NETWORK LAYOUT OF BLOCK-14

PROJECT REPORT

Submitted in the partial fulfillment for the award of the Degree of

BACHELOR OF ENGINEERING

Under the Supervision of:

Mr. Nadeem Sir

IN

B.E- CSE (IBM BD&MC)

Submitted by:

Divyajyoti	**(17BCS3955)**
Ankit	**(17BCS3974)**
Kawal	**(17BCS3967)**
Shubham Sharma	**(17BCS4318)**

CHANDIGARH UNIVERSITY, GHARUAN, MOHALI-
140413, PUNJAB

TABLE OF CONTENT

1.1 Introduction

A computer Network is a system in which a number of independent computers are linked together to share data and peripherals, such as files and printers. In the modern world, computer networks have become almost indispensable. All major businesses and governmental and educational institutions make use of computer networks to such an extent that it is now difficult to imagine a world without them.

1.2 Computer Networks

Computer networks exist on various scales, from links between two computers in one room to connecting computers in a building or campus to national and global networks. Various media are used to carry the communications signals: copper wire, fibre-optic cables and wireless or radio transmissions etc. Similarly, the network connecting an organization's computers might be owned and managed by the organization itself (typically in small-scale networks linking machines in a room or building) or capacity can be rented from a firm providing telecommunications services (typically in wider area networks).

Components of a computer network

A computer network is composed of:

- Hosts (PCs, laptops, handhelds)
- Routers & switches (IP router, Ethernet switch)
- Links (wired, wireless)
- Protocols (IP, TCP, CSMA/CD, CSMA/CA)
- Applications (network services)

Client/Server

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request. Although programs within a single computer can use the client/server idea, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across.

Some basic concepts of networking include:

Networking Devices, Topologies, Network Types, Protocols and models, IP addresses etc.
Networking Devices include switches, routers, CISCO packet tracer, etc.

Switches:

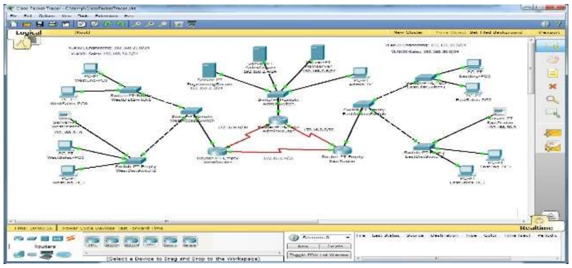
Switches are the foundation of most business networks. A switch acts as a controller, connecting computers, printers, and servers to a network in a building or a campus.
Switches allow devices on your network to communicate with each other, as well as with other networks, creating a network of shared resources. Through information sharing and resource allocation, switches save money and increase productivity.
There are two basic types of switches to choose from as part of your networking basics: managed and unmanaged.
An unmanaged switch works out of the box but can't be configured. Home-networking equipment typically offers unmanaged switches.
A managed switch can be configured. You can monitor and adjust a managed switch locally or remotely, giving you greater control over network traffic and access.

Routers:

Enable all networked computers to share a single Internet connection, which saves money. Beyond those basic networking functions, routers come with additional features to make networking easier or more secure. Depending on your needs, for example, you can choose a router with a firewall, a virtual private network (VPN), or an Internet Protocol (IP) communications system.

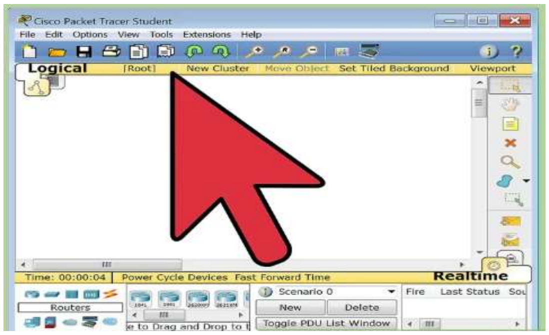
CISCO Packet Tracer:

Is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Suppose, if you want to deploy any change in your production network, you can use packet tracer to first test the required changes and if everything is working fine then you can deploy that changes into production.

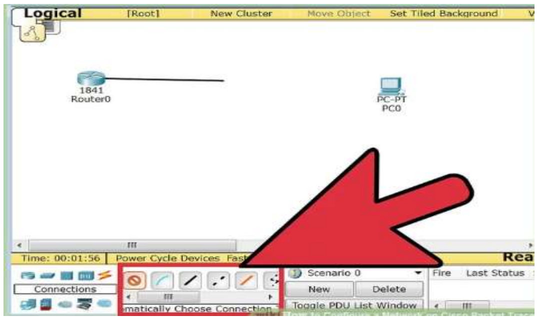


1.3 Project Overview/Specifications

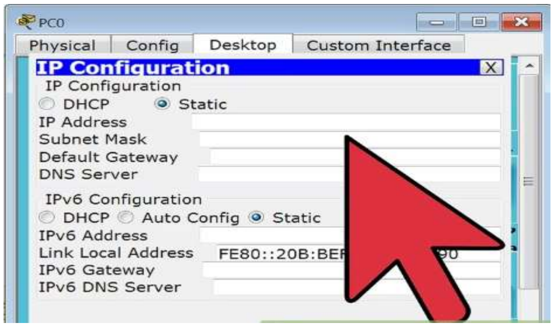
Open your Network Topology: Once you've opened your Network Topology on Cisco Packet Tracer, access your network and identify the components of your network, for example; Servers, Routers, End Devices, etc.



Complete the cabling: Access the cables section and connect completely and correctly the cables between the network in order to ensure connectivity between the devices in the network using the connections table given.



