table entry contains the next hop to the destination and the distance to the destination. Nodes only feed the estimated link costs for each destination (e.g. the number of hops to destination) to their neighbors, instead of flooding the whole network. All nodes calculate the shortest paths to the destinations using that broadcasted information.

**Routing Information Protocol** (**RIP)**

The **Routing Information Protocol** (**RIP**) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

RIP implements the split horizon, route poisoning and holddown mechanisms to prevent incorrect routing information from being propagated. These are some of the stability features of RIP. It is also possible to use the Routing Information Protocol with Metric-Based Topology (RMTI) algorithm to cope with the count-to-infinity problem. With RMTI, it is possible to detect every possible loop with a very small computation effort.

### RIP version 1

The original specification of RIP,uses clasfull routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size. There is also no support for router authentication, making RIP vulnerable to various attacks.

### RIP version 2

Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993[]](http://en.wikipedia.org/wiki/Routing_Information_Protocol#cite_note-5) and last standardized in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all *Must Be Zero* protocol fields in the RIPv1 messages are properly specified. In addition, a *compatibility switch* featureallows fine-grained interoperability adjustments.

**OPEN SHOREST PATH FIRST**

**Open Shortest Path First** (**OSPF**) is a link-state routingprotocol for InterneProtocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).

OSPF is perhaps the most widely used Interior gateway protocol (IGP) in large enterprise networks. IS-IS, another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet.

OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets. OSPF was designed to support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing(CIDR) addressing models.

OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure within seconds. It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm.

The OSPF routing policies to construct a route table are governed by link cost factors (*external metrics*) associated with each routing interface. Cost factors may be the distance of a router (round-trip time), network throughput of a link, or link availability and reliability, expressed as simple unitless numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

OSPF does not use a TCP/IP transport protocol (UDP, TCP), but is encapsulated directly in IP datagrams with protocol number 89. This is in contrast to other routing protocols, such as the Routing Information Protocol (RIP), or the Border Gateway Protocol (BGP). OSPF handles its own error detection and correction functions.

OSPF uses multicast addressing for route flooding on a broadcast domain. For non-broadcast networks special provisions for configuration facilitate neighbor discovery.

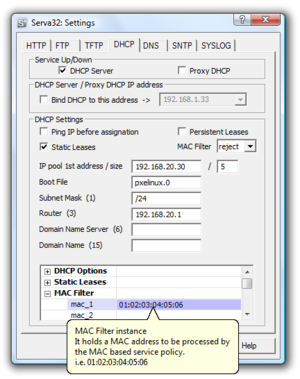
**Enhanced Interior Gateway Routing Protocol**

The Enhanced Interior Gateway Routing Protocol (EIGRP) represents an evolution from its predecessor IGRP (refer to Interior Gateway Routing Protocol). This evolution resulted from changes in networking and the demands of diverse, large-scale internetworks. EIGRP integrates the capabilities of link-state protocols into distance vector protocols. Additionally, EIGRP contains several important protocols that greatly increase its operational efficiency relative to other routing protocols. One of these protocols is the Diffusing update algorithm (DUAL) developed at SRI International by Dr. J.J. Garcia-Luna-Aceves. DUAL enables EIGRP routers to determine whether a path advertised by a neighbor is looped or loop-free, and allows a router running EIGRP to find alternate paths without waiting on updates from other routers.

EIGRP provides compatibility and seamless interoperation with IGRP routers. An automatic-redistribution mechanism allows IGRP routes to be imported into EIGRP, and vice versa, so it is possible to add EIGRP gradually into an existing IGRP network. Because the metrics for both protocols are directly translatable, they are as easily comparable as if they were routes that originated in their own autonomous systems (ASs). In addition, EIGRP treats IGRP routes as external routes and provides a way for the network administrator to customize them.

This article provides an overview of the basic operations and protocol characteristics of EIGRP.

**DYNAMIC HOST CONFIGURATION PROTOCOL**

[](http://en.wikipedia.org/wiki/File:DHCP_Server.png)

The **Dynamic Host Configuration Protocol** (**DHCP**) is a network protocol used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). The protocol is implemented in a client-server model, in which DHCP clients request configuration data, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server.

