**CHAPTER 1**

INTRODUCTION

**Introdution to the System:**

The project is on Network Security Management System.Security is most important aspect of organization.With all of the vital personal and business data being shared on computer networks every day, security has become one of the most essential aspects of networking. No one recipe to fully safeguard networks against intruders exists. Network security technology improves and evolves over time as the methods for both attack and defence grow more sophisticated.This system helps to make secured industrial network

Main purpose of a computer network is to facilitate the users to communicate among themselves and share resources with other users. A Organization network is an important part of Organization life and network security is essential for a Organization. The Company Network Architecture is about designing a network topology that is a LAN (Local Area Network) for a Company in which various computers of different departments are set up so that they can interact and communicate with each other by interchanging data.

Organization network faces challenges to address core issues of security which are governed by network architecture. Secured network protects an institution from security attacks associated with network. Network security will prevent the company network from different types of threats and attacks.

In this project, a tested and secure network design is implemented based on the practical requirements and this proposed network infrastructure is realizable with adaptable infrastructure.

**Objective**

Our vulnerability to cyber-attacks continues to escalate as technology continues to move into mobile devices and everyday business practices. You can't hide from the danger and hope you won't be targeted. Now is the time to take control of your network security

Network Security is a branch of computer science that involves in securing a computer network and network infrastructure devices to prevent unauthorized access, data theft, network misuse, and device and data modification. Another function of Network Security is in preventing DoS (Denial of Service) attacks and assuring continuous service for legitimate network users. Network Security involves proactive defence methods and mechanisms to protect data, network and network devices from external and internal threats.

Data is the most precious factor of today’s businesses. Top business organizations spend billions of dollars every year to secure their computer networks and to keep their business data safe. Imagine the loss of all important research data on which the company has invested millions of dollars and working for years!!!

We are dependent on computers today for controlling large money transfers between banks, insurance, markets, telecommunication, electrical power distribution, health and medical fields, nuclear power plants, space research and satellites. We cannot negotiate security in these critical areas.

As the complexity of the systems and the networks are increasing, vulnerabilities are also increasing and the task of securing the networks is becoming more complex.

This makes Network Security an essential part of today's businesses.

So in this project we will deal with various types of network securities and how to manage them to create a secured industrial network.

**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. Fig 1 gives an example of a network in a college comprising of a local area network or LAN connecting computers with each other, the internet, and various servers.

School ‘Local Area

Network’ (LAN)

Modem or Router

Access to:

Internet content & learning resources, Scoilnet etc

Email communication

Cache, Proxy,

Filtering, Firewall

Server

Users

computers

Other users,

computers

File and Print Server

CD or Multimedia Servers

Printers , Scanners etc

**Fig 1: Representation of Network in a college**

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

Table 1 provides a summary comparison between Peer-to-Peer and Client/Server Networks.

|  |  |
| --- | --- |
| **Peer-to-Peer Networks vs Client/Server Networks** | |
| **Peer-to-Peer Networks** | **Client/Server Networks** |
| · Easy to set up | · More difficult to set up |
| · Less expensive to install | · More expensive to install |
| · Can be implemented on a wide range of operating systems | · A variety of operating systems can be supported on the client computers, but the server needs to run an operating system that supports networking |
| · More time consuming to maintain the software being used (as computers must be managed individually) | · Less time consuming to maintain the software being used (as most of the maintenance is managed from the server) |
| · Very low levels of security supported or none at all. These can be very cumbersome to set up, depending on the operating system being used | · High levels of security are supported, all of which are controlled from the server. Such measures prevent the deletion of essential system files or the changing of settings |
| · Ideal for networks with less than 10 computers | · No limit to the number of computers that can be supported by the network |
| · Does not require a server | · Requires a server running a server operating system |
| · Demands a moderate level of skill to administer the network | · Demands that the network administrator has a high level of IT skills with a good working knowledge of a server operating system |

**Table 1: Peer-to-Peer Networks vs Client/Server Networks**

**Components of a Network**

A computer network comprises the following components:

* A minimum of at least 2 computers
* Cables that connect the computers to each other, although wireless communication is becoming more common (see Advice Sheet 20 for more information)
* A network interface device on each computer (this is called a network interface card or NIC)
* A ‘Switch’ used to switch the data from one point to another. Hubs are outdated and are little used for new installations.
* Network operating system software

**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.

**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. Schools may want to consider upgrading any hub based networks with switches to improve network performance – i.e. 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**

**Main challenges of installing a Network**

**Costs**

Although a network will generally save money over time, the initial costs can be substantial, and the installation may require the services of a technician.

**Requires Administrative Time.**

Proper maintenance of a network requires considerable time and expertise. Many schools have installed a network, only to find that they did not budget for the necessary administrative support.

**File Server May Fail.**

Although a file server is no more susceptible to failure than any other computer, when the files server "goes down," the entire network may come to a halt. When this happens, the entire school may lose access to necessary programs and files.

**IP Addressing and Subnetting**

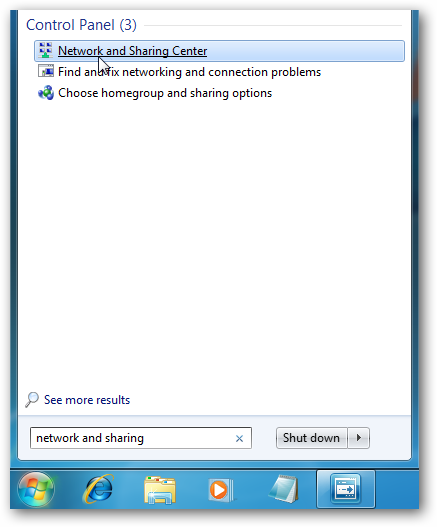
When organizing your home network it’s easier to assign each computer it’s own IP address than using DHCP. Here we will take a look at doing it in XP, Vista, Windows 7, Windows 8.x, and Windows 10.

If you have a home network with several computes and devices, it’s a good idea to assign each of them a specific address. If you use DHCP (Dynamic Host Configuration Protocol), each computer will request and be assigned an address every time it’s booted up. When you have to do troubleshooting on your network, it’s annoying going to each machine to figure out what IP they have.

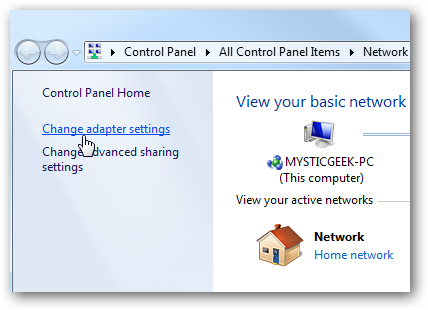
Using Static IPs prevents address conflicts between devices and allows you to manage them more easily. Assigning IPs to Windows is essentially the same process, but getting to where you need to be varies between each version.

### **Windows 7 or Windows 8.x or Windows 10**

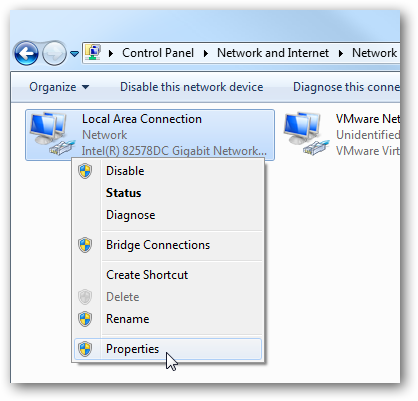
To change the computer’s IP address in Windows, type network and sharing into the Search box in the Start Menu and select Network and Sharing Center when it comes up. If you are in Windows 8.x it will be on the Start Screen itself, like the screenshot at the top of this article. If you’re in Windows 7 or 10 it’ll be in the start menu.



Then when the Network and Sharing Center opens, click on Change adapter settings. This will be the same on Windows 7 or 8.x or 10.



Right-click on your local adapter and select Properties.

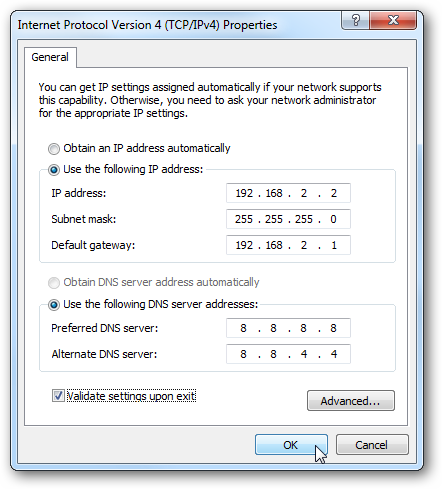


In the Local Area Connection Properties window highlight Internet Protocol Version 4 (TCP/IPv4) then click the Properties button.

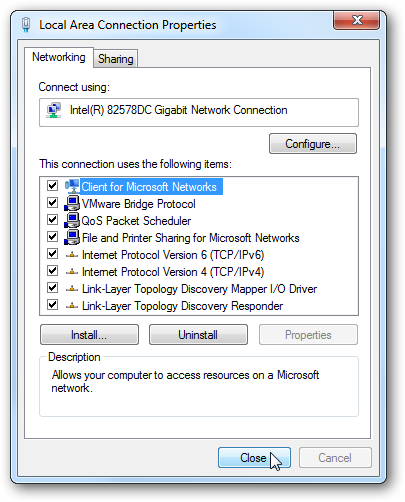


Now select the radio button Use the following IP address and enter in the correct IP, Subnet mask, and Default gateway that corresponds with your network setup. Then enter your Preferred and Alternate DNS server addresses. Here we’re on a home network and using a simple Class C network configuration and Google DNS.

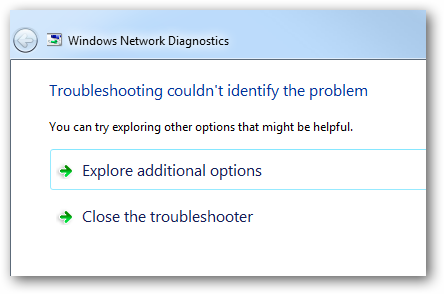
Check Validate settings upon exit so Windows can find any problems with the addresses you entered. When you’re finished click OK.



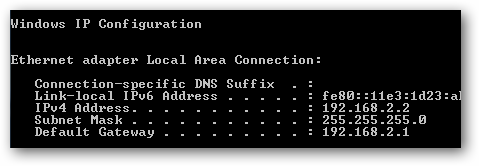
Now close out of the Local Area Connections Properties window.



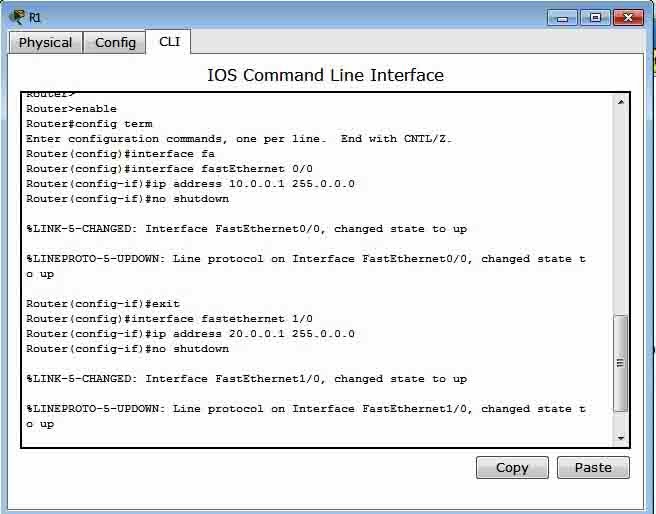
Windows will run network diagnostics and verify the connection is good. Here we had no problems with it, but if you did, you could run the network troubleshooting wizard.

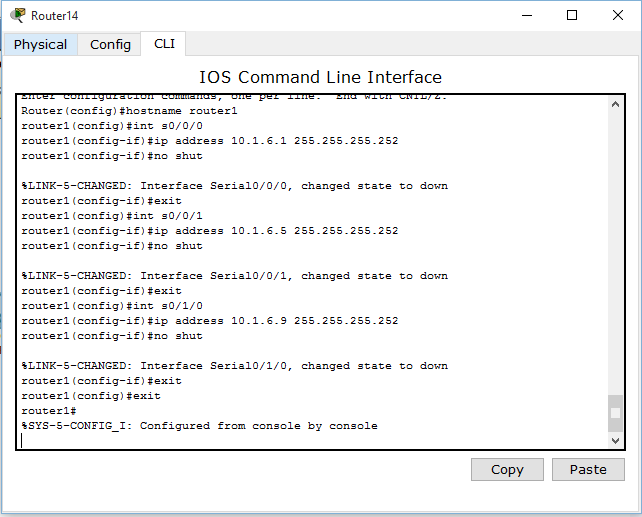


Now you can open the command prompt and do an ipconfig  to see the network adapter settings have been successfully changed.



**Giving IP address to routers**

****

****

**Subnetting**

Subnetting is a process of dividing large network into the smaller networks based on layer 3 IP address. Every computer on network has an IP address that represent its location on network. Two version of IP addresses are available IPv4 and IPv6. In this article we will perform Subnetting on IPv4.

**IPv4**

IP addresses are displayed in dotted decimal notation, and appear as four numbers separated by dots. Each number of an IP address is made from eight individual bits known as octet. Each octet can create number value from 0 to 255. An IP address would be 32 bits long in binary divided into the two components, network component and host component. Network component is used to identify the network that the packet is intend for, and host component is used to identify the individual host on network.

IP addresses are broken into the two components:

**Network component: -** Defines network segment of device.

**Host component: -** Defines the specific device on a particular network segment

**IP Classes in decimal notation**

Class A addresses range from 1-126

Class B addresses range from 128-191

Class C addresses range from 192-223

Class D addresses range from 224-239

Class E addresses range from 240-254

* 0 [Zero] is reserved and represents all IP addresses.
* 127 is a reserved address and is used for testing, like a loop back on an interface.
* 255 is a reserved address and is used for broadcasting purposes.
* In decimal notation subnet mask value 1 to 255 represent network address and value 0 [Zero] represent host address.
* In binary notation subnet mask **ON** bit [1] represent network address while **OFF** bit [0] represent host address.

**In decimal notation**

IP address 192.168.1.10

Subnet mask 255.255.255.0

Network address is **192.168.1** and host address is **10**.

**In binary notation**

IP address 11000000.10101000.00000001.00001010

Subnet mask 11111111.11111111.11111111.00000000

Network address is 11000000.10101000.00000001 and host address is 00001010

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IP Class** | **Default Subnet** | **Network bits** | **Host bits** | **Total hosts** | **Valid hosts** |
| A | 255.0.0.0 | First 8 bits | Last 24 bits | 16, 777, 216 | 16, 777, 214 |
| B | 255.255.0.0 | First 16 bits | Last 16 bits | 65,536 | 65,534 |
| C | 255.255.255.0 | First 24 bits | Last 8 bits | 256 | 254 |

**Network ID**

First address of subnet is called network ID. This address is used to identify one segment or broadcast domain from all the other segments in the network.

**Block Size**

Block size is the size of subnet including network address, hosts addresses and broadcast address.

**Broadcast ID**

There are two types of broadcast, direct broadcast and full broadcast.