Configure the IP addresses on the end devices: Using the address table still, correctly and completely configure the IP addresses on all end devices. This can be done by accessing the desktop platform on each device and locating the IP configuration section. The reason for doing this is to enable the devices be on the right network.



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

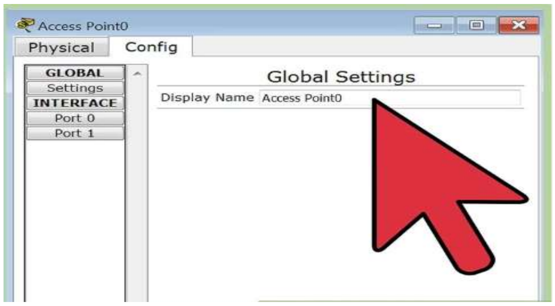
IPv6 Address

Link Local Address FE80::20B:BE

IPv6 Gateway

IPv6 DNS Server

Configure the IP addresses on your routers and switches: After configuring the right IP addresses on the end devices, you will have to do the same on the routers and switches also, using the address table.

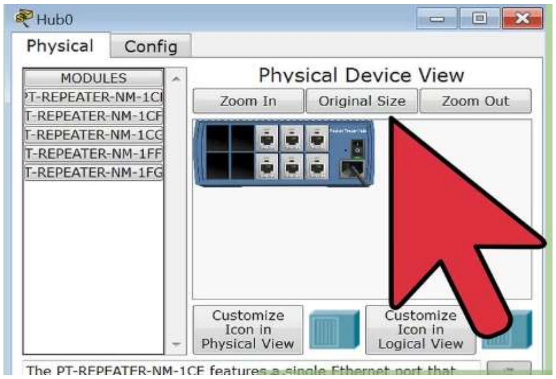


Global Settings

Display Name Access Point0

Configure your default gateway:

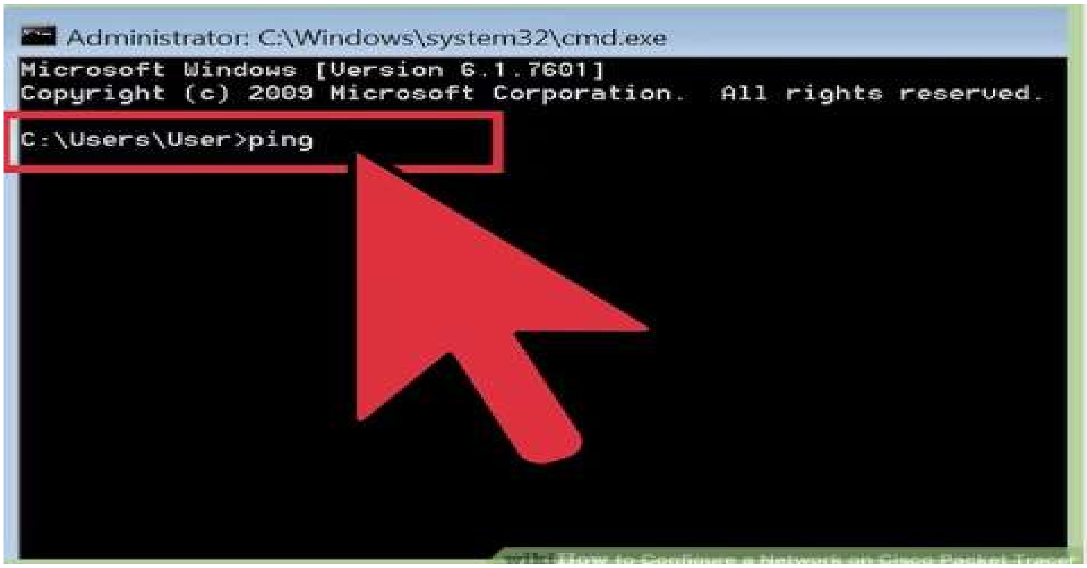
After configuring the IP addresses, you will need to configure the default gateway also. The reason for this is so the end devices would know what network they are operating on. You can find the default gateway either in the addressing table (if given) or in the network topology.



The PT-REPEATER-NM-1CE features a single Ethernet port that

Test connectivity:

After configuring the addresses, you will have to test connectivity by opening a command prompt window on the end devices and try pinging the address which the network operates on. If it gives you a reply, it means your network was configured correctly.


Administrator: C:\Windows\system32\cmd.exe
wikiHow to Configure a Network on Cisco Packet Tracer