An example of use of the protocol is in a residential local area network (LAN). In this case, a DHCP server is contained in the router while the clients are hosts, e.g., personal computers, smart phones, or printers on the local network. The router itself is a client within the network of the Internet service provider (ISP) and receives its configuration information upstream from the ISP's DHCP server.

A DHCP server maintains a database of available IP addresses and configuration information. When the server receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, and then allocates an IP address or prefix that is appropriate for the client, and sends configuration information appropriate for that client. DHCP servers typically grant IP addresses to clients only for a limited interval. DHCP clients are responsible for renewing their IP address before that interval has expired, and must stop using the address once the interval has expired, if they have not been able to renew it.

DHCP is used for Internet Protocol version 4 (IPv4), as well as IPv6. While both versions serve the same purpose, the details of the protocol for IPv4 and IPv6 are sufficiently different that they may be considered separate protocols.

Hosts that do not use DHCP for address configuration may still use it to obtain other configuration information. Alternatively, IPv6 hosts may use stateless address autoconfiguration. IPv4 hosts may use link-local addressing to achieve limited local connectivity.

**TECHNICAL OVERVIEW**

Dynamic Host Configuration Protocol automates network-parameter assignment to network devices from one or more DHCP servers. Even in small networks, DHCP is useful because it makes it easy to add new machines to the network.

When a DHCP-configured client (a computer or any other network-aware device) connects to a network, the DHCP client sends a broadcast query requesting necessary information to a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, other servers such as time servers, and so forth. On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting, and must complete before the client can initiate [IP](http://en.wikipedia.org/wiki/Internet_Protocol)-based communication with other hosts. Upon disconnecting, the IP address is returned to the pool for use by another computer. This way, many other computers can use the same IP address within minutes of each other.

Because the DHCP protocol must work correctly even before DHCP clients have been configured, the DHCP server and DHCP client usually must be connected to the same network link. In larger networks, this is not practical. On such networks, each network link contains one or more DHCP relay agents. These DHCP relay agents receive messages from DHCP clients and forward them to DHCP servers. DHCP servers send responses back to the relay agent, and the relay agent then sends these responses to the DHCP client on the local network link.

Depending on implementation, the DHCP server may have three methods of allocating IP-addresses:

Dynamic allocation : A network administrator assigns a range of IP addresses to DHCP, and each client computer on the LAN is configured to request an IP address from the DHCP server during network initialization. The request-and-grant process uses a lease concept with a controllable time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed.

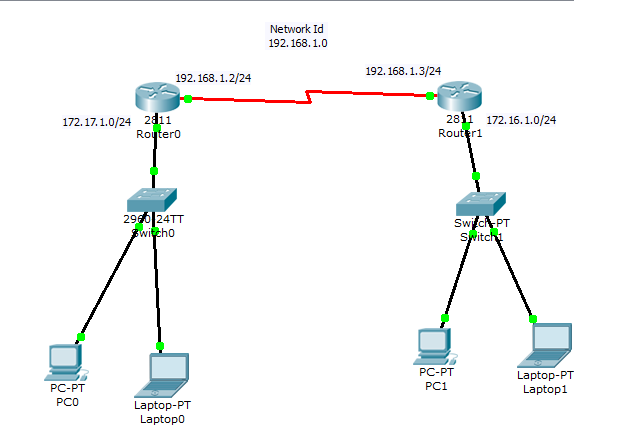
Automatic allocation : The DHCP server permanently assigns a free IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.

Static allocation: The DHCP server allocates an IP address based on a table with MAC address/IP address pairs, which are manually filled in (perhaps by a network administrator). Only clients with a MAC address listed in this table will be allocated an IP address. This feature, which is not supported by all DHCP servers, is variously called *Static DHCP Assignment* by DD-WRT, *fixed-address* by the dhcpd documentation, *Address Reservation* by Netgear, *DHCP reservation* or *Static DHCP* by Cisco and Linksys, and *IP reservation* or *MAC/IP binding* by various other router manufacturers.