**Direct broadcast or local broadcast** is the last address of subnet and can be hear by all hosts in subnet.

**Full broadcast** is the last address of IP classes and can be hear by all IP hosts in network. Full broadcast address is 255.255.255.255

The main difference between direct broadcast and full broadcast is that routers will not propagate local broadcasts between segments, but they will propagate directed broadcasts.

**Host Addresses**

All address between the network address and the directed broadcast address is called host address for the subnet. You can assign host addresses to any IP devices such as PCs, servers, routers, and switches.

**Advantage of Subnetting**

* Subnetting breaks large network in smaller networks and smaller networks are easier to manage.
* Subnetting reduces network traffic by removing collision and broadcast traffic, that overall improve performance.
* Subnetting allows you to apply network security polices at the interconnection between subnets.
* Subnetting allows you to save money by reducing requirement for IP range.

**Subnetting math**

Subnetting process involves binary math calculation. Computers communicate with each other's in binary language. To succeed in any kind of networking career, you might be fluent in binary math calculation. Subnetting needs two type of calculation, convert decimal to binary and convert binary to decimal.

Binary system works exactly same as decimal system, except the base number. Base number is 2 in binary system and 10 in decimal system. To calculate decimal equivalent value of a binary number, you have to replace base value 10 with 2. Binary numbers are displayed in columns and each position in binary system has double value than the position in right. From earlier section of this article you know that each number of an IP address is made from eight individual bits known as octet. So you should remember at least eight decimal equivalent value from binary position.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Base position** | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 |
| **Decimal value** | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

**Method of Subnetting**

In Subnetting we find the answer of following questions.

* What is subnet mask for given address?
* How many subnets does given subnet mask provide?
* What is block size for given subnet mask?
* What are the valid subnets?
* What are the total hosts?
* How many valid hosts are available per subnet?
* What is broadcast address of each subnet?
* What is network address of each subnet?

To answer above questions we use following method of Subnetting.

**What is subnet mask for given address?**

Subnetting take places when we extend the default subnet mask. We cannot perform subnetting with default subnet mask and every classes have default subnet mask. To figure out subnetted subnet mask, we first need to write down the default subnet mask. Now find the host bits borrowed to create subnets and convert them in decimal. For example find the subnet mask of address 188.25.45.48/20? This address belong to class B and class B has default subnet mask 255.255.0.0[/16 in CIDR]. We borrowed 4 bits from hosts portion. As you know subnetting move from left to right and it cannot skip any network bit. So this subnet mask in binary would be 11111111. 11111111.11110000.00000000. First two octet have default value so its decimal value would be 255.255. We will convert third octet in decimal value. To convert a binary number in decimal we add its decimal equivalent value. In our example it would be 128+64+32+16+0+0+0+0 = 240. Our fourth octet has all bits off so its decimal value would be 0+0+0+0+0+0+0+0 =0. Our answer subnet mask would be 255.255.240.0

**How many subnets does given subnet mask provide?**

To calculate the number of subnets provided by given subnet mask we use 2N , where N = number of bits borrowed from host bits to create subnets. For example in 192.168.1.0/27, N is 3. By looking at address we can determined that this address is belong to class C and class C has default subnet mask 255.255.255.0 [/24 in CIDR]. In given address we borrowed 27 - 24 = 3 host bits to create subnets. Now 23 = 8, so our answer is 8.

**What is block size for subnet mask?**

Block size or increment number is used to calculate the valid subnets. Once you figure out the block size, calculation of valid subnets become piece of cake. To figure out the block size, use this formula 256 - Subnet mask = block size. For example block size for subnet mask 255.255.255.240 is 256 - 240 = 16.

**What are the valid subnets?**

Calculating valid subnet is two steps process. First calculate total subnet by using formula 2N. In second step find the block size and count from zero in block until you reach the subnet mask value. For example calculate the valid subnets for 192.168.1.0/26.

Borrowed host bits are 2 [26-24].  
Total subnets are 22 = 4.  
Subnet mask would be 255.255.255.192.  
Block size would be 256-192 = 64.  
Start counting from zero at blocks of 64, so our valid subnets would be 0, 64,128,192.

**What are the total hosts?**

Total hosts are the hosts available per subnet. To calculate total hosts use formula 2H = Total hosts. H is the number of host bits. For example in address 192.168.1.0/26 we have 32 - 26 [Total bits in IP address - Bits consumed by network address] = 6. Total hosts per subnet would be 26 = 64.

**How many valid hosts are available per subnet?**

Valid hosts are the number of hosts those can be assigned to devices. As we know, we need to reduce two address per subnet, one for network ID and another for broadcast ID. So our formula, to calculate valid hosts would be Total hosts - 2 = Valid hosts. In above example we have 64 hosts per subnet, so valid hosts in each subnet would be 64 - 2 = 62.

**What is broadcast address of each subnet?**

Broadcast address is the last address of subnet. This address is reserve for network broadcast, and cannot be assigned to any host. In above example

0 Subnet has broadcast address 63  
64 Subnet has broadcast address 127  
128 Subnet has broadcast address 191  
192 Subnet has broadcast address 255

**What is the network address of each subnet?**

Network address is the first address of subnet. This address is used to locate the network, and cannot be assigned to any host. In above example address 0, 64,128,192 are the network address.

* Network address is always the first IP address of subnet.
* Broadcast address is always the last IP address of subnet (IP address before the next subnet).
* Valid hosts are the IP addresses between network address and broadcast address.

At this point you have powered with all essential tools for subnetting. In last section of this article we will practically implement what we have learn so far. Due to length of this article I will include examples only from class C.

**Switching**

Switching is an approach of delivering frames across the network. Switching method decides how a switch receives, processes, and forwards the frames. Switch may supports three switching methods store-forward, cut-through and fragment-free. In this article we will understand these methods in details with switching concept used by various layer two devices.

Switching concept may confuse sometime, as a lot of terms are associated with switching such as packet switching, circuit switching. These are the WAN implementation of layer 2 LAN technology. To make this process easier to understand we will start from LAN and gradually extend it to WAN.

**Collision**

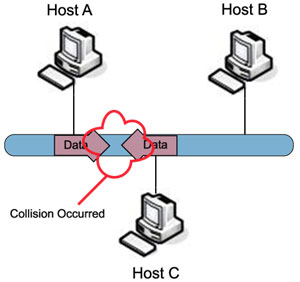
In LAN network multiple devices can share the same segment that create the collision. Collision is the effect of two devices sending transmissions simultaneously in Ethernet. When they meet on the physical media, the frames from each device collide and damaged.

**Collision domain**

Group of devices that share same collision effects over the Ethernet network.

**CSMA/CD**

It is mechanism of removing collision from network. When two or more nodes simultaneously sense the wire and found no frame, and each device places its frame on the wire. These frame would be collide in wire and a collision will occur. NIC (Network Interface Card) actually examine wire before placing any frame on it, this collision detection method is known as CSMA/CD.



If the NICs see a collision for their transmitted frames, they have to resend the frames. In this situation, each NIC that was transmitting a frame when a collision occurred creates a special signal, called a jam signal, on the wire, waits a small random time period, and examine the wire again. If no frame is currently on the wire, NIC will retransmit its original frame again.

The more devices you place on a segment, the more likely you are to experience collisions. More devices means more random time interval, creating even more collisions, greatly slowing down a device’s access when trying to transmit data.

**Switch**

Switches are data link layer devices that switch frames between different layer 2 cables or segments. Each port connected to switch has a separate collision domain.

When a frame entered into a port of switch, switch checks FCS (Frame checksum sequence) field of frame and process it only if it is valid. All invalided frames are automatically dropped. All valid frames are processed and forwarded to their destination MAC address.

Switch makes their switching decisions in hardware by using application specific integrated circuits (ASICs). Unlike generic processor such as we have in our PC, ASICs are specialized processors built only to perform very few particular tasks. In cisco switch ASICs has single task, switch frames blazingly fast. For example an entry level catalyst 2960 switch has frame rate of 2.7 million frames per second. Higher end switches have higher FPS rate such as Catalyst 6500 has a rate of 400 million FPS rate.

Basically switch perform three main tasks

1. Learn where the devices are located and store their location in MAC table.
2. Forward frame intelligently based on MAC address of frame
3. Removing layer 2 loops.

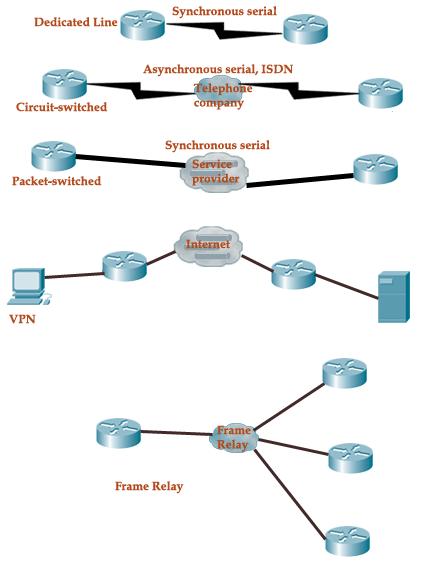
**Address function of switch**

* Switch stores MAC address in MAC address table.
* MAC table is also known as port or CAM address table.
* When a frame enters into the port, switch examines the source MAC address and compares it with its CAM (Content Addressable Memory) table.
* If switch doesn’t see a corresponding entry in the CAM table, it will add the source MAC address to the table, including the source port identifier.
* If switch found address in CAM table, then it compare associated entries and update them.
* Whenever the switch updates an entry in the CAM table, the switch also resets the timer for the specific entry.
* Switch uses timer to remove older information automatically. Switches may have different default timer.
* MAC address table can be built statically or dynamically.
* All dynamic entries are automatically flushed when you turn off the switch.
* When you power on a switch it has an empty CAM table or static entries in it (if you have configured any).
* All identified frames are forwarded only from specific ports that have corresponding addresses.
* All unidentified frames (frames those MAC address are not available in CAM table) are flooded from all ports.
* Three types of frames; Unknown Unicast address frame (Unidentified frame), broadcast frame and multicast frame are always flood out from all possible ports except to the port on which the frame came in.

**Type of Switching**

In the starting of this article we have divided switching concept in two terms LAN and WAN. So far we have explained switching in LAN terms, now in remaining article would focus on WAN terms.

WAN supports a number of switching types, among those following are the most popular and covered in CCNA Exam objectives.



**Dedicate Line**

This is usually known as leased line or point to point connection. In this type of connection, lines remain always open. You have to pay for all times whether you transmit data or not. HDLC and PPP encapsulations are used for this type of connection. This is the most expensive method of data transmission. It uses synchronous serial lines.

**Circuit Switching**

It uses asynchronous serial lines. You only need to pay when actual data transmits. It works like a telephone call where you only need to pay for call duration. In circuit switch, we need to established connection every times whenever we have data to transmit. Circuit switching uses dial-up modems or ISDN. It is suitable for low-bandwidth data transfers.

**Packet Switching**

In this method you share bandwidth with other companies. This is cost effective simulation of lease line. It is suitable for bursty type data transmission. VPN and frame really are two popular implementations of this method.

**VPN**

VPN (Virtual Private Network) is an extended private network over the public network such as internet. VPN enables us to transmit data across the shared public networks. We need to implement data encryption and security polices to ensure data integrity. Major implementations of VPN include Open VPN and IPsec.

**Frame Relay**

Frame Relay is the cost effective switching method. Frame relay breaks data in variable size units, known as frames. It does not implement any error correction solution in carrier. In this technology any necessary error correction methods need to be setup on end devices. This speeds up over all data transmission.

**Routing**

As you already know, routers look at the destination IP address of a packet and route it to the destination. Though the routing process itself is easy, building a list of networks, called the routing table, is not as easy. This chapter looks at the IP routing process itself and various ways to build to the routing table.

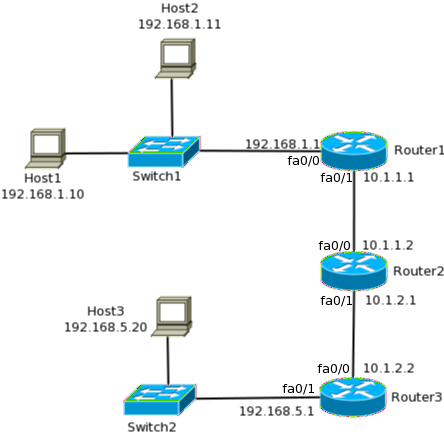
**Understanding IP Routing**

In the simplest terms, IP Routing is the process of moving packets from its source to its destination across internetworks. To be able to route packets, a router must know at a minimum the following:

* Destination address
* Neighbor routers from which it can learn about remote networks
* Possible routes to all remote networks
* The best route to each remote network
* Be able to maintain and verify routing information

Unfortunately the process is not as simple as it sounds because it involves multiple protocols at multiple layers. To understand the complete process of how a packet moves from the source to the destination, consider the network shown in Figure 4-1.

**Figure 4-1** *Understanding IP Routing*

**

In the network shown above, when Host1 sends a TCP segment to Host3, the following happens:

1. The TCP segment is handed off to IP, which adds a header consisting of the source address, 192.168.1.10 and destination address 192.168.5.20 and hands off that packet to the next layer.
2. Using the subnet mask of the host, it is determined that the destination address lies in a remote network and hence the packet must be sent to the default gateway, 192.168.1.1. So Host1 sends out an ARP request to find the MAC address of Router1. When a response is received, it frames the packet with the source MAC address of Host1 and destination MAC address of Router1.
3. When Router1 receives the frame, it strips of the header and trailer and looks at the destination address in the IP header. Since the packet is not destined to Router1, it must be routed out.
4. It tries to match the destination address to a list of known networks, called the routing table. It finds that the destination network is reachable via Router2, so it frames the packet with the source MAC address of its exit interface (interface with the IP address of 10.1.1.1) and the destination address of Router2’s interface.
5. When Router2 receives the frame, it repeats the strip and lookup process and frames the packet again before sending it to Router3. This time the MAC address of Router2’s exit interface is the source address while the MAC address of Router3 is the destination address.
6. Finally Router3 looks at the destination MAC address and realizes that the destination network is directly connected. It finds the MAC address of the destination host and frames the packet using its own MAC address as the source while the MAC address of Host3 as the destination address. At last the frame is sent out and reaches the destination host.
7. At the destination, the frame is stripped and the destination IP address is verified. Then the IP header is stripped and the TCP segment reaches Layer 4 of the destination.
8. Now when Host3 needs to reply back to Host1, TCP will hand off the reply segment to IP.
9. IP will add a header consisting of a source address of 192.168.5.20 and a destination address of 192.168.1.10 and will send it to layer 2 for framing.
10. By the subnet mask of Host3, it is determined that the destination lies in a remote network. Hence the frame will need the MAC address of the default gateway as destination. If Host3 does not have the MAC address of Router3, it will send an ARP query to get it. Once Host3 has the MAC address, it will frame the segment and send it out to Router3.
11. Router3 strip the frame header and look at the destination IP address in the IP header. From its routing table, it will know that the packet needs to go to Router2. It will frame the packet with a source MAC address of its fa0/0 interface and the destination MAC address will be the address of Router2’s fa0/1 interface and then send it out to the wire.
12. Router2 receives the frame and repeats process to send the packet to Router 1.
13. Router1 receives the frame from Router2 and removes the frame. By the destination IP address it knows that the packet belongs to a directly connected interface.
14. Since it received a frame from Host1 earlier, it has the MAC address of the host mapped to its IP address in the ARP table. The router uses that to create a frame with its fa0/0 interface’s MAC address as source and Host1’s MAC address as destination and sends the frame out the interface.
15. When Host1 receives the frame, it verifies the destination address, strips the frame and IP header and sends the TCP segment to layer 4.