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User>ping
```

1.4 Objective of Project

- ➔ Understand the purpose of cisco packet Tracer.

- ➔ Interconnect device s and configure them using simple interface.

- ➔ Configure network device using CLI (Common Line Interface).

- ➔ Track packets in Packet Tracer and simulate real traffic conditions and different protocols.

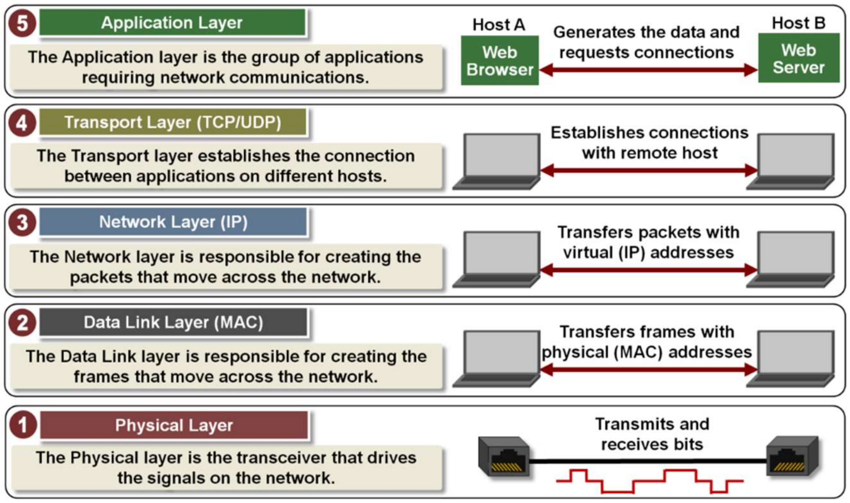
- ➔ We make the connectivity of different PCs with the networking by giving the IP address by DHCP Concept.

- ➔ Used of DHCP Server, Routers, switches & we have made two levels of Block 14 PCs Connects.

1.5 TCP/IP MODEL:

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer


5
Application Layer
The Application layer is the group of applications requiring network communications.
Host A
Web Browser
Generates the data and requests connections
Host B
Web Server
4
Transport Layer (TCP/UDP)
The Transport layer establishes the connection between applications on different hosts.
Establishes connections with remote host
3
Network Layer (IP)
The Network layer is responsible for creating the packets that move across the network.
Transfers packets with virtual (IP) addresses
2
Data Link Layer (MAC)
The Data Link layer is responsible for creating the frames that move across the network.
Transfers frames with physical (MAC) addresses
1
Physical Layer
The Physical layer is the transceiver that drives the signals on the network.
Transmits and receives bits

Application Layer

Its jobs are to convert all data into computer language. Language that computer understand.

Ex: -Browser

Protocols: -HTTP, FTP, Telnet.

It encodes, compress and encrypts data.

It initiates setting and termination of session.

Transport Layer

This is where port number and segmentation are allowed to data packets.

It adds port Number.

Protocols: TCP & UDP

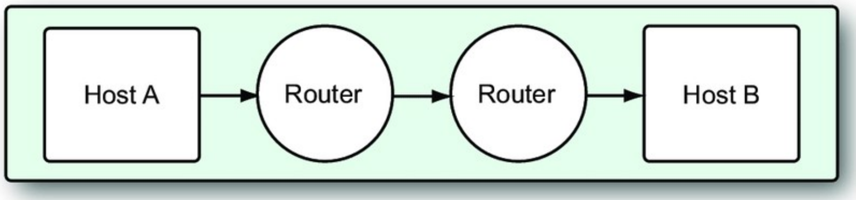
Network Layer

This layer adds sender and receiver IP address on the data packets.
It handles IP addressing, routing & virtual pathing.
It adds MAC address of the client and the server.
Protocols: -
DHCP: for assigning the IP address
ARP: for convention between IP &MAC address
ICMP: for Debugging network stability

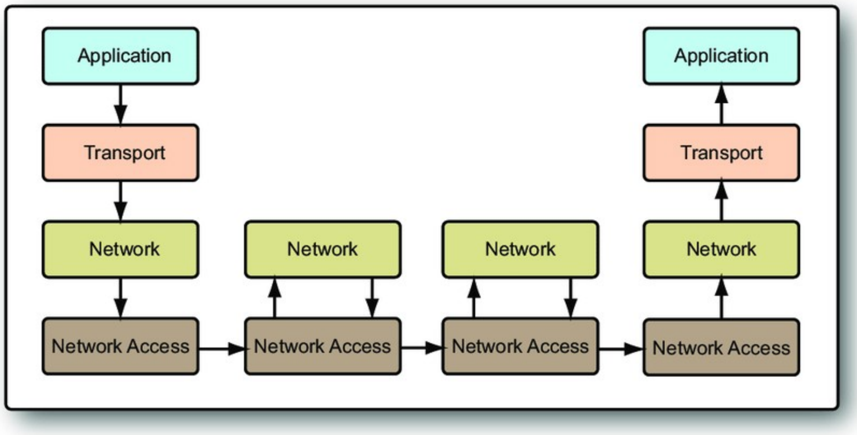
Physical Layer

It connects binary signals to electrical signal for data transfer.
It checks itself for errors & control the flow of data.
Protocols:
Ethernet for LAN cable
802.11(wireless connection like Wi-Fi, Bluetooth)
DSL: for telephone cable

Network Connections View



TCP/IP Model



BRIEF DESCRIPTION ABOUT CISCO PACKET TRACER

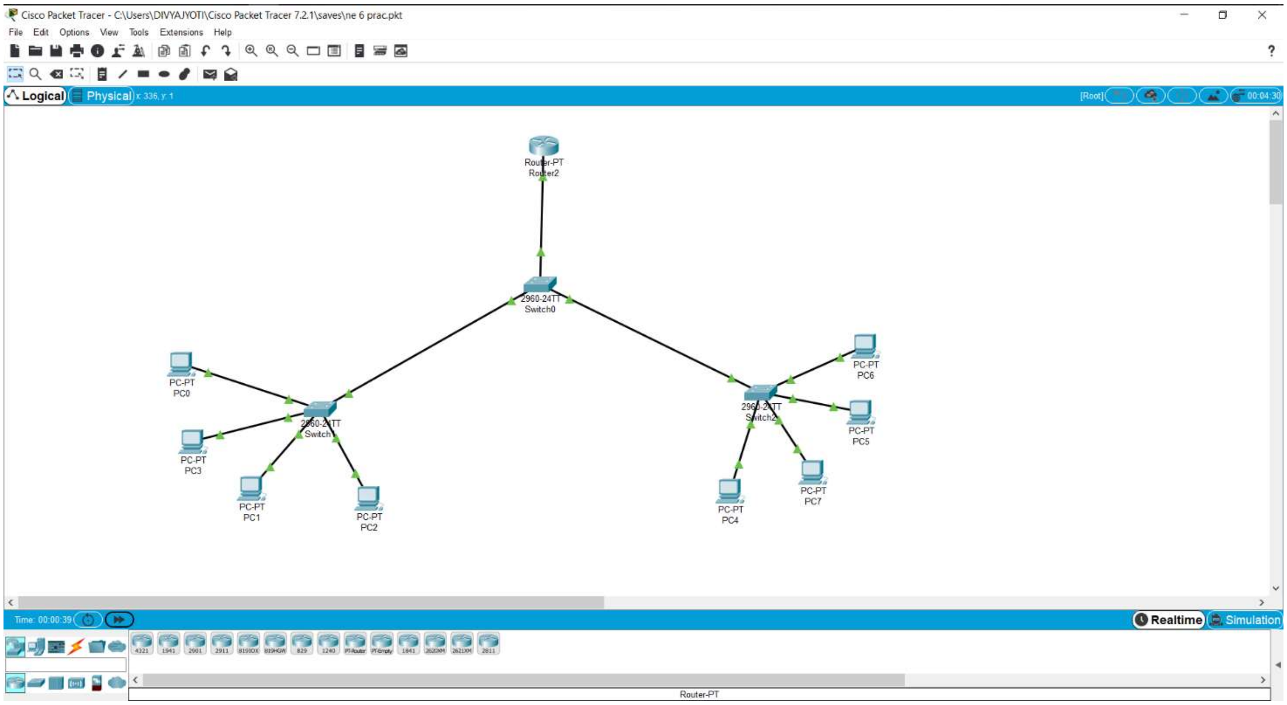
Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet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

Packet Tracer can also be run on Linux and Microsoft Windows and also macOS. Similar Android and iOS apps are also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a 'cable' item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum. As of version 5.3, Packet Tracer also supports the Border Gateway Protocol.

In addition to simulating certain aspects of computer networks, Packet Tracer can also be used for collaboration. As of Packet Tracer 5.0, Packet Tracer supports a multi-user system that enables multiple users to connect multiple topologies together over a computer network. Packet Tracer also allows instructors to create activities that students have to complete. Packet Tracer is often used in educational settings as a learning aid. Cisco Systems claims that Packet Tracer is useful for network experimentation.

Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs. Packet Tracer is commonly used by CCNA Academy students, since it is available to them for free. However, due to functional limitations, it is intended by CISCO to be used only as a learning aid, not a replacement for Cisco routers and switches. The application itself only has a small number of features found within the actual hardware running a current Cisco IOS version. Thus, Packet Tracer is unsuitable for modelling production networks. It has a limited command set, meaning it is not possible to practice all of the IOS commands that might be required. Packet Tracer can be useful for understanding abstract networking concepts, such as the Enhanced Interior Gateway Routing Protocol by animating these elements in a visual form. Packet Tracer is also useful in education by providing additional components, including an authoring system, network protocol simulation and improving knowledge an assessment system.

SCREENSHOT OF PACKET TRACER:



STATIC AND DYNAMIC ROUTING

Static Routing:

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximize routing efficiency and to provide backups in the event that dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.

Uses of Static Routing:

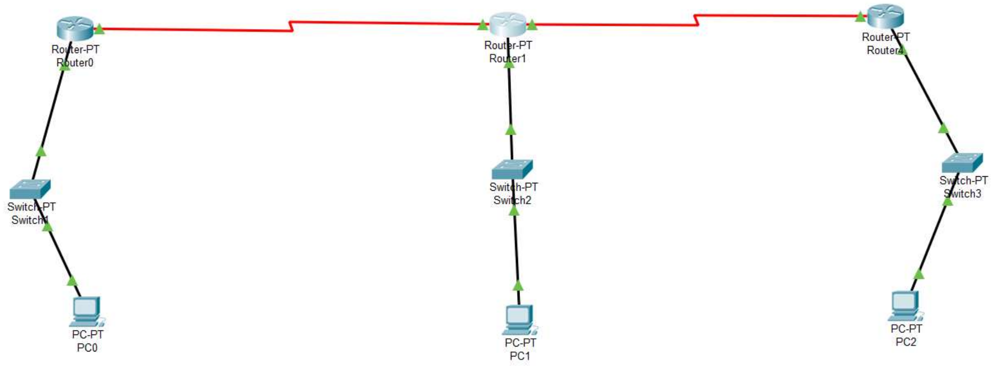
- Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.
- Static routing can be used for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- Static routing is often used as a complement to dynamic routing to provide a failsafe backup in the event that a dynamic route is unavailable.
- Static routing is often used to help transfer routing information from one routing protocol to another (routing redistribution).

Advantages:

- Static routing causes very little load on the CPU of the router, and produces no traffic to other routers.
- Static routing leaves the network administrator with full control over the routing behavior of the network.
- Static Routing Is very easy to configure on a small network.

Disadvantages:

- **Human error:** In many cases, static routes are manually configured. This increases the potential for input mistakes. Administrators can make mistakes and mistype in network information, or configure incorrect routing paths by mistake.
- **Fault tolerance:** Static routing is not fault tolerant. This means that when there is a change in the network or a failure occurs between two statically defined devices, traffic will not be re-routed. As a result, the network is unusable until the failure is repaired or the static route is manually reconfigured by an administrator.
- **Administrative distance:** Static routes typically take precedence over routes configured with a dynamic routing protocol. This means that static routes may prevent routing protocols from working as intended. A solution is to manually modify the administrative distance.
- **Administrative overhead:** Static routes must be configured on each router in the networks. This configuration can take a long time if there are many routers. It also means that reconfiguration can be slow and inefficient. Dynamic routing on the other hand automatically propagates routing changes, reducing the need for manual reconfiguration.



Dynamic Routing:

Dynamic routing, also called **adaptive routing**, is a process where a router can forward data via a different route or given destination based on the current conditions of the communication circuits within a system. The term is most commonly associated with data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so long as other path choices are available. Dynamic routing allows as many routes as possible to remain valid in response to the change.