**Configuration of DHCP In Cisco PacketTracer**

Consider a scenario in which there are two Routers ,two Switches and single Computer and a Laptap are connected to each other. Router–Router connnection are made by using Serial cable (DTE)

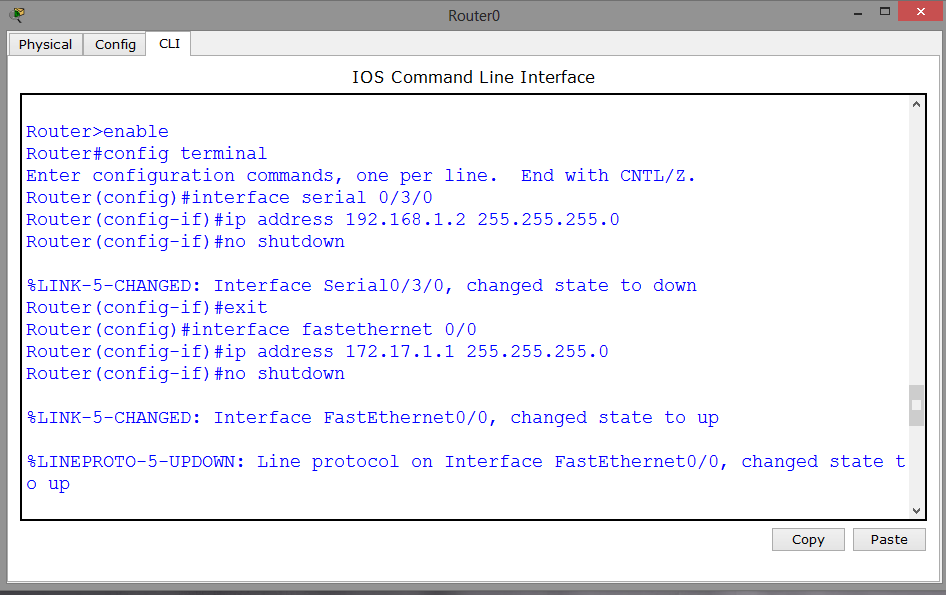
Router-switch and Switch-Computer/Laptop are made by using Fast-Ethernet Cable.



**IP configuration of Router 0 and Router 1**

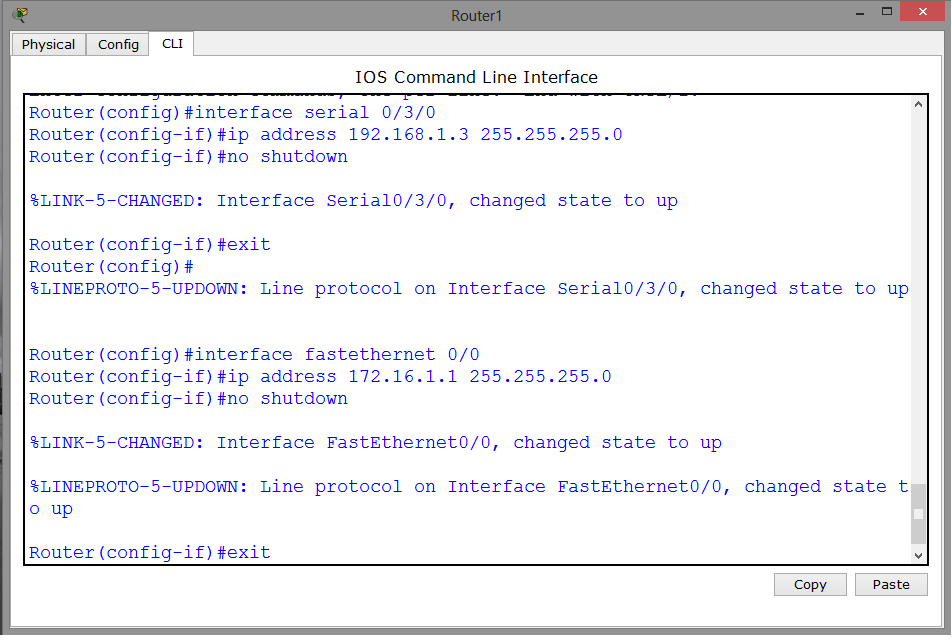
**IP Configuraton of Router 0:**

The Routers are always configured in IOS Command Line Interface in the Configuraton Mode.



In Router 0,Serial interface is configured with 192.168.1.2 as I.P Address and 255.255.255.0 as Subnet mask. Fast Ethernet is configured with 172.17.1.1 as I.P Address and 255.255.255.0 as Subnet Mask.