# **Routing protocol types & concept of administrative distance**

The routing protocols are created for the routers. These protocols are designed to permit the exchange of the routing tables or the known networks between the routers. There are a variety of routing protocols based on the specific network. The administrative distance helps to select the best path when 2 or more routes to a same destination from the 2 different routing protocols. Let us see more about the routing protocol types and the concepts of the administrative distance in the coming section.

**Distance vector**

The distance vector is one among the routing protocol. It uses the Ford Fulkerson algorithm, Bellman ford algorithm or the DUAl FSM (for Cisco) calculate the paths. The neighbors are the routers which share the link and that are configured to use a same routing protocol. A router is the only one aware of a network address of its own interface as well as a remote network address, it will reach via its neighbor. The routers with uses the distance vector routing will never aware of a network topology. The best examples of the distance vector routing protocols are such as:

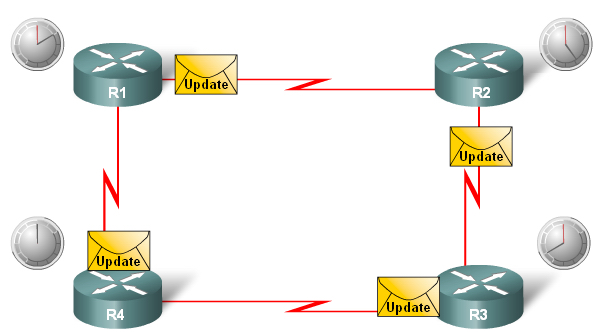
**Routing information protocol (version 1 &2)**

The metric of the RIP is hop count and the routing update sent is 30 seconds.

**Enhanced interior gateway routing protocol**

The metric of the EIGRP is the proprietary protocol and hybrid. The routing update sent is a topology change triggers.

The periodic updates of the distance vector routing protocol is 30 to 90 seconds and the broadcast updates are 255.255.255.255.



The entire routing table is included with the routing table. The distance vector routing protocol just requires less maintenance and simple implementation only. The level of knowledge needs to deploy and also maintain the network with this protocol is not so high like other protocols. It typically do not require a large number of memory to save the information and nor do they need the powerful central processing unit. Based on the network size and an IP addresses implemented, it typically do not need the high level of link bandwidth to send the routing updates. Anyway, it can become the problem if the distance vector protocol is deployed in the large network.

The use of a periodic update will cause the slow convergence in this protocol. However, if some of the advanced techniques are used such as the triggered updates. The overall convergence is slow when compared to the link state routing protocols. The slow convergence can limit the network size, because the larger networks need much time to propagate the routing information. The routing loops will occur when the inconsistent routing table is not updated due to the slow convergence in the changing network. The core of the distance vector protocol is a routing algorithm. This algorithm is widely used to calculate the paths and this algorithm is defined in the following processes are:

Mechanism for sending and also receiving the routing information

Mechanism for calculating the paths and also installing routes in a routing table.

Mechanism for identifying and reacting to the topology changes.

Different routing protocols will use different algorithms to install the routes in a routing table and sends updates to the neighbors and also make path determination decisions.

## Link state

The link state routing protocol is the major class of the routing protocols used in the packet switching network for the computer communications. The best example of the link state routing protocol is IS-IS (intermediate system to intermediate system) and OSPF( open shortest path first.

The link state protocol is performed by each switching node in a network. The main concept of this protocol is that each node constructs the map of the connectivity to a network, which nodes are connected with other nodes. Every node will independently calculate a next logical path from that to each possible destination in a network. This collection of the best path will form the node routing table. The link state packet, or the link state advertisement is the small packet of the routing information which is sent in between the routers. The SPF algorithm is the calculation performed on a database which results in an SPF tree. The link state database or topological database is the collection of the information which is gathered from the LSAs.

In the link state routing algorithm, each router has the responsibility for meeting its neighbors as well as learning its names. It used the Hello protocol, that send the data packet contains RID and the network address on which the packets are being sent.

Each router constructs the LSA or LSP which is comprised of the cost for every neighbor and list of names. The LSA/LSP is transmitted to the entire routers. Each router saves the very recently generated LSA/LSP from the every other router. The Dikjstra's algorithm is also known as the SPF - shortest path first algorithm.

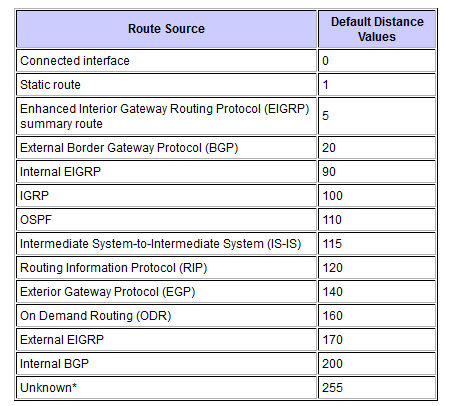
In the process, the routers will first learn of directly connected networks, after that the routers will say hello to neighbors which will link the state packets. Then the routers flood the LSP to all the neighbors. Finally, the routers use the LSP database to build the network topology map and also to calculate the perfect path to each destination. After initial flooding, the additional LSP will send out when the change in the topology occurs.

**Describe administrative distance**

Most of the routing protocols have the metric structures as well as algorithms which are not at all compatible with the other protocol. In the network with multiple routing protocol, the capability to select the perfect path and exchange of the route information across the multiple protocol is very critical.

Administrative distance is the suitable feature that the routers will use to select the perfect path when there are 2 or more different routes to a same destination from the 2 different routing protocol. Generally, AD (administrative distance) is an arbitrary numerical value that assigned to the routing protocol. The AD value is used by the Cisco routers to find the best route which should be used in the multiple paths to the exist same destination. The routing protocol with the lower AD is better and provide priority for the routing protocol with higher AD. This AD value can be set manually by the network administrator. If the network administrator fails to set it properly, then the router will use the default AD.

The Ad defines a reliability of the routing protocol. Every routing protocol is prioritized to the least reliable using the Ad value. The below table shows the default AD value of the protocols.



The administrative distance is the numeric value which ranges from 0 to 255. The smaller the AD is more trusted by the router, hence, the best AD being 0 and the far worst is 255. The AD is the initial criterion that the router uses to find which routing protocol to use, and if 2 protocols offer route information for a same destination. It is the measure of the source trustworthiness of a routing information. The AD has only the local significance and it is not advertised in the routing updates.

When the route redistribution is used, then it is required to change the AD of the protocol. Suppose, if you like to chose the RIP learned routers instead of IGRP learned routes to a same destination, then you has to decrease the AD of the RIP to less than 100 or increase the AD for the IGRP to 120+.

You can change the AD of the protocol via the distance command in a routing process of the sub configuration mode. Then this command indicates that the AD is assigned to a route learned from the specific routing protocol. When migrating the network from the one protocol to the other, use this procedure and later has the higher AD.

In some cases, the AD can lead to unexpected results or lead to being chosen which is not essential for the best route. It is true, if the routing destination is used on the router. In that case, the administrator would modify the AD manually, so that a desired routing protocols path takes the precedence over the other paths. The static routes can be used to offer the alternative path when the link fails. To configure the static routes as the backup, the static route's AD has to be adjusted. Or else, it will take the precedence over the entire routing protocol and the routes provided from the routing protocol cannot be inserted into a routing table.

The routing protocols are effectively distributed database systems. It propagates the information about the network topology among the routers within the network. The 3 main types of the routing protocols such as distance vector, link state and path vector widely used. By distributing the vector, it classified into distance vector and path vector and by means of distributing the state of the links, it is classified as a link state routing. Based on the needs and requirements of the network topology, those types of routing protocols are used. When there are 2 or more different routes on to the same destination, the Administrative distance is the one which helps to select the best path.

**RIP-:**

* + RIP Stands For Routing Information protocol
  + It Is a Industry standard Dynamic Routing Protocol
  + IT Is not a More Intelligent Dynamic Routing Protocol
  + It Is Basically Use For Smaller Size Organization
  + It Support Maximum 15 Routers in the Network. 16 Router Is Unreachable
  + It is denoted By R in Routing Table.
  + It’s Administrative Distance Is 120.
  + In RIP Routing protocol We Can not create A Separate Administrative boundary in The Network.
  + It Calculate the Metric In Terms Of Hop Count From source Network to destination Network. Lower the Hop count that Is the Best route For That Particular Network.
  + It works on Bellman Ford algorithm
  + RIPV.1 Do Not Support VLSM
  + RIPV.2 Support VLSM

**EIGRP-:**

* + EIGRP Stands For Enhanced Interior Gateway Routing protocol
  + It Is a Cisco standard routing protocol
  + It Is a More Intelligent routing protocol Than RIP And IGRP
  + It Is Basically Use For Medium to Lager Size Organization in the network.
  + It supports Maximum 255 Routers in The Network
  + It’s Administrative distance Is 90
  + It calculates the Metric In Terms Of Bandwidth And delay
  + EIGRP Works on DUAL(Diffusing Update Algorithm) Algorithm
  + EIGRP is denoted by D in Routing Table.
  + EIGRP Supports VLSM
  + EIGRP Creates three table In the Router

**OSPF-:**

* + OSPF stands For Open shortest path First
  + It Is A Industry standard Routing protocol
  + It supports Unlimited router in the Network
  + It Is Denoted By O in routing Table
  + It’s Administrative distance is 110
  + It Is basically Use For Larger Size Organization in The Network
  + In OSPF Routing protocol We Can Create a separate administrative boundary in the Network through Area No. within The same area all of The routers Are exchanging The Route information From Neighbor router in the network.
  + It Calculates the Metric in terms of Bandwidth
  + OSPF works on DIJKSTRA Algorithm
  + It Is a More Intelligent routing protocol
  + OSPF Supports VLSM
  + OSPF Routing protocol Creates three Table in the router—

**CHAPTER 2**

LITERATURE SURVEY

In Design and Implementation of Organization Network This focuses on network design using bus topology which will be used for an entire university and every user of the network will be interlinked with each other. Research work proposes a novel approach to communicate among various users that are present at different sites at the same time. Departments will share information among faculty members and students where the whole university works on a single network which includes various facilities such as transmitting messages, accessing data on any physical computer within the network, accessing same speed in various geographical areas within university network.

**Proposed approach** takes the help of sharing common network domain by DNS and applies heterogeneous BUS topology model to explore various concepts like topology design, creating dynamic host configuration protocol, sub net masking, DNS and VLAN within a single network with the help of Cisco Packet Tracer to make the network more secured and cost effective.

In Network Security and Management . This focuses on the designing of the organization area network using star topology and the project comprises of the different Departments of a organization spread in different buildings. Multiple Routing protocols have been used in different branches and all the departments can communicate with other different departments through the redistribution among different Routing Protocols. It has a DHCP server for assigning the IP Addresses to the Hosts in the building as well as a DHCP server has been used in the other Buildings as well.

The Internet Service Provider has been used for Communication of the Buildings of Organization with the Data Centre & Internet through ISP, using the Frame Relay Switching Technology available for Wide Area Network. Routing Protocol EIGRP, Static Routing & its concepts including the Default Routing as well has been applied. The different Routing Protocols are running and which has been synchronized to work with Frame Relay Switching Technology.

In Security Problems in Organization Problems and its solutions . This focuses on the importance of network security and services at higher education institutions. Users and institutions are demanding more and more network services and the exchange of more potentially sensitive information within these services. Firstly, in Organization there is definite requirement of the network access and building Organization network has become crucial. The Organization network has a number of tasks such as teaching, research, management and communication with the outside.

Therefore, the issue of network security has become a priority to Organization network management. Obviously, the current Internet is convenient but at the same time it is unsafe. While using network services in Organization area network it can be more easily attacked. This paper represents the current security status of the Organization network, analyze security threats to Organization network and describe the strategies to maintain robust network system

In Design and Implementation of a Secure Organization Network This focuses on network attacks. There are various types of attacks such as Passive Attack, Active Attack, Distributed Attack, Insider Attack, Close-in Attack, Phishing Attack, Hijack attack, Spoof attack, Buffer overflow, exploit attack, Password attack. Denial of service (DoS) is a interruption of service either as a result of the system is destroyed, or as a result of it‘s quickly out of stock. ARP spoofing could be a style of attack during which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over Local Area Network (LAN). This ends up in the linking of associate attacker's mackintosh (MAC) (address with IPaddress) of a server on the network.

**CHAPTER 3**

FEASIBILITY STUDY:

**3.1 Overview**

“Feasibility Study” is a test of the system according to its workability, impact of the organization, ability to meet user needs and effective use of the resources.

We can test our system by different type of the feasibilities.

**3.2 Technical Feasibility:** A study of resource availability that may affect the ability to achieve an acceptable system. This evaluation determines whether the technology needed for the proposed system is available or not. This system can be made in any language that support good user interface and easy database handling. Technical needs may include:

**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.Cisco Packet Tracer is one of the most useful visual simulation programs for networking certifications, such as CCNA

**3.3 Economic Feasibility**:

In this we consider following costs:

The cost to conduct a full system investigation.

The cost of hardware and software for class of application being considered.

The benefit in the form of the reduced cost.

Our system is a Network security system. It can be simulated in packet tracer which is not practical implementation .It is virtual implementation. Packet Tracer Implementation cost Nothing but in actual implementation we require organization and we have to configure router and switches .The cost for making this system is not much but for physical implementation we require huge network devices.

3**.4 Schedule Feasibility**: Time evaluation is most important consideration in development of the project. So the project is concerned should be completed with fixed in scheduled time as far as company is concerned. New system is not so much big so it is easy to make in few days.

**3.5 Behavioral Feasibility:**People are inherently resisted to change and a computer means “change is the only certainty”. An estimate should be made of how strong a reaction the user staff in going to have towards development of new system. The personal of the user organization will be affected by the proposed system. As the aim of the system is only to satisfy the information needs, no employees will loose their position by the proposed system.

In fact the proposed system will help the organization in reducing the voluminous work involved. Also the involvement of users in every stage of the project is going to increase the success factor. Thus special efforts can be made to educate and train the staff. The purposed system provide more secured environment in the organization no person gets affected .It provides great security to organization

**5. Operational Feasibility:**

In this feasibility we consider following points:

* What changes will be brought with the system.
* What new skills will be required? Do the existing staff members have these skills? If not, can they be trained in due course of time?

In This System Network Engineer can configure access control .He can add restrictions to users and also he can fool intruders by Network Address Translation(NAT).

**CHAPTER 4**

SYSTEM ANALYSIS:

## Software and Hardware Requirements

To implement this project we have to meet some software and hardware requirements.

For Software Requirement it is required to have (CISCO PACKET TRACER) installed on the System. Every implementation is doneon thistool.