Systems that do not implement dynamic routing are described as using static routing, where routes through a network are described by fixed paths. A change, such as the loss of a node, or loss of a connection between nodes, is not compensated for. This means that anything that wishes to take an affected path will either have to wait for the failure to be repaired before restarting its journey, or will have to fail to reach its destination and give up the journey.

Advantages:

More automation: Routing updates are automatically sent to all other routers.

- Change notification: The dynamic routing protocol may be able to reroute traffic around a link that is down or congested.
- Greater uptime for users: Because the routing protocol has intelligence and can react faster, the users may see more uptime.
- Greater network throughput: Because the routing protocol may be able to calculate the most responsive network link to use, the users may see less latency and more performance out of the network.
- Less work for administrators: As the network grows, the administrator doesn't have to worry about configuring all the other routers on the network. Instead, the administrator configures the dynamic routing protocol on the new router to talk to the other routers and let them know what networks the new router has to offer.

Disadvantages:

- Updates are shared between routers, thus consuming bandwidth
- Routing protocols put additional load on router CPU/RAM
- The choice of the “best route” is in the hands of the routing protocol, and not the network administrator.

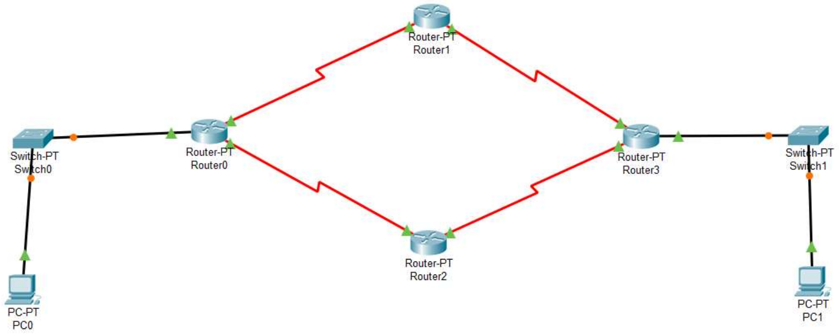
PROTOCOLS USED IN THE PROJECT

RIP (Routing Information Protocol)

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.
Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

Features of RIP:

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbor routers. This is also known as *Routing on rumors*.



DHCP (Dynamic Host Configuration Protocol)

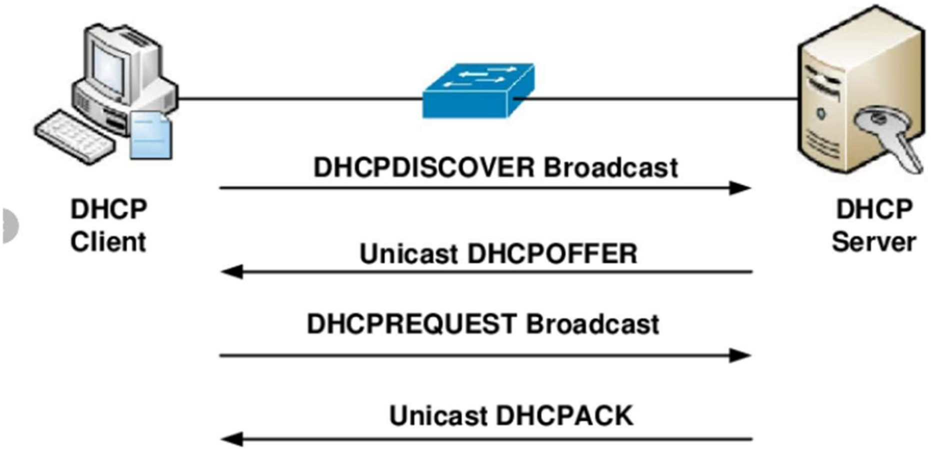
DHCP protocol stands for dynamic host configuration protocol which is an application layer protocol which provides:

1. Subnet mask
2. Router address
3. DNS address
4. Vendor class identifier

DHCP is based on client-server model, port number for server is 67 and for that of client is 68. It uses UDP services and IP addresses are assigned from poll of address for a particular interval of time. Server and client exchange 4 messages in order to make a connection between them.

Messages for making the connection:

1. DHCP discover the message.
2. DHCP offer a message.
3. DHCP request a message.
4. DHCP acknowledgement message.
5. DHCP negative acknowledgment message
6. DHCP decline
7. DHCP release
8. DHCP inform



Advantages of the DHCP protocol:

1. Centralized management of IP addresses.
2. Ease of adding new clients.
3. Reducing the total number of IP required by reusing them.
4. Simple configuration without the need to configure it by our own.

Disadvantage: IP conflict can occur.

Working of DHCP:
DHCP runs at the application layer of the transmission control protocol stack to dynamically assign IP addresses to DHCP clients and to allocate TCP/IP configuration information to DHCP clients. This includes subnet mask, default gateway, domain name and DNS address.
DHCP is a client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools. DHCP – enabled clients send a request to the DHCP server whenever they connect to a network.