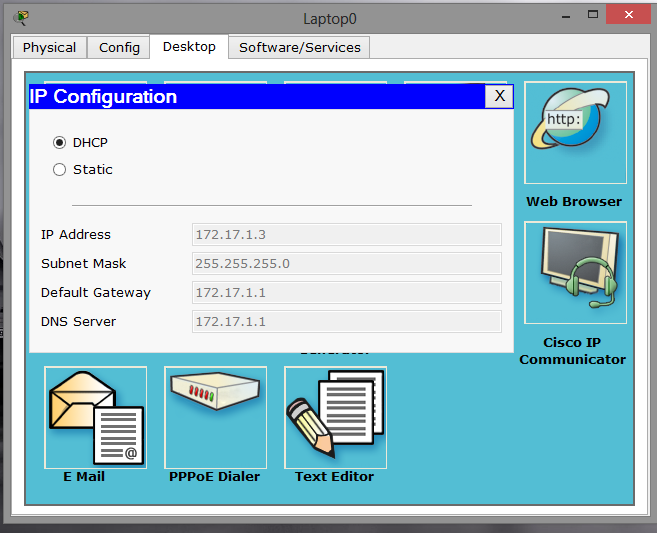
**IP Configuraton of Router 0:**



In Router 0,Serial interface is configured with 192.168.1.2 as I.P Address and 255.255.255.0 as Subnet mask. Fast Ethernet is configured with 172.17.1.1 as I.P Address and 255.255.255.0 as Subnet Mask.

Once the IP gets configured in Routers , the Red Light will turn into Green Light.

**PC is Getting the I.P through DHCP Server**

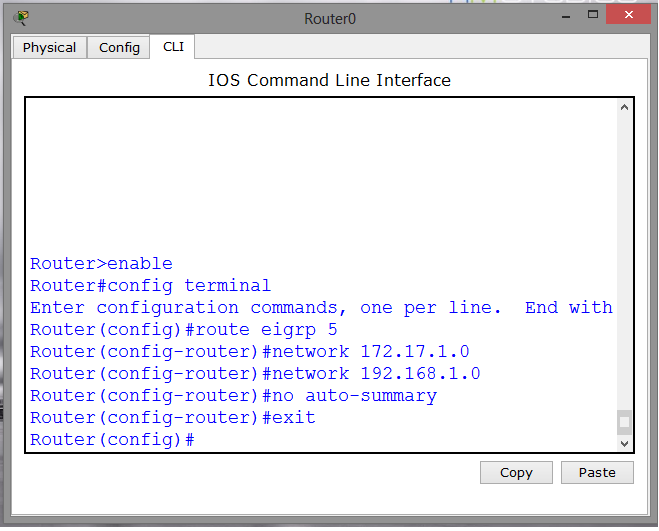


In Personal Computers, there is an option for choosing either DHCP or Static I.P. If a user chooses DHCP server’s option then automstically I.P is provided to his computer .If he chooses static I.P address ,then he has to provide I.P address itself.In case if the I.P configured by the user is already given to some one by DHCP server then the connection to the internet will not be established.

The user has to hit and trail number of times in order to established internet connection.

**Configuration of Routing Protocol in Routers**

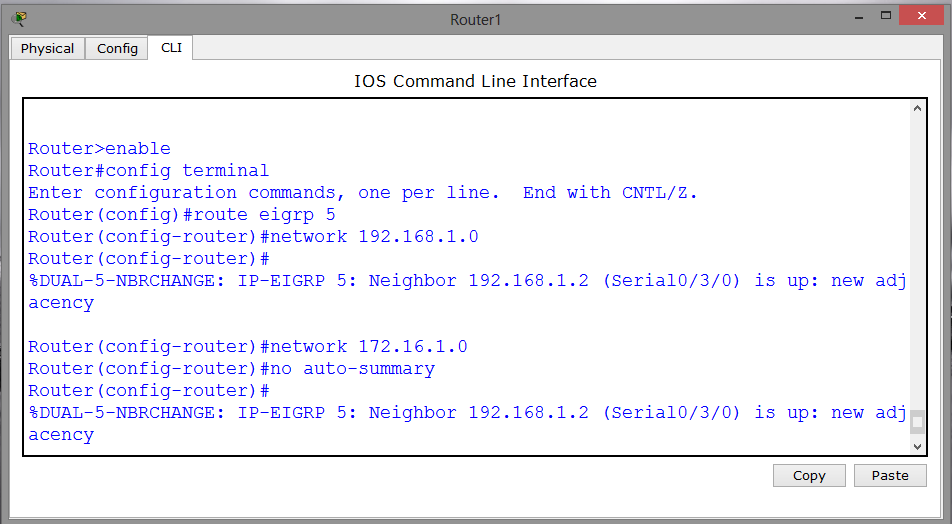
Configuring Routing Protocol in Router 0:



The router 0 is configured with EIGRP Routing Protocol. The Domain of the Eigrp is 5.