For Hardware Requirement it is required to have the followings

* Intel Pentium4,2.53GH zor equivalent Processor
* 2 GB Ram
* 1GB of free storage space
* Display of resolution 1024\*768
* Language font supporting Unicode encoding
* Latest videocard and OS updates

### CiscoPacketTracer

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems thatallows users to create network topologies and imitate modern computer networks. Thesoftware allows users to simulate the configuration of Cisco routers and switches using asimulatedcommandlineinterface.PacketTracermakesuseofadraganddropuserinterface,allowing users to add and remove simulated network devices as they see fit. The software ismainly focused towards Certified Cisco Network Associate Academy students as aneducational tool for helping them learn fundamental CCNA concepts. Previously studentsenrolled in a CCNA Academy program could freely download and use the tool free of chargeforeducational use.

Packet Tracer can be run on Linux, Microsoft Windows, and macOS. Similar Android andiOS apps are also available. Packet Tracer allows users to create simulated networktopologies by dragging and dropping routers, switches and various other types of networkdevices. A physical connection between devices is represented by a 'cable' item. PacketTracer supports an array of simulated Application Layer protocols, as well as basic routingwith RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum. Asofversion 5.3,Packet Tracer alsosupports theBorderGateway Protocol.

In addition to simulating certain aspects of computer networks, Packet Tracer can also beused for collaboration. As of Packet Tracer 5.0, Packet Tracer supports a multi-user systemthatenablesmultipleuserstoconnectmultipletopologiestogetheroveracomputernetwork.PacketTraceralsoallowsinstructorstocreateactivitiesthatstudentshavetocomplete.

Packet Tracer is often used in educational settings as a learning aid. Cisco Systems claimsthatPacket Tracer is usefulfor network experimentation.

Packet Tracer allows students to design complex and large networks, which is often notfeasible with physical hardware, due to costs. Packet Tracer is commonly used by CCNAAcademy students, since it is available to them for free. However, due to functionallimitations, it is intended by CISCO to be used only as a learning aid, not a replacement forCisco routers and switches.

It ispossible to practice all of the IOS commands that might be required. Packet Tracer can beuseful for understanding abstract networking concepts, such as the Enhanced InteriorGateway 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.

**CHAPTER 5**

SYSTEM DESIGN

Introduction:

In this project we created Organization area network topology using cisco packet tracer. We used bus topology to design the Organization network. Organization consists of COMPUTER LAB 1(Web Developers), COMPUTER LAB 2(App Developers), COMPUTER LAB 3(Business Analyst), STAFF ROOM, Inter vlan,Acl. As every entity is in different network we created virtual LANs in which with the help of inter VLAN routing we can communicate with different networks. The server consists of Yahoo(DHCP), youtube(DHCP), IIT DELHI(DHCP), Gmail(DHCP), DNS Server, Technoheer(Organization), Zcc india, Zcc india.

Problem Statement:

Organization network faces the security challenges which are influenced by network infrastructure. To maintain data privacy and organization integrity the company network needs to have secure network design to protect from different types of threats and attacks. The aim of this project is to build a secured company network design, which can defend against specified attacks.

**Elements used in project**

**Access Control lists**

Cisco Access Control Lists are the set of conditions grouped together by name or number. These conditions are used in filtering the traffic passing from router. Through these conditions we can filter the traffic; either when it enters in router or when it exits from router.

**What is access control list?**

Basically ACL is the integrated feature of IOS software that is used to filter the network traffic passing through the IOS devices. Network traffic flows in the form of packets. A packet contains small piece of data and all necessary information which are required to deliver it. By default when a router receives a packet in interface, it takes following actions:-

* Grab destination address from the packet
* Find an entry for destination address in routing table
* If match found, forwards the packet from associate interface
* If no match found, discard the packet immediately.

This default behaviour does not provide any security. Anyone who know the correct destination address can send his packet through the router. For example following figure illustrates a simple network.

In this network, no security policy is applied on router. So router will not be able to distinguish between user’s packet and adversary’s packet. From router’s point of view, both packets have correct destination address so they should be forwarded from exit interface.

Suppose we tell the router that only 10.0.0.10 has the right to access the 30.0.0.1. To match with this condition router will take following actions:-

* Grab source and destination address from the packet
* Match both addresses with given condition
* If packet is not arrived from 10.0.0.10, drop the packet immediately.
* If packet is not intended from 30.0.0.1, drop the packet immediately.
* If both condition match find an entry for destination address in routing table
* If match found, forwards the packet from associate interface
* If no match found, discard the packet immediately.



Now only the packets from 10.0.0.10 are allowed to pass from router. With this condition adversary will not be able to access the server. We can create as much conditions as we want. Technically these conditions are known as ACLs. Besides filtering unwanted traffic, ACLs are used for several other purposes such as prioritizing traffic for QoS (Quality of Services), triggering alert, restricting remote access, debugging, VPN and much more. Due to complexity, these uses of ACLs are not tested in CCNA level exams. CCNA level exams test only basic uses of ACLs such as filtering the traffic and blocking specific hosts.

Okay now we have basic understating of what ACLs are and what they do. In next section we will understand technical concept of ACLs.

**Direction and location of ACLs**

A packet interacts with three locations during its journey from router:-

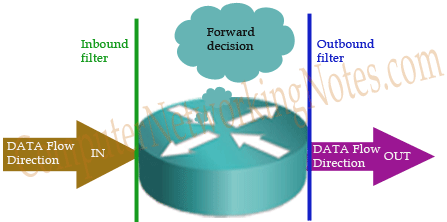
1. Packet arrives in interface (Entrance)
2. Router makes forward decision
3. Packet outs from interface (Exit)

We cannot filter the packet in the middle of router where it makes forward decision. Decision making process has its own logic and should not be interfered for filtering purpose. After excluding this location, we have two locations; entrance and exit. We can apply our ACLs conditions on these locations.

ACL conditions applied on entrance work as **inbound** filter. ACL conditions applied on exit work as **outbound** filter.

Inbound ACLs filter the traffic before router makes forward decision. Outbound ACLs filter the traffic after the router makes forward decision.

An ACL filter condition has to two actions; permit and deny. We can permit certain types of traffic while blocking rest or we can block certain types of traffic while allowing rest.



**Key points**

* We must have to apply ACLs on interface which process the packet.
* ACLs must be applied in data flow direction. Inbound ACLs must be placed in entrance interface. Outbound ACLs must be placed in exit interface.

|  |  |  |
| --- | --- | --- |
| **Router without ACLs** | **Router with inbound ACLs** | **Router with outbound ACLs** |
| Packet enters in router. | Packet enters in router. | Packet enters in router. |
| Grab source and destination address from the packet | Grab source and destination address from the packet | Grab source and destination address from the packet |
|  | *Run ACL conditions to determine the action. If deny condition matches, drop the packet immediately. If permit condition matches, let the packet enter in router.* |  |
| Find an entry for destination address in routing table | Find an entry for destination address in routing table | Find an entry for destination address in routing table |
| If match found, forwards the packet from associate interface. If no match found, discard the packet. | If match found, forwards the packet from associate interface. If no match found, discard the packet. | If match found, forwards the packet from associate interface. If no match found, discard the packet. |
|  |  | *Run ACL conditions to determine the action. If deny condition matches, drop the packet immediately. If permit condition matches, let the packet out from interface.* |
| Packet outs from router. | Packet outs from router. | Packet outs from router. |

* Once applied, ACL will filter every packet passing through the interface.

Types of ACLs

There are two types of ACLs:

1. Standard ACLs (1 – 99 and 1300 - 1999)
2. Extended ACLs (100 – 199 and 2000 - 2699)

### Standard ACLs (1 – 99 and 1300 - 1999)

ACLs are the part of Cisco IOS from its beginning. In earlier days simple filtering was sufficient. Standard ACLs are used for normal filtering. Standard ACLs filter the packet based on its source IP address.

### Extended ACLs (100 – 199 and 2000 - 2699)

Over the time security becomes more challenging. To mitigate current security threats, advance filtering is required. Extended ACLs takes this responsibility. Extended ACLs can filter a packet based on its sources address, destination address, port number, protocol and much more.

### Named ACLs

Named ACLs are the extended version of existing ACLs. Named standard ACL is the extended version of standard ACL. Named extended ACL is the enhanced version of extended ACL. Existing ACLs (Standard and Extended) assign a unique number among all the ACLs. While Named ACLs assign a unique name among all the ACLs.

I will explain above ACLs in detail with examples in next parts of this article.

**NAT**

When communicating to devices in a public network, your device needs to use a source address that is a public address. NAT device enables private IPv4 to connect to the Internet. NAT enable you to change an IP address in a packet to a different address. Usually, NAT connects two networks and translates the private (inside local) addresses into public addresses (inside global) before packets are forwarded to another network. In other word Address translation allows you to translate your internal private addresses to public addresses before these packets leave your network.

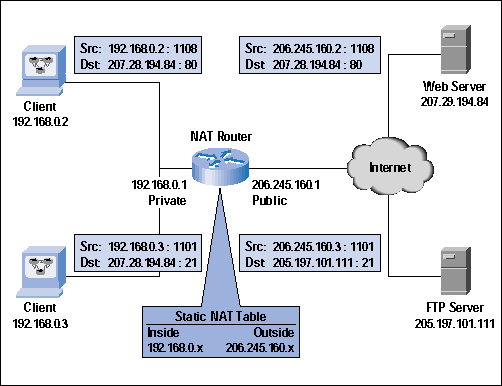
### Situation where you should use NAT

* Your ISP did not provide you sufficient public IP address
* Your company is going to merge in a company which use same address space
* Where you want to hide your internal IP address space from outside
* You want to assign the same IP address to multiple machines

### There are three types of NAT

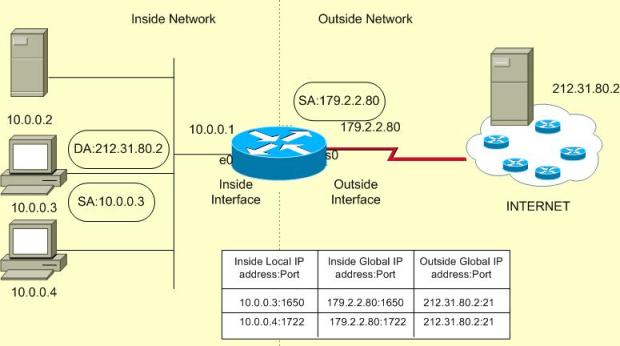
* Static
* Dynamic
* PAT

## STATIC NAT



In static NAT manual translation is performed by an address translation device, translating one IP address to a different one. If you have 100 devices, you need to create 100 static entries in the address translation table. Typically, static translation is done for inside resources that outside people want to access.

## Dynamic NAT

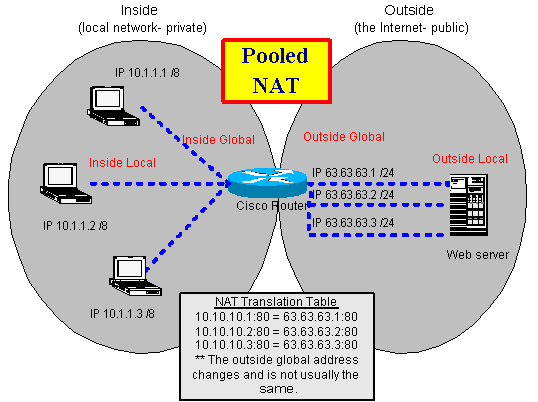


Dynamic NAT is mostly used when inside users needs to access outside resources. The global address assigned to the internal user isn't important, since outside devices don't directly connect to your internal users they just return traffic to them that the inside user requested.

Dynamic NAT is used when inside use wants to access external resource. When an inside user sends traffic through the address translation device, say a router, it examines the source IP address and compares it to the internal local address pool. If it finds a match, then it determines which inside global address pool it should use for the translation. It then dynamically picks an address in the global address pool that is not currently assigned to an inside device. The router adds this entry in its address translation table, the packet is translated, and the packet is then sent to the outside world. If no matching entry is found in the local address pool, the address is not translated and is forwarded to the outside world in its original state.

When returning traffic comes back into your network, the address translation device examines the destination IP addresses and checks them against the address translation table. Upon finding a matching entry, it converts the global inside address to the local inside address in the destination IP address field of the packet header and forwards the packet to the inside network

## PAT



With PAT, all devices that go through the address translation device have the same global IP address assigned to them, so the source TCP or UDP port numbers are used to differentiate the different connections. If two devices have the same source port number, the translation device changes one of them to ensure uniqueness.

Major difference between NAT and PAT is In NAT Only IP addresses are translated (not port numbers).

### Disadvantages of Address Translation

Three main disadvantage with address translation are:

* Each connection has an added delay.
* Troubleshooting is more difficult.
* Not all applications work with address translation.

## Address Translation Terms and Types

|  |  |
| --- | --- |
| **Term** | **Explanation** |
| Inside | Addresses located on the inside of your network |
| Outside | Addresses located outside of your network |
| Local | The IP address physically assigned to a device |
| Global | The public IP address physically or logically assigned to a device |
| Inside local IP address | The IPv4 address that is assigned to a host on the inside network |
| Inside global IP address | A legitimate IPv4 address assigned by the ISP that represents one or more inside local IPv4 addresses to the outside world |
| Outside global IP address | An outside device with a registered public IP address |
| Outside local IP address | An outside device with an assigned private IP address |
| Static NAT | A manual address translation is performed between two addresses and possibly port numbers. |
| Dynamic NAT | An address translation device automatically performs address translation between two addresses and possibly port numbers. |
| Port Address Translation (PAT) | Many inside IP addresses are translated to a single IP address, where each inside address is given a different TCP or UDP port number for uniqueness. |

**DHCP**

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as

Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

A DHCP server automatically sends the required network parameters for clients to properly communicate on the network. Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client’s lease for that IP address has expired.

**InterVLANRouting (Router on stick method)**

• Inter VLAN routing is a process in which we make different virtual LANs

Communicate with each other irrespective of where the VLANs are present(on

Sames with or different switch).

• Inter Vlan Routing can be achieved through a layer-3 device

i.e. Router or layer-3 Switch. When the Inter VLAN Routing is done through

Router it is known as Router on a stick.

**Internal Security**

1. ARP Spoofing (ARP Poisoning)

• It is used for resolving IP addresses to machine MAC addresses. All the devices which

Want to communicate in the network , broadcast ARP-queries in the system to find out

the MAC addresses of other machines.

• ARP Spoofing constructs a huge number offorced ARP requests and replies packets

To overload the switch. The intention of the attacker all the network packets ands witch

setinforwardingmode.

2. DHCP Snooping

• DHCP snooping is done onswitches that connects end devices to prevent DHCP

Based attack. Basically DHCP snooping divides interfaces of switch into two parts

• Trusted Ports–Allthe portswhichconnects managementcontrolled devices like

switches,routers,serversetcaremadetrustedports.

• Untrusted Ports–Allthe portsthat connect end devices like PC,Laptops,Access

Point set care made untrusted port.

Software Requirements:

1. 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.

 It can be run on Linux, Microsoft Windows, and macOS.

 It 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.