DHCP Discover: It is a DHCP message that marks the beginning of a DHCP interaction between client and server. This message is sent by a client (host or device connected to a network) that is connected to a local subnet.

DHCP Offer: It is DHCP message that is sent in response to DHCP Discover by a DHCP server to DHCP client. This message contains the network configuration settings for the client that sent the DHCPDISCOVER message.

DHCP Request: This DHCP message is sent in response to DHCP Offer indicating that the client has accepted the network configuration sent in DHCP Offer message from the server.

DHCP Nak: This message is the exact opposite to DHCPACK described above. This message is sent by the DHCP server when it is not able to satisfy the DHCP Request message from the client.

DHCP Decline: This message is sent from the DHCP client to the server in case the client finds that the IP address assigned by DHCP server is already in use.

DHCP Inform: This message is sent from the DHCP client in case the IP address is statically configured on the client and only other network settings or configurations are desired to be dynamically acquired from DHCP server.

VTP (VLAN Truncking Protocol)

VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network.[1] To do this, VTP carries VLAN information to all the switches in a VTP domain. VTP advertisements can be sent over 802.1Q, and ISL trunks. VTP is available on most of the Cisco Catalyst Family products. Using VTP, each Catalyst Family Switch advertises the following on its trunk ports:

- Management domain
- Configuration revision number
- Known VLANs and their specific parameters

There are three versions of VTP, namely version 1, version 2, version 3.

The comparable IEEE standard in use by other manufacturers is GVRP or the more recent MVRP.

There are different modes of VTP:

1. Server mode
2. Client mode
3. Transparent mode

On Cisco Devices, VTP (VLAN Trunking Protocol) maintains VLAN configuration consistency across a single Layer 2 network. VTP uses Layer 2 frames to manage the addition, deletion, and renaming of VLANs from switches in the VTP client mode. VTP is responsible for synchronizing VLAN information within a VTP domain and reduces the need to configure the same VLAN information on each switch thereby minimizing the possibility of configuration inconsistencies that arise when changes are made.

Benefits of VTP:

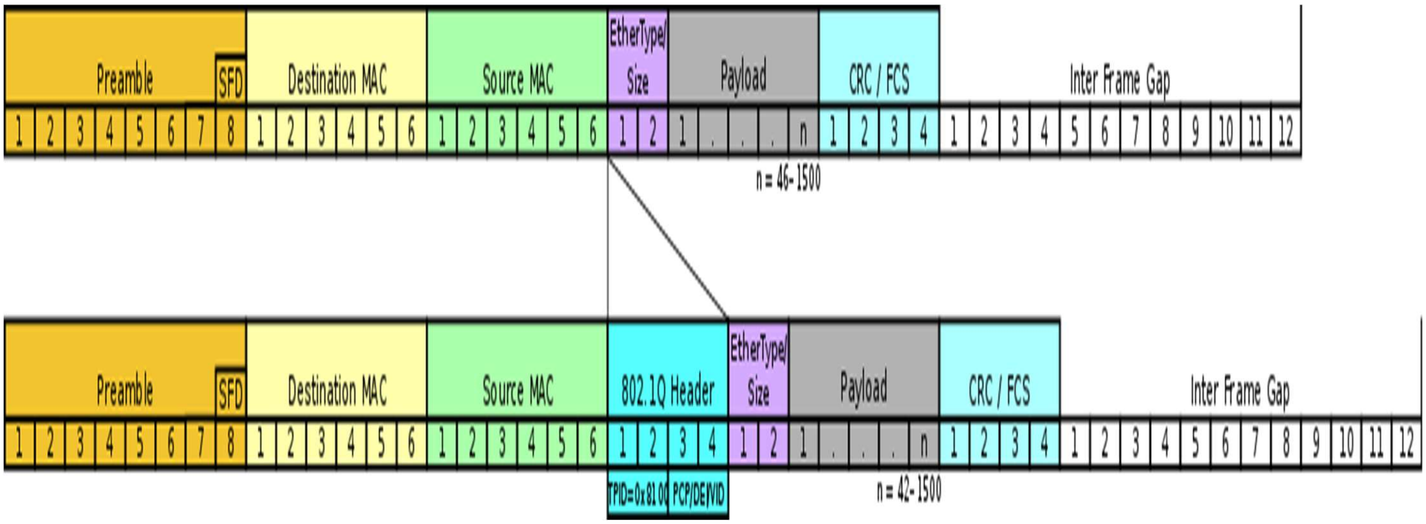
- VLAN configuration consistency across the layer 2 network
- Dynamic distribution of added VLANs across the network
- Plug-and-play configuration when adding new VLANs

DOT1Q

IEEE 802.1Q, often referred to as Dot1q, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality-of-service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

Portions of the network which are VLAN-aware (i.e., IEEE 802.1Q conformant) can include VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership. Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the native VLAN.

The standard was developed by IEEE 802.1, a working group of the IEEE 802 standards committee, and continues to be actively revised. One of the notable revisions is 802.1Q-2014 which incorporated IEEE 802.1aq (Shortest Path Bridging) and much of the IEEE 802.1D standard.



VLAN (Virtual Local Area Network)