Under Domain 5, 172.17.1.0 and 192.168.1.0 network id’s are provided.

**Configuring Routing Protocol in Router 0:**



The router 0 is configured with EIGRP Routing Protocol. The Domain of the Eigrp is 5.

Under Domain 5, 172.17.1.0 and 192.168.1.0 network id’s are provided.

**VIRTUAL LAN**

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a **Virtual Local Area Network**, **Virtual LAN** or **VLAN**.

This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each VLAN. More sophisticated devices can mark packets through *tagging*, so that a single interconnect (*trunk*) may be used to transport data for various VLANs.

Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs. Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain.

.

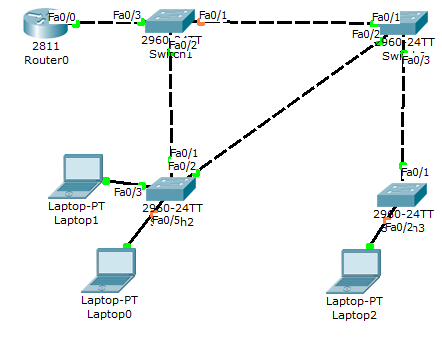
Network architects set up VLANs to provide the segmentation services traditionally provided only by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic-flow management. By definition, switches may not bridge IP traffic between VLANs as doing so would violate the integrity of the VLAN broadcast domain.

VLANs can also help create multiple layer 3 networks on the same layer 2 switch. For example, if a DHCP server is plugged into a switch it will serve any host on that switch that is configured to get its IP from a DHCP server. By using VLANs you can easily split the network up so some hosts won't use that DHCP server and will obtain link-local addresses, or obtain an address from a different DHCP server. Hosts may also use a DNS server if a DHCP is not available.

VLANs are layer 2 constructs, compared with IP subnets, which are layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN. VLANs and IP subnets provide independent layer 2 and layer 3 constructs that map to one another and this correspondence is useful during the network design process.

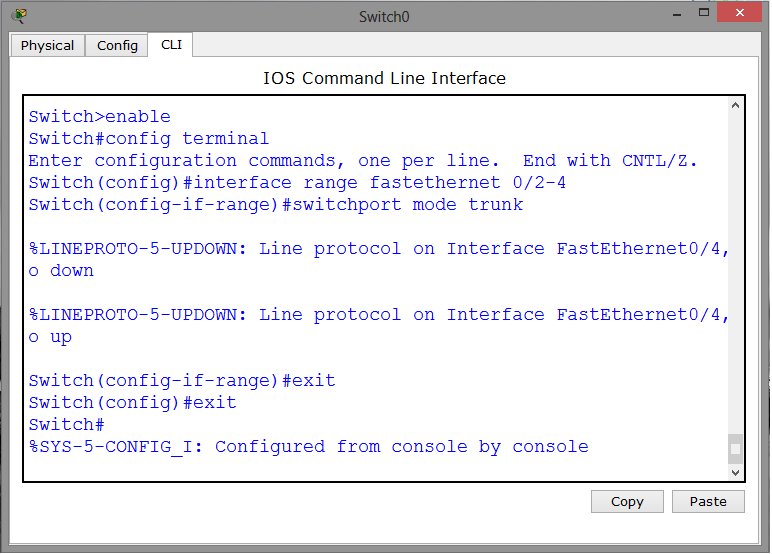
**Vlan Configuration :**

Consider another scenario in which there are one Router,four Switches,two Computers and Laptops.