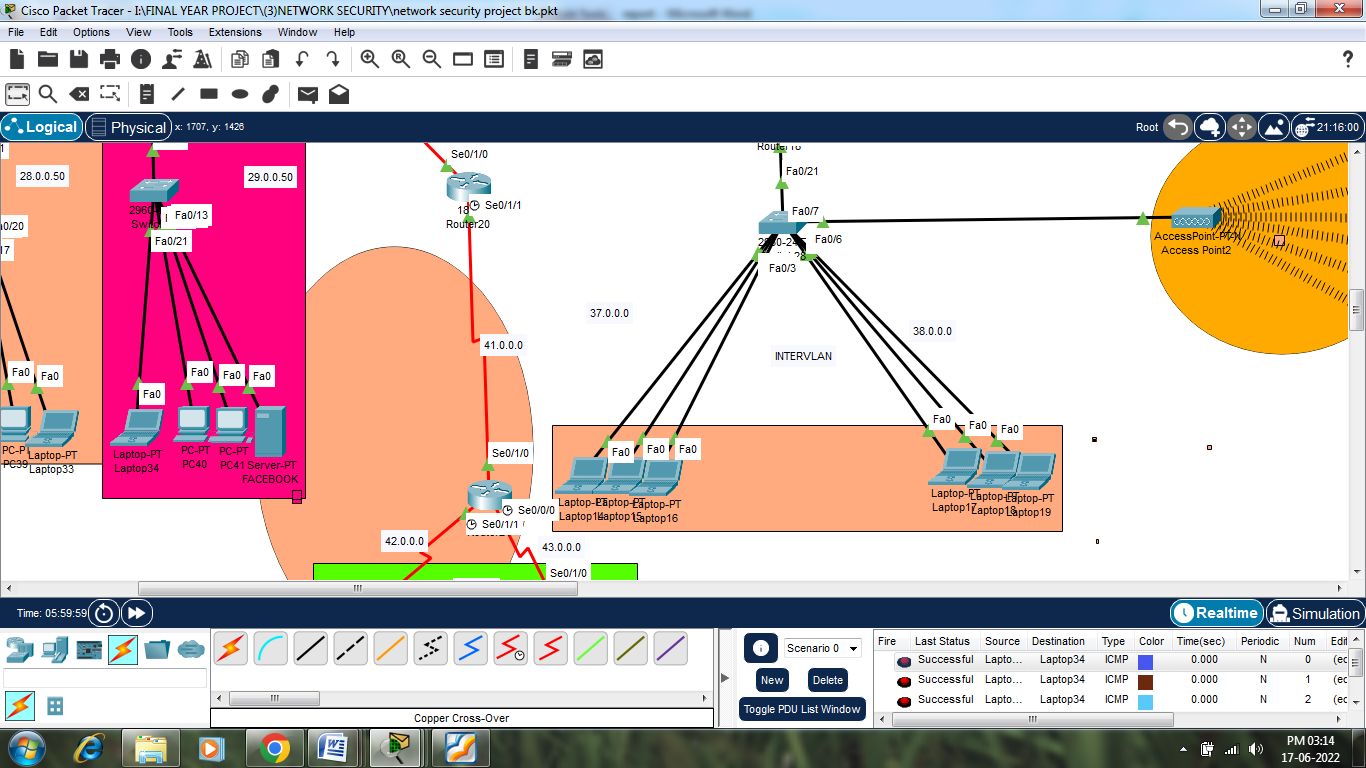
InterVLAN Routing (Router on a stick Method):

 Inter VLAN routing is a process in which we make different virtual LANs communicate with

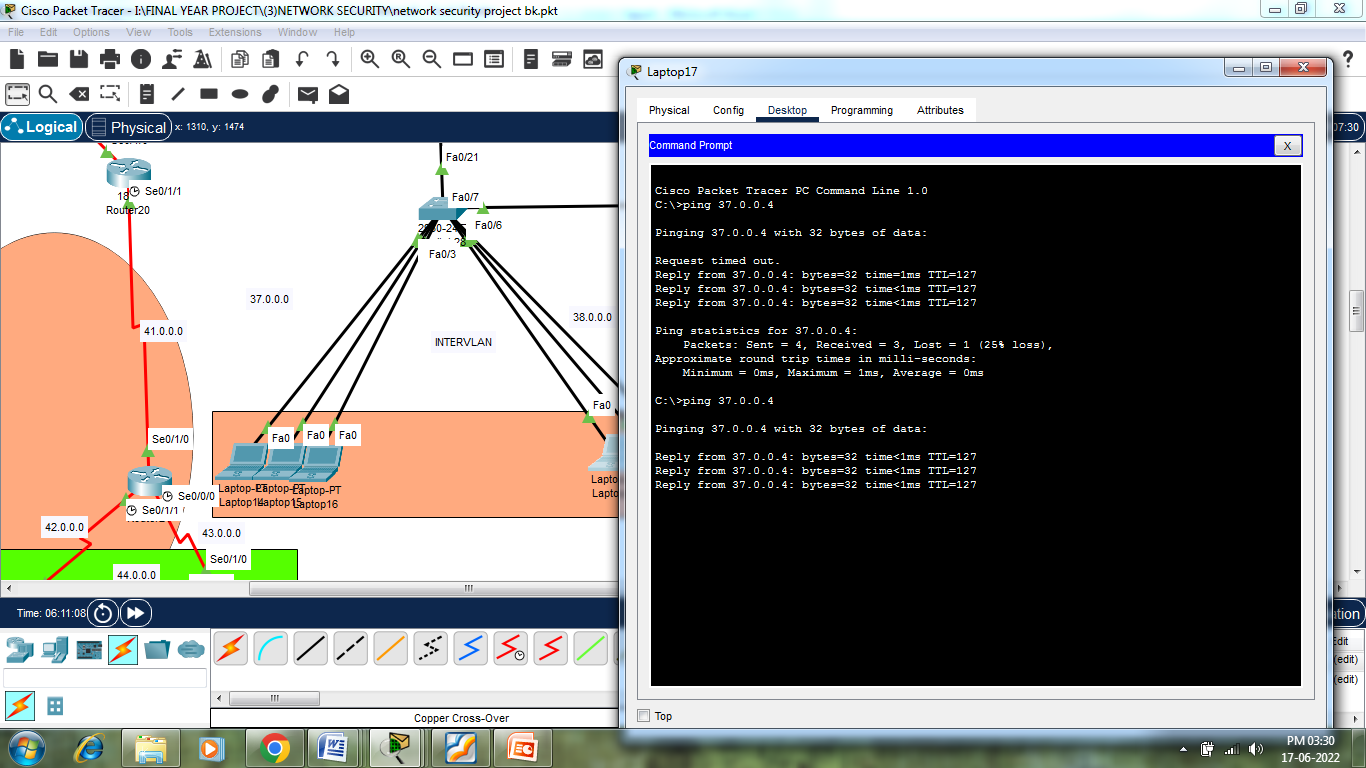
each other irrespective of where the VLANs are present (on same switch or different switch).

 It can be achieved through a layer-3 device i.e. Router or layer-3 Switch. When the Inter VLAN

Routing is done through Router it is known as Router on a stick. .

I have created one inter vlan And it is pinging

Results & Analysis of IntervlanCommunication:-



SSH:

 It is a cryptographic network protocol that is used for transferring encrypted data over network.

 It allows you to connect to a server, or multiple servers, without having you to remember or enter

your password for each system that is to login remotely from one system into another.

 It always comes in key pair:

1. Public key – Everyone can see it, no need to protect it. (for encryption function)

2. Private key – Stays in computer, must be protected. (for decryption function)

 Key pairs can be of the following types:

1. User Key – If public key and private key remain with the user.

2. Host Key – If public key and private key are on a remote system.

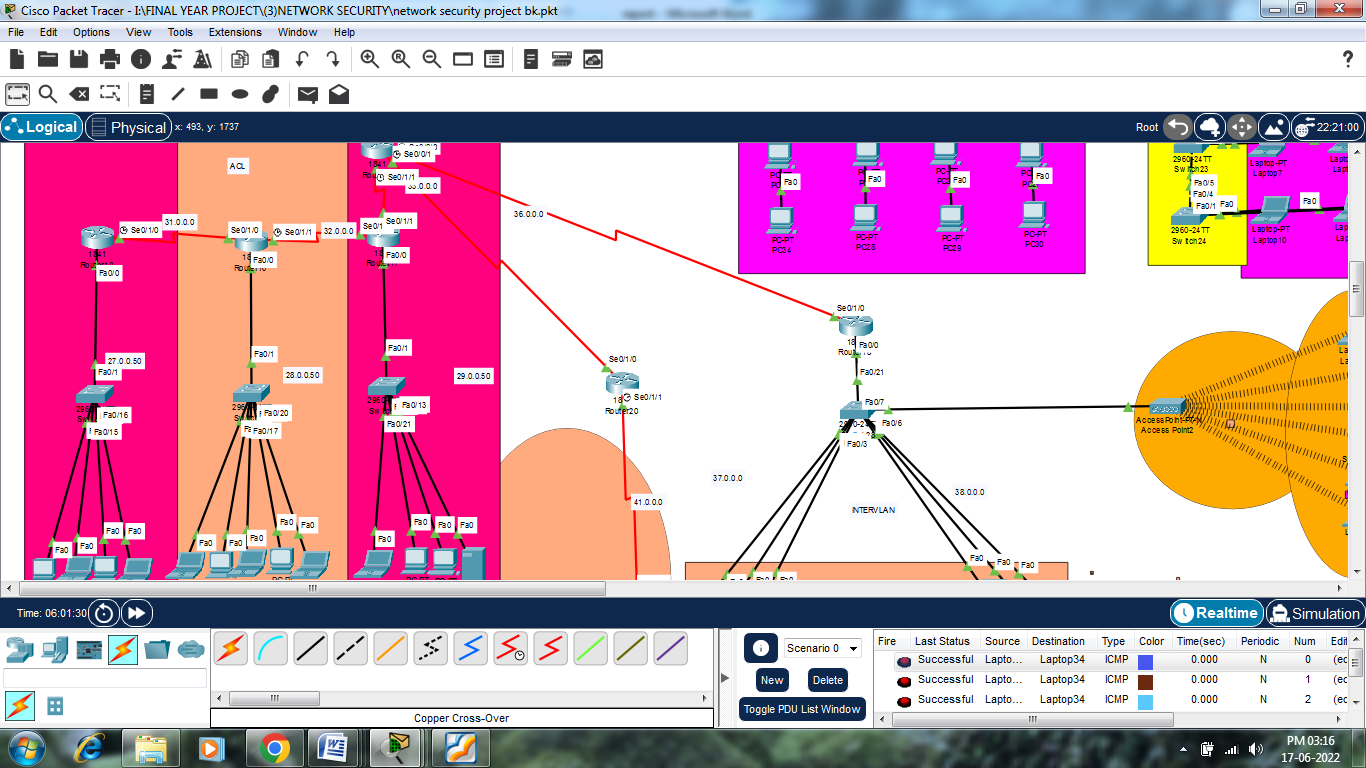
3. Session key – Used when large amount of data is to be transmitted.

 We used RSA Encryption method in our topology

**ACL:-**

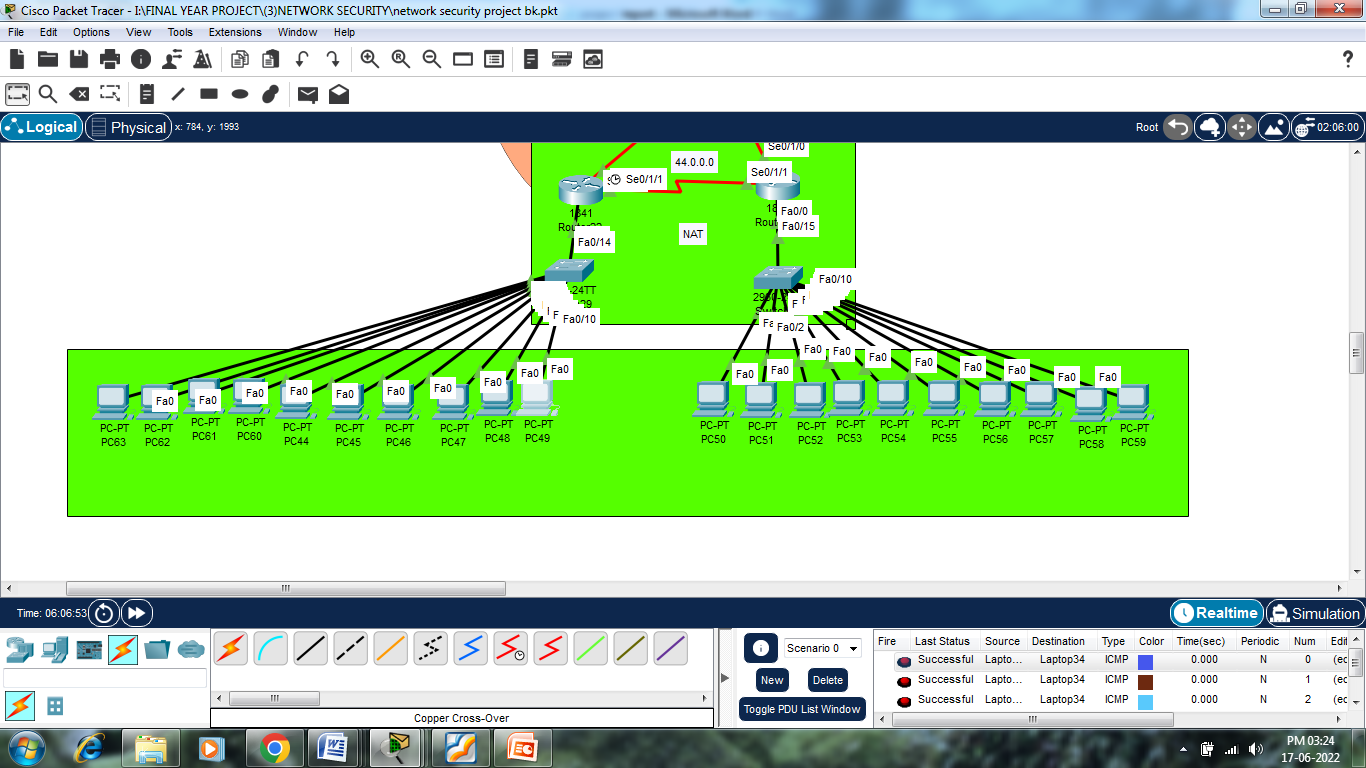
ACL is a list of access control entries . Each entry in an ACL identifies an trustee and specifies t-he access rights allowed , denied or audited for that trustee.

I have applied Acl and it is working well.Acl is applied to 27.0.0.0 ,28.0.0.0,29.0.0.0 networks.