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).[1][2] *LAN* is the abbreviation for *local area network* and in this context *virtual* refers to a physical object recreated and altered by additional logic. VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. Because VLAN membership can be configured through software, this can greatly simplify network design and deployment. Without VLANs, grouping hosts according to their resource needs necessitates the labour of relocating nodes or rewiring data links. VLANs allow networks and devices that must be kept separate to share the same physical cabling without interacting, improving simplicity, security, traffic management, or economy. For example, a VLAN could be used to separate traffic within a business due to users, and due to network administrators, or between types of traffic, so that users or low priority traffic cannot directly affect the rest of the network's functioning. Many Internet hosting services use VLANs to separate their customers' private zones from each other, allowing each customer's servers to be grouped together in a single network segment while being located anywhere in their data centre. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.

To subdivide a network into VLANs, one configures network equipment. Simpler equipment can partition only per physical port (if at all), in which case each VLAN is connected with a dedicated network cable. More sophisticated devices can mark frames through VLAN tagging, so that a single interconnect (*trunk*) may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk can use link aggregation, quality-of-service prioritization, or both to route data efficiently.

Advantages of VLANs

When set up correctly, virtual LANs improve the performance of busy networks. VLANs group together client devices that communicate with each other frequently. The traffic between devices split across two or more physical networks is usually handled by a network's core routers. With a VLAN, that traffic is handled more efficiently by network switches.

VLANs also bring security benefits to larger networks by allowing greater control over which devices have local access to each other. Wi-Fi guest networks are often implemented using wireless access points that support VLANs.

Static and Dynamic VLANs

Network administrators often refer to static VLANs as port-based VLANs. In a static VLAN, an administrator assigns individual ports on the network switch to a virtual network. No matter what device plugs into that port, it becomes a member of that pre-assigned virtual network.

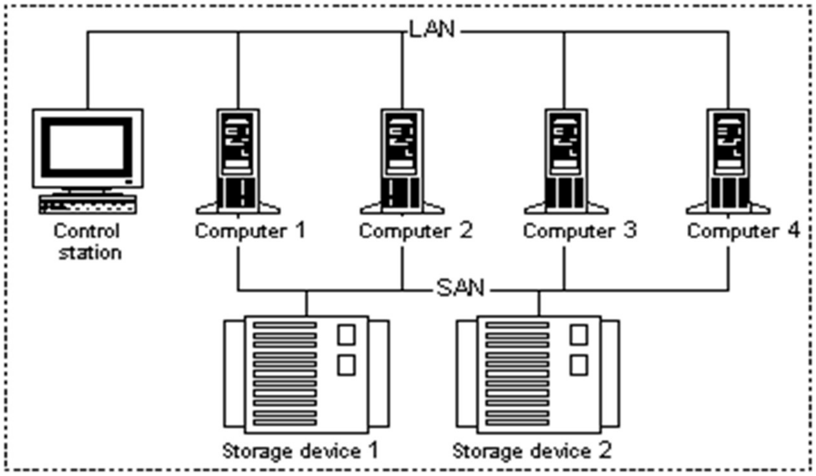
In dynamic VLAN configuration, an administrator defines network membership according to characteristics of the devices rather than the switch port location. For example, a dynamic VLAN can be defined with a list of physical addresses (MAC addresses) or network account names.

NETWORK CLUSTRING

A network cluster consists of loosely or tightly connected computers that work together so that they can be viewed as a single system. In network cluster there are various computers and each one performs the same task which is controlled and managed by software.

Various things can be achieved using clustering

1. High computation
2. Cluster storage
3. Load balancing.



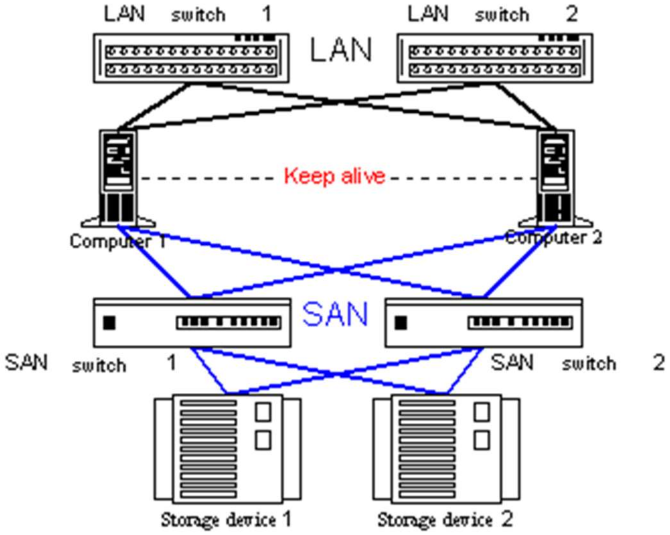
Requirements for cluster systems are:

1. High performance
2. Scalability
3. Shared resources access.
4. Availability.
5. Service ability.
6. Reliability

Computer cluster works as a single system i.e. for a user it's only a single computer but actually it consists of various computers which work as a single system, this is one of the most important things in arrangement of cluster system.