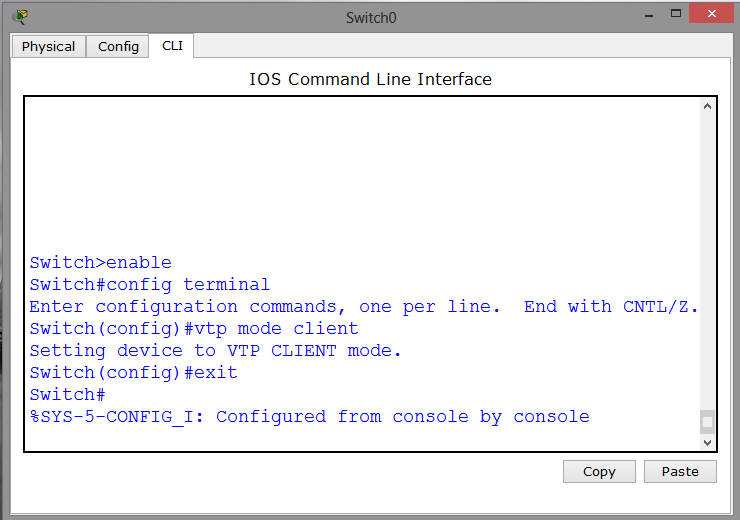
In this scenario,the Switch number 0 is considered as the Primary Switch and the other Switches are considered as the Secondary Switch. This means that the Primary Switch will act as a Master and the rest Secondary Switch will act as Slaves.

**Making Switches Ports To Trunk Mode :**



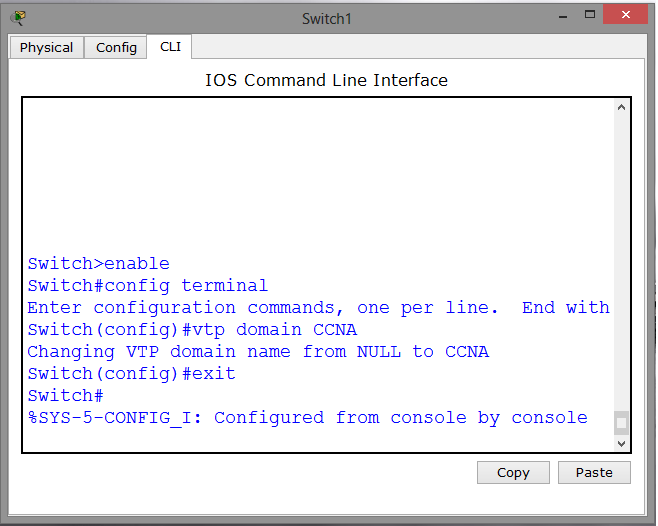
This is switch0 in which the fastethernet ports are configured as Trunk.Similarly ,all other Switch’s Ports are configured as Trunk mode. After then except Switch1,in all other Switches , Client mode is configured.Now Except Switch 1 no other Switch can make any changes in the Networking setting.

**Client Mode Configuration in Switches**



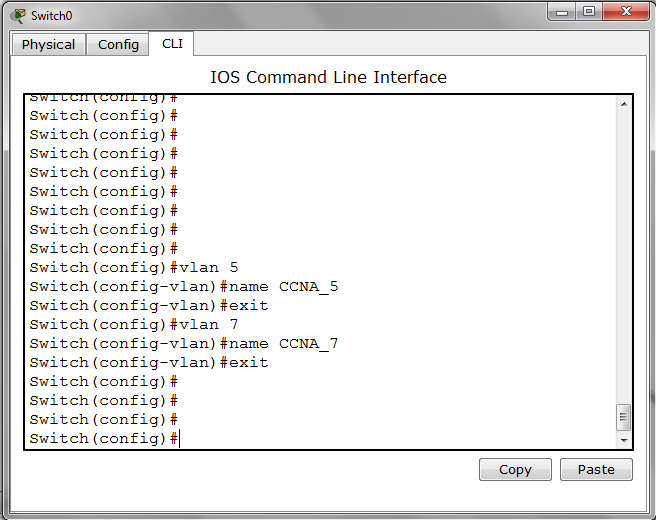
Except the Master Switch, in all other Switches the client mode is configured.In a client mode,no switch can made any changes to the Setting which are configured by the master switch.

**Virtual Trunk Protocol Configuration in Switches**



The Virtual Trunk Protocol is configured on master switch.And its domain name is CCNA.This means all the vlans which comes under this domain can communicate with each other.No vlans from different vtp domain can communicate with each other.

VLAN Configuration



In the master switch two vlans are created that is vlan5 and vlan6.It cannot be configured on the switches having client access.