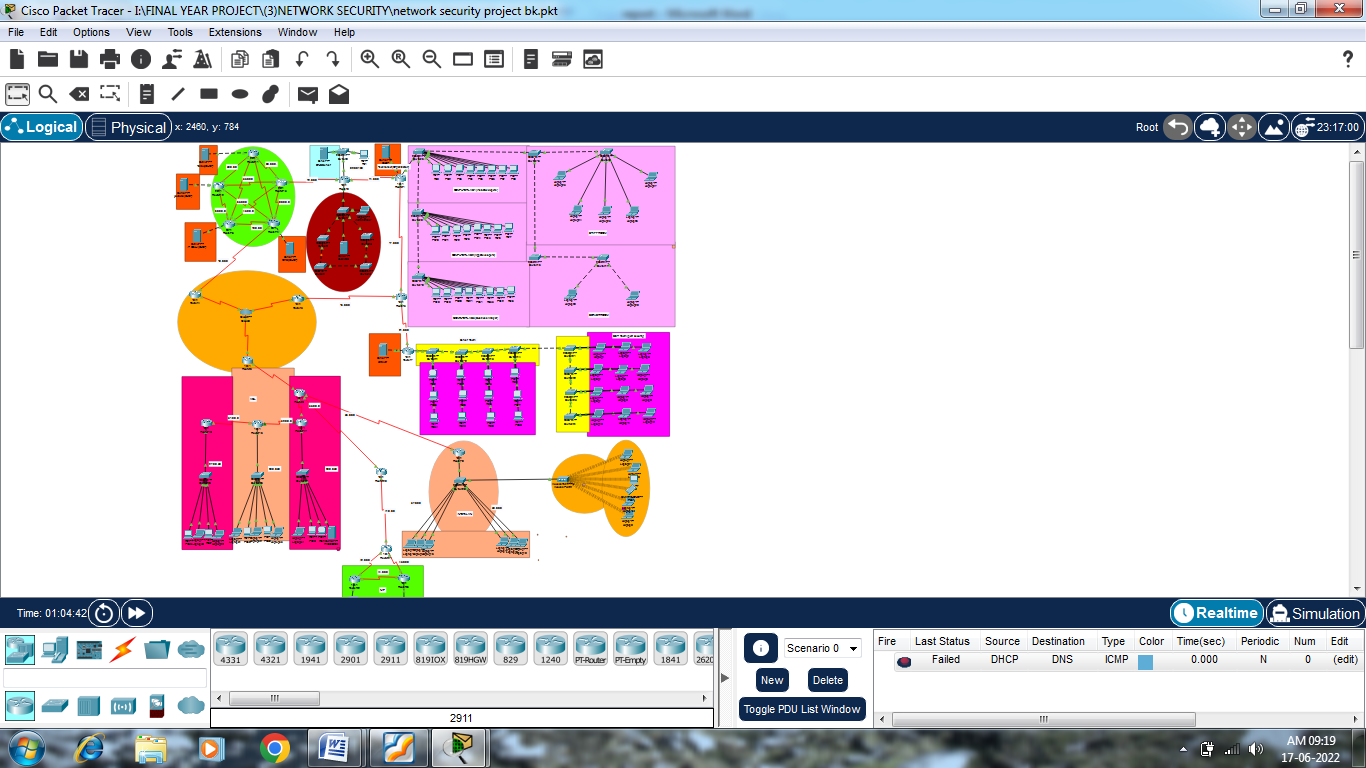
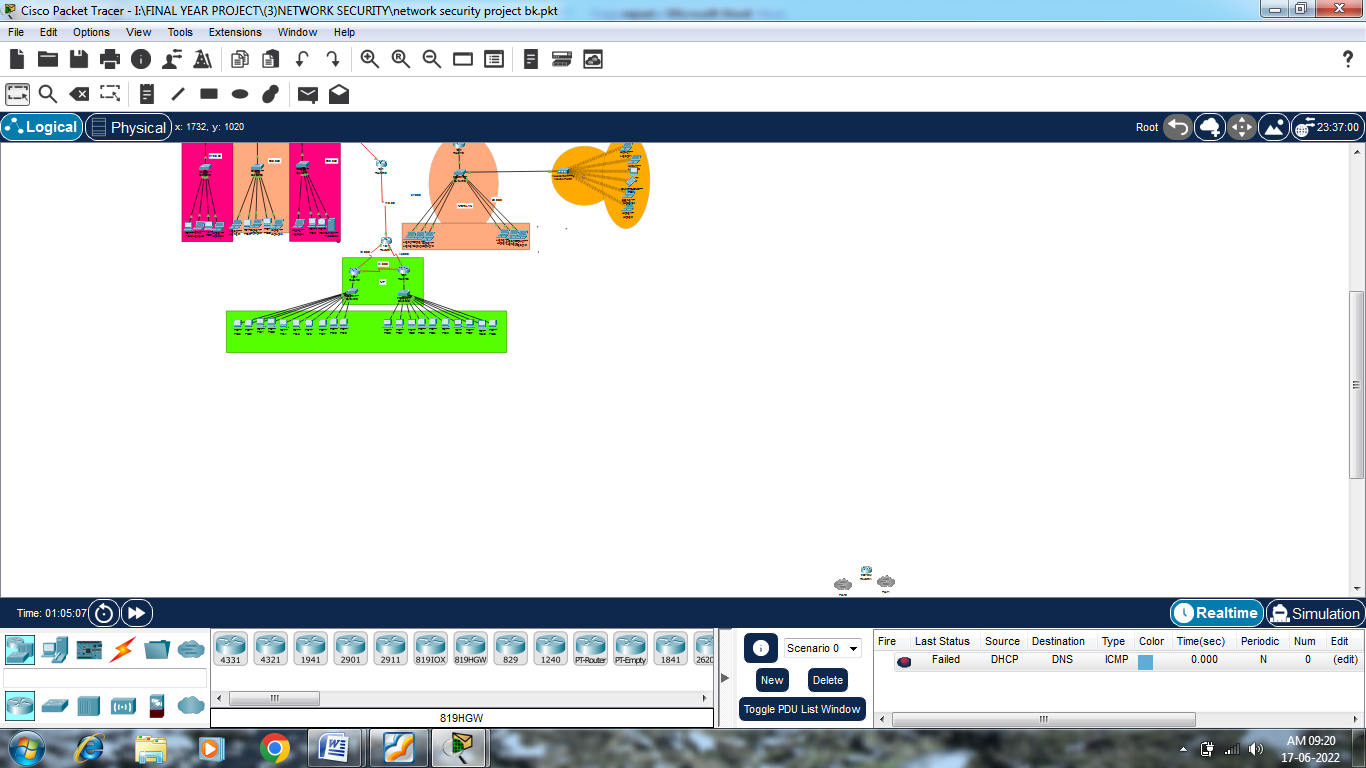


**NETWORK ADDRESS TRANSLATION (NAT) :-**

Network address translation is a method of remapping one IP address space to another by modifying network address information in internet protocol datagram packet headers, while they are in transit. I have applied NAT to my 46.0.0.0 and 47.0.0.0 network whenever attackers tries to access the network he will get modified ip .It will Increase Security of the system.



Network Topology:



**CHAPTER 6**

IMPLEMENTATION

The implementation process taken palce as follow:-

**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.

**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. But this time in a different way because there's no desktop platform on the routers and switches. You will have to access the configuration panel on both devices and this can be done in two ways:

Click on the device and open the Command Line Interface (CLI) and then type in the table.

Use a console cable from an end device and connect it to the device you wish to configure and access the terminal platform on the end device and it will take you to the device's Command Line Interface and then you type in the commands in other to configure the right addresses.

**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.

**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.

**Apply Routing**

Apply routing protocol eigrp on all lan for the communication of different lans.

**Configure dns routing**

Apply step wise dns protocol on dns server

**Configure Inter Vlan**

Create Inter Vlan’s of Network.

**Apply NAT to Host or Network**

**PSEUDOCODE:**

**Router 11 Config(Connected with Server):-**

interface FastEthernet0/0

ip address 10.0.0.50 255.0.0.0

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 75.0.0.2 255.0.0.0

!

interface Serial0/0/1

ip address 85.0.0.1 255.0.0.0

clock rate 2000000

!

interface Serial0/1/0

ip address 90.0.0.1 255.0.0.0

clock rate 2000000

!

interface Serial0/1/1

ip address 50.0.0.1 255.0.0.0

clock rate 2000000

!

interface Serial0/2/0

no ip address

clock rate 2000000

shutdown

!

interface Serial0/2/1

no ip address

clock rate 2000000

shutdown

!

interface Serial0/3/0

no ip address

clock rate 2000000

shutdown

!

interface Serial0/3/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

router rip

version 2

network 10.0.0.0

network 50.0.0.0

network 75.0.0.0

network 85.0.0.0

network 90.0.0.0

no auto-summary

!

ip classless

!

All other devices Coonected to server have similar kind of configuration but change is in corresponding networks Conneccted to it

**Intervlan Devices Config:**

**Switch Config**:-

interface FastEthernet0/1

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/2

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/3

switchport access vlan 2

switchport mode access

!

interface FastEthernet0/4

switchport access vlan 3

switchport mode access

!

interface FastEthernet0/5

switchport access vlan 3

switchport mode access

!

interface FastEthernet0/6

switchport access vlan 3

switchport mode access

**Intervlan Router:-**

ip dhcp pool mynetwork

network 37.0.0.0 255.0.0.0

default-router 37.0.0.1

dns-server 82.0.0.5

no ip cef

no ipv6 cef

spanning-tree mode pvst

interface FastEthernet0/0

no ip address

duplex auto

speed auto

interface FastEthernet0/0.1

encapsulation dot1Q 2

ip address 37.0.0.1 255.0.0.0

interface FastEthernet0/0.2

encapsulation dot1Q 3

ip address 38.0.0.50 255.0.0.0

interface FastEthernet0/1

no ip address

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

clock rate 2000000

!

interface Serial0/0/1

no ip address

clock rate 2000000

shutdown

!

interface Serial0/1/0

ip address 36.0.0.2 255.0.0.0

!

interface Serial0/1/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

ip flow-export version 9

**Router 1(Lan Router In Which we configured DHCP for Differenrt LAN’s)**

ip dhcp pool network

network 11.0.0.0 255.0.0.0

default-router 11.0.0.1

dns-server 82.0.0.5

no ip cef

no ipv6 cef

spanning-tree mode pvst

interface FastEthernet0/0

ip address 12.0.0.50 255.0.0.0

ip access-group 1 in

duplex auto

speed auto

!

interface FastEthernet0/1

ip address 11.0.0.1 255.0.0.0

ip access-group 1 in

duplex auto

speed auto

!

interface Serial0/0/0

ip address 74.0.0.2 255.0.0.0

!

interface Serial0/0/1

ip address 17.0.0.1 255.0.0.0

ip access-group 100 out

!

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

!

interface Serial0/1/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

router rip

version 2

network 11.0.0.0

network 12.0.0.0

network 17.0.0.0

network 74.0.0.0

no auto-summary

!

ip classless

!

ip flow-export version 9

!

!

access-list 1 deny host 29.0.0.3

access-list 1 permit any

**Network Address Translation(Router 1 Config):**-

ip dhcp pool sonia

network 46.0.0.0 255.0.0.0

default-router 46.0.0.1

dns-server 82.0.0.5

no ip cef

no ipv6 cef

spanning-tree mode pvst

interface FastEthernet0/0

ip address 46.0.0.1 255.0.0.0

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

no ip address

clock rate 2000000

shutdown

!

interface Serial0/0/1

no ip address

clock rate 2000000

shutdown

!

interface Serial0/1/0

ip address 42.0.0.2 255.0.0.0

!

interface Serial0/1/1

ip address 44.0.0.1 255.0.0.0

clock rate 2000000

!

interface Vlan1

no ip address

shutdown

!

router rip

version 2

network 42.0.0.0

network 44.0.0.0

network 46.0.0.0

no auto-summary

!

ip nat pool ccna1 200.0.0.1 200.0.0.20 netmask 255.255.255.0

ip nat inside source list 1 pool ccna1

ip classless

**NAT Router 2 Config:-**

ip dhcp pool zakir

network 47.0.0.0 255.0.0.0

default-router 47.0.0.1

dns-server 82.0.0.5

no ip cef

no ipv6 cef

spanning-tree mode pvst

interface FastEthernet0/0

ip address 47.0.0.1 255.0.0.0

ip nat inside

duplex auto

speed auto

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

no ip address

clock rate 2000000

shutdown

interface Serial0/0/1

no ip address

clock rate 2000000

shutdown

interface Serial0/1/0

ip address 43.0.0.2 255.0.0.0

ip nat outside

interface Serial0/1/1

ip address 44.0.0.2 255.0.0.0

ip nat outside

interface Vlan1no ip address

shutdown

router rip

version 2

network 43.0.0.0

network 44.0.0.0

network 47.0.0.0

no auto-summary

!