Today one can come across such cluster architectures which combine high-availability systems and high-performance cluster architectures where applied problems are distributed among nodes of the system.

A fault-tolerant system can be build using clustering which can be further improved by adding more nodes to make computation system. But making such high computation system can increase price of overall cluster so these high-performance systems are not added these days to maintain price in a normal range. And to make high availability systems its necessary that all of its components are maximum reliable, fault-tolerant and it have no point of fault and system must be serviceable and allow replacing components without the need to be turned off.



Advantages of Network Clustering:

1. Performance
2. Availability
3. Incremental Growth
4. Scaling

PERFORMANCE

Throughput and response time are improved as we use many machines at the same time as computation speed will be increased, storage will be increased and chances of system failure will be decreased.

AVAILABILITY

Availability comes into play when one node fails at that time without interrupting user workload will be distributed among other users and will not affect operations.

INCREMENTAL GROWTH

Performance and availability as discussed can be enhanced by adding mode nodes to cluster so that to increase its efficiency which is termed as incremental growth.

SCALING

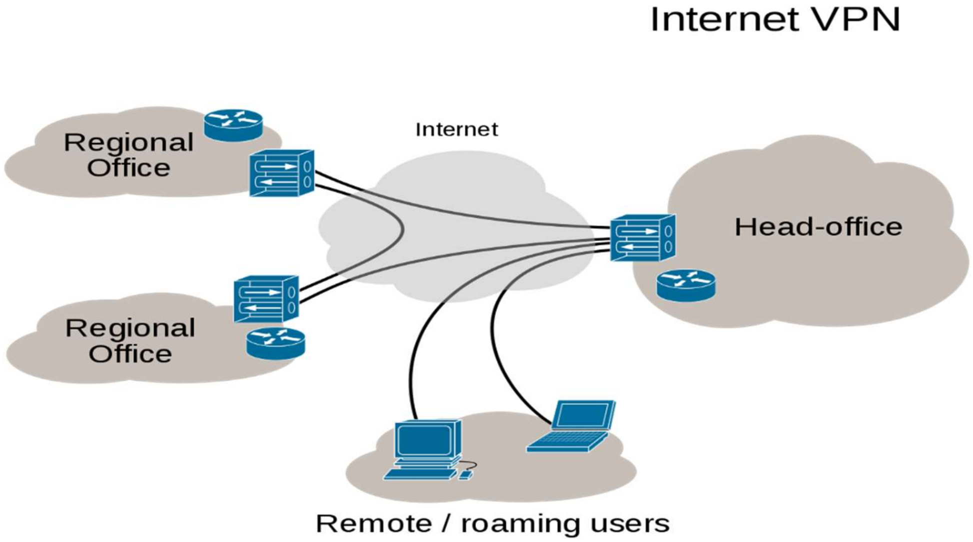
We can add as many as nodes to our cluster which is another advantage of network clustering.

VPN (Virtual Private Network)/Tunnelling

A **virtual private network** (**VPN**) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g., a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common though not an inherent part of a VPN connection.[1]

VPN technology was developed to allow remote users and branch offices to access corporate applications and resources. To ensure security, the private network connection is established using an encrypted layered tunnelling and VPN users use authentication methods, including passwords or certificates, to gain access to the VPN. In other applications, Internet users may secure their connections with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. However, some websites block access to known VPN technology to prevent the circumvention of their geo-restrictions, and many VPN providers have been developing strategies to get around these roadblocks.

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunnelling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

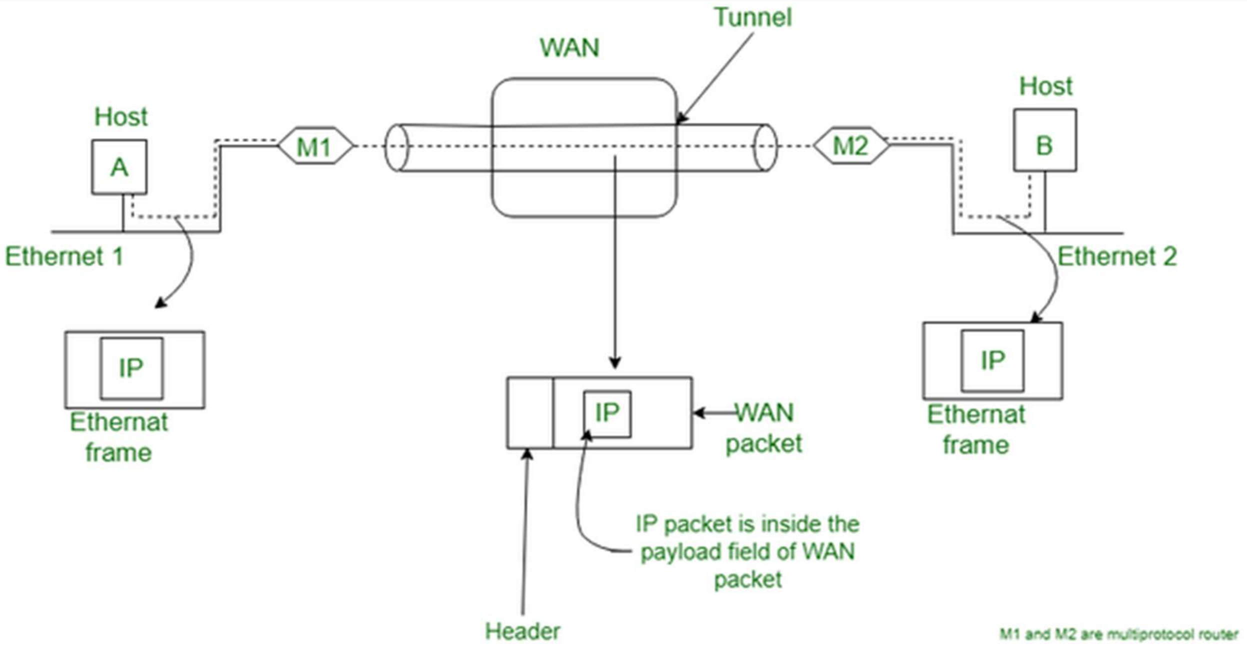


Tunnelling

A technique of internetworking called tunneling is used when source and destination networks of same type are to be connected through a network of different type.

Steps for Tunneling

1. Host A construct a packet which contains the IP address of Host B.
2. It then inserts this IP packet into an Ethernet frame and this frame is addressed to the multiprotocol router M1
3. Host A then puts this frame on Ethernet.
4. When M1 receives this frame, it removes the IP packet, inserts it in the payload packet of the WAN network layer packet and addresses the WAN packet to M2. The multiprotocol router M2 removes the IP packet and send it to host B in an Ethernet frame.



REFERENCES

Links:

https://www.google.com

https://www.wikipedia.com

https://geeksforgeeks.com

https://www.youtube.com

Books:

COMPUTER NETWORKS by Andrew S. Tanenbaum