ip nat pool mewar 195.0.0.1 195.0.0.20 netmask 255.0.0.0

ip nat inside source list 1 pool mewar

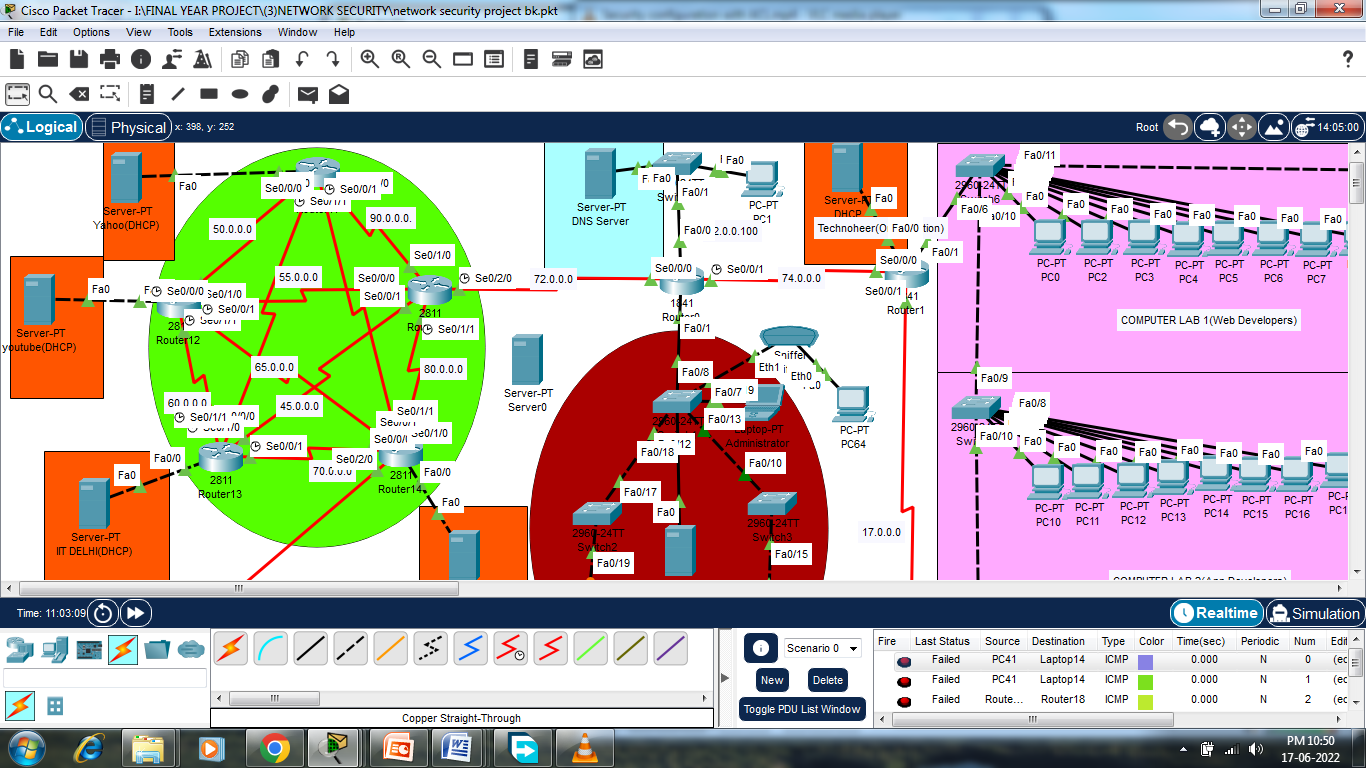
ip classless

ip flow-export version 9

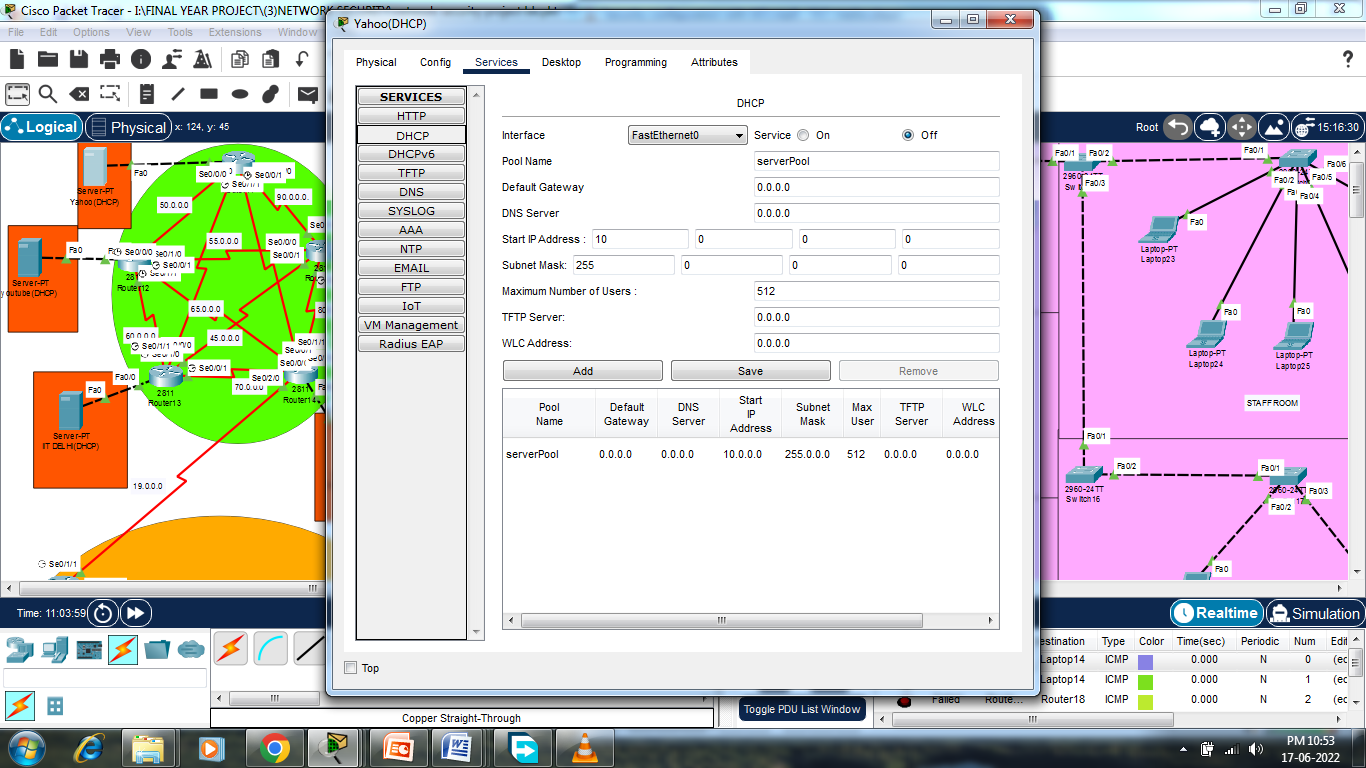
access-list 1 permit 47.0.0.0 0.0.0.255

**SNAPSHOTS:-**

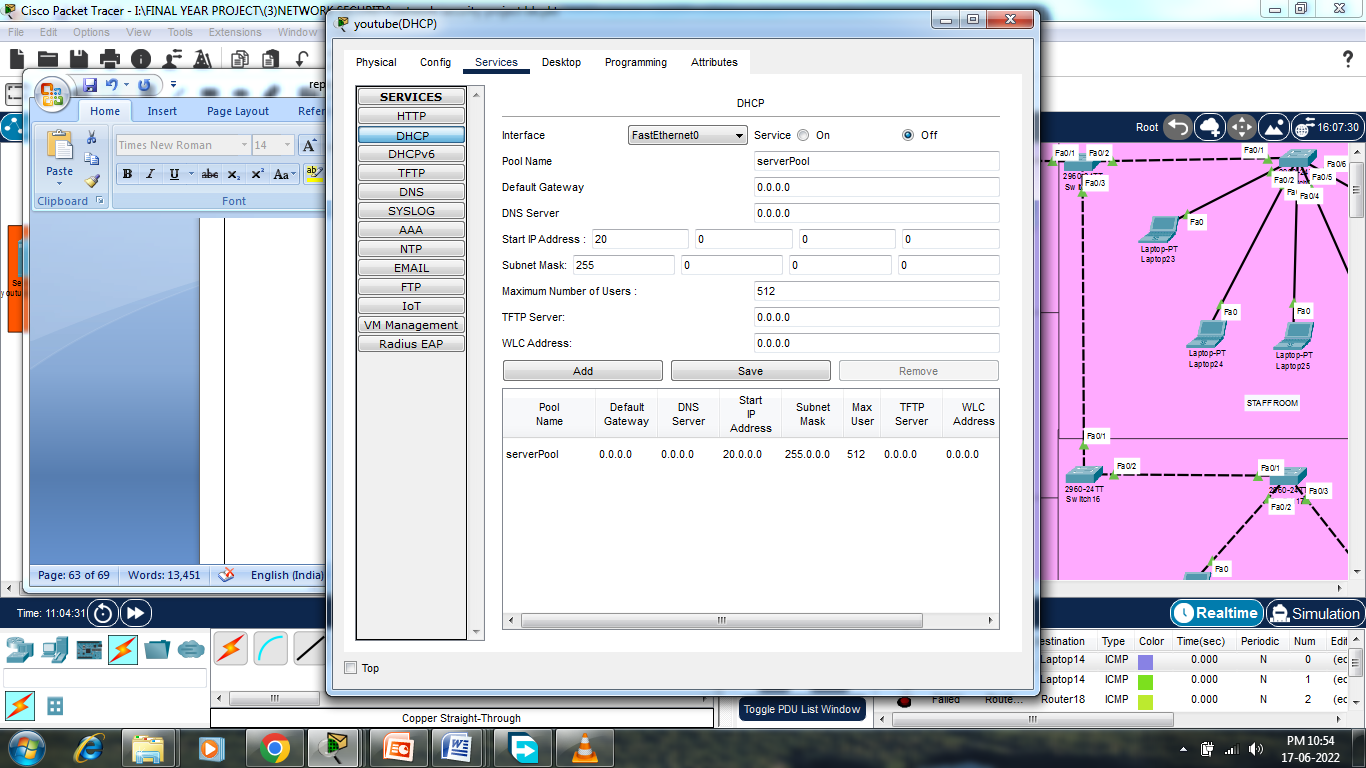
Partially Mesh Topology Design of Routers and Servers



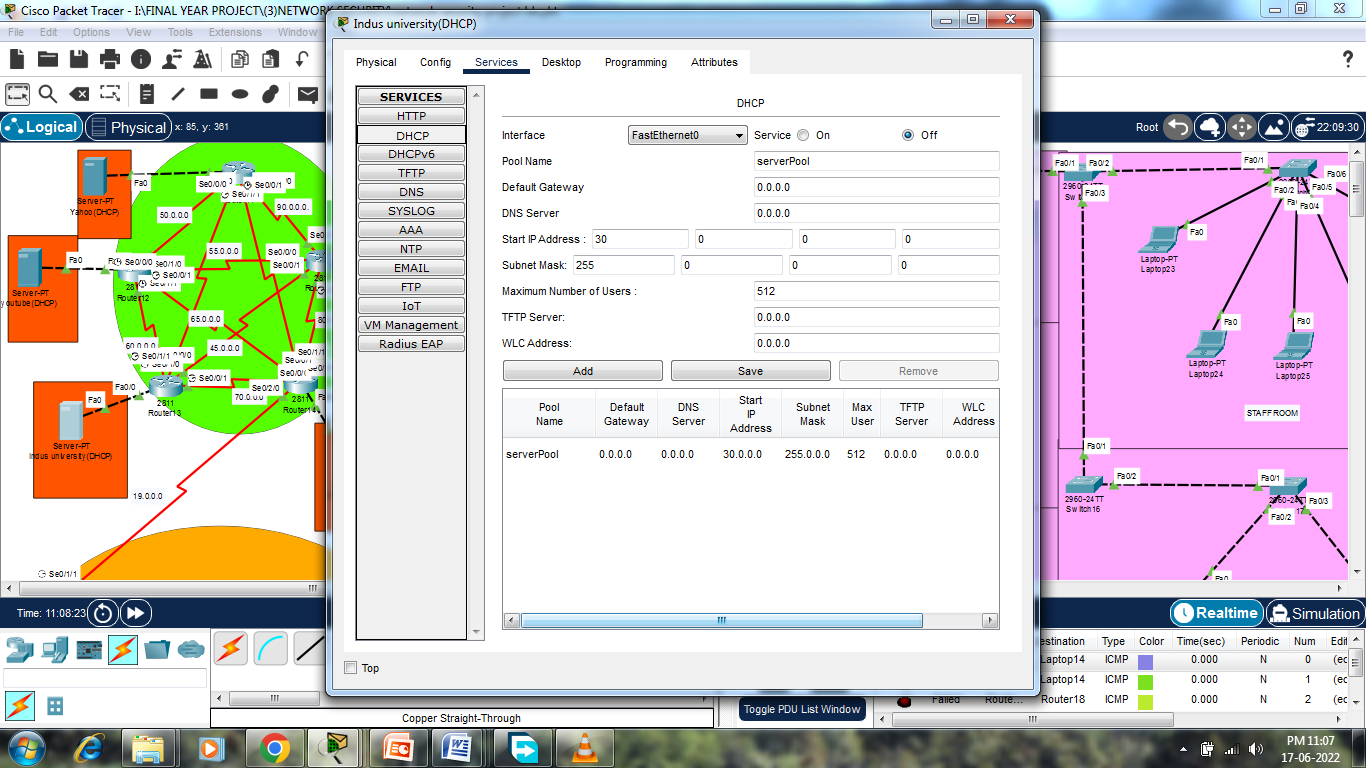
Yahoo(DHCP) Server



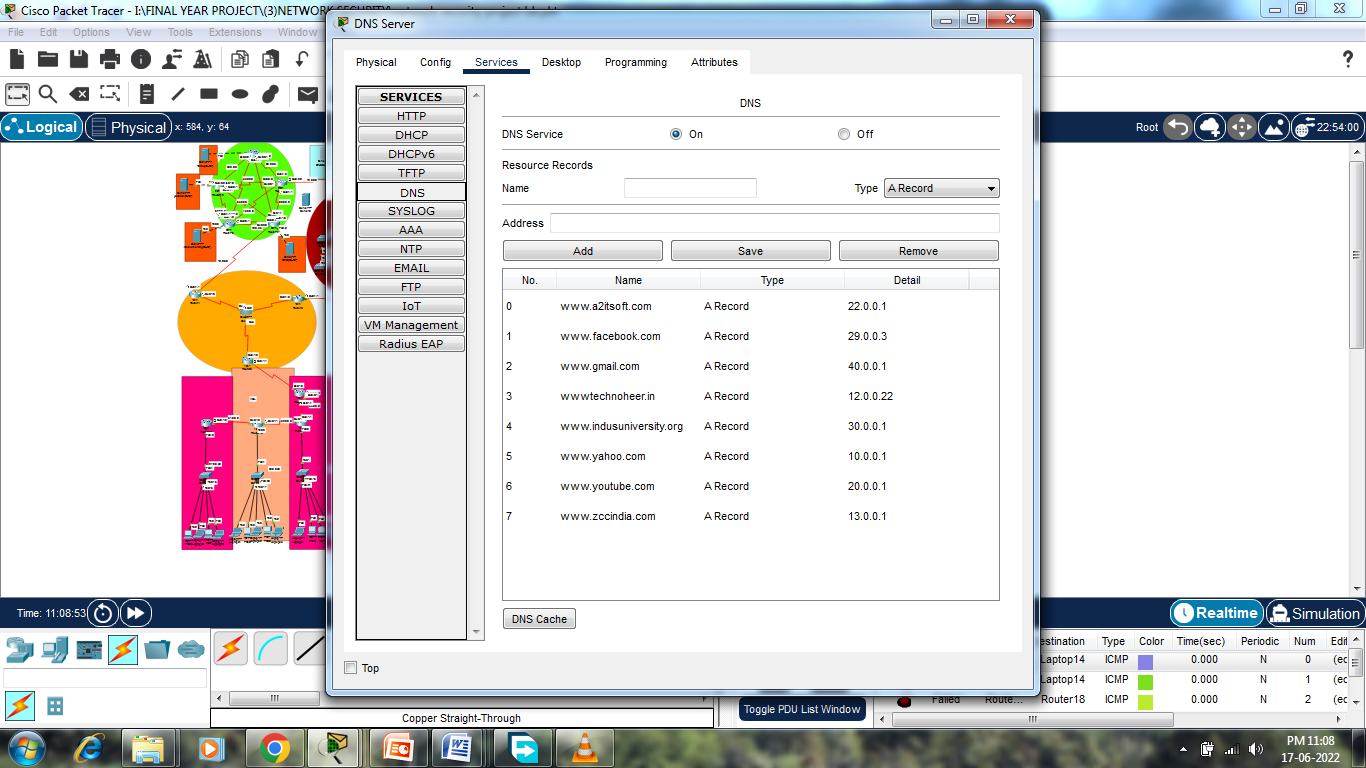
Youtube (DHCP) Server:-



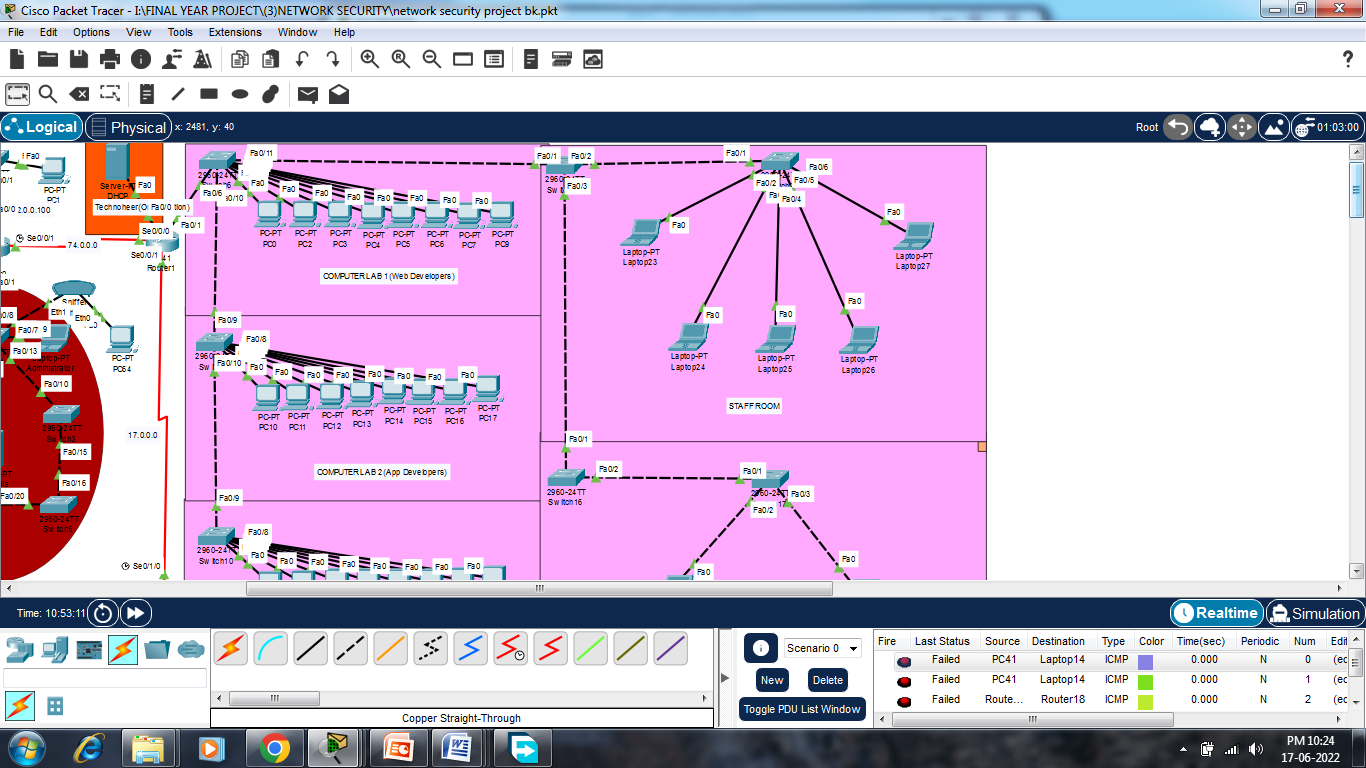
Indus University (DHCP) Server:-



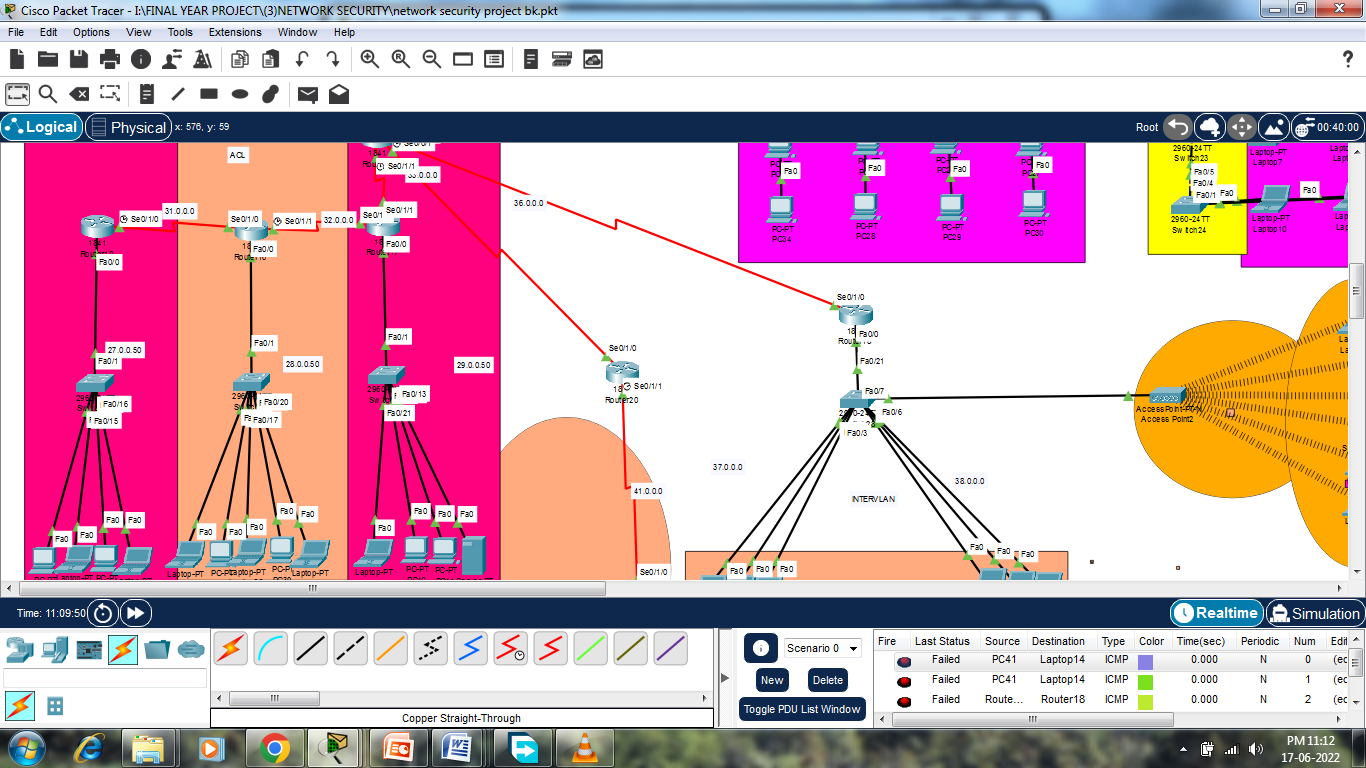
DNS Server:-



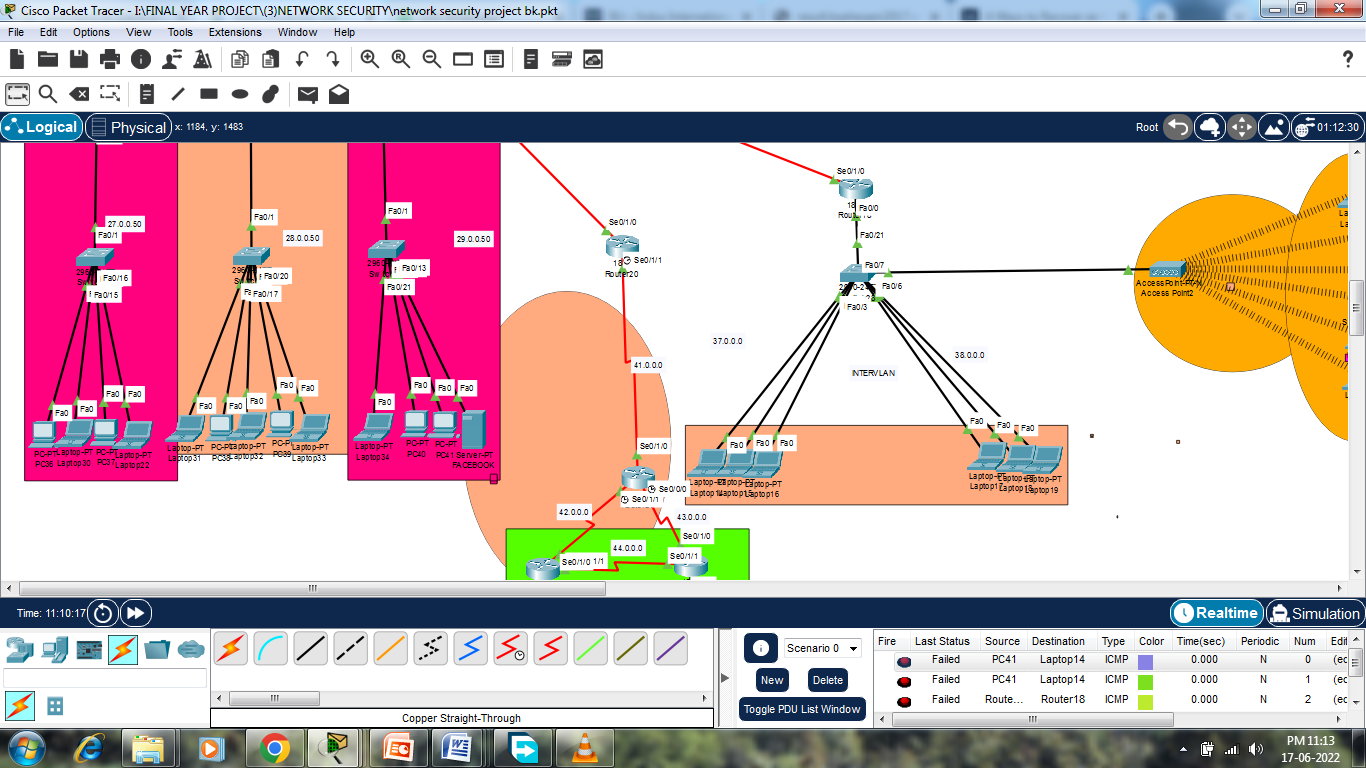
**LAN Networks:-**

****

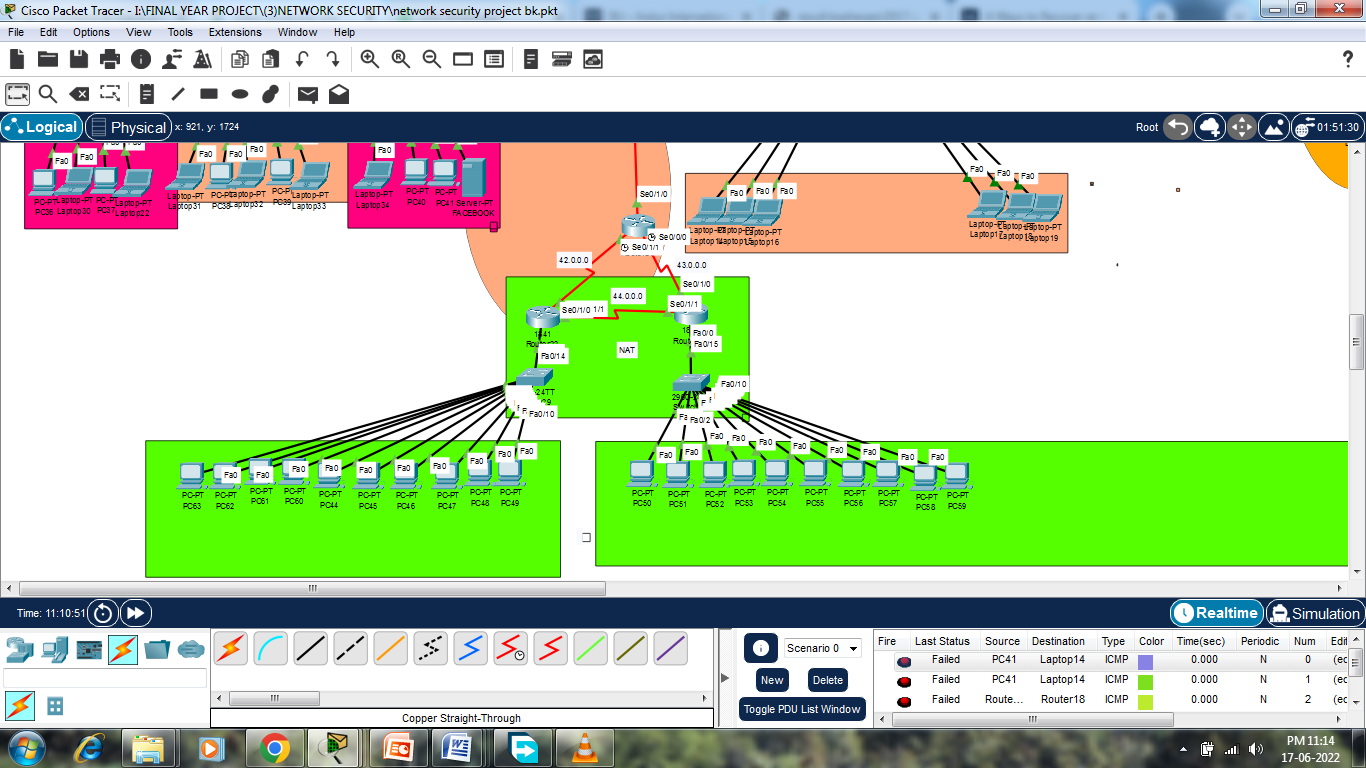
**Network With Acl:-**

**\**

**Intervlan Network:-**

****

**NAT Network :-**

****

**FUTURE SCOPE OF PROJECT:**

Active Networking is vital to career growth. Often confused with selling, Networking is actually about building long-term relationships and a good reputation over time. It involves meeting and getting to know people who you can assist, and who can potentially help you in return. Your network includes everyone from friends and family to work colleagues and members of groups to which you belong.

In today’s word networking is most necessary but everyone wants a secured network in this project I used NAT which provide us a fully secured Organization network. Security is much more difficult in network; this project can control the user of network and make a secure network. In this project, we replace a router with a pc. In this project ACL used which provide us the service to deny any service from the network.

**Future Changes:**

* Limiting bandwidth and access to internet to specific users in the network
* Conduct a survey at data center to learn about possible attacks and disaster recovery and thereby implementing it on mininet software.
* Identify and analyze threats and take preventive measures
* Validation of Small network using Hardware Setup

## CONCLUSION

In this project Network Security Management System using Cisco Packet Tracer, I created a networkusing different components likes pc’s, routers, switches, servers,connectingwires, hubs, etc.

After Connecting the network, I accessed the networks and allotted different protocols to different components like FTP, HTTP etc. to servers, IP’s to all the devices in the network,AndShared ICMPpackets through the network to ensure its flawless working.

Then we fed and flooded the network using Pings and monitored the ping, type of message and connection status.This wasdonetotest the Network Security Management System.

In a sense, security in networks is the combination and culmination of everything we know about security, and certainly everything we have discussed in this book so far. A network's security depends on all the cryptographic tools at our disposal, good program development processes, operating system controls, trust and evaluation and assurance methods, and inference and aggregation controls.

**REFERENCES**

1. [https://www.google.co.in/search?q=local+area+network&source=lnms&tbm=isch&sa=X&ved=0ahUKEwig7PTKsMbTAhUJuY8KHdbqBEoQ\_AUIBigB&biw=1366&bih=613#tbm=isch&q=local+area+network+for+companyhttp://](https://www.google.co.in/search?q=local+area+network&source=lnms&tbm=isch&sa=X&ved=0ahUKEwig7PTKsMbTAhUJuY8KHdbqBEoQ_AUIBigB&biw=1366&bih=613#tbm=isch&q=local+area+network+for+collegehttp://)
2. <http://vfu.bg/en/e-Learning/Computer-Networks--Introduction_Computer_Networking.pdf>
3. <http://www.sfu.ca/~sihengw/ENSC427_Group9/Final%20Report%20.pdf>
4. <http://research.ijcaonline.org/volume48/number18/pxc3880401.pdf>
5. <http://www.cisco.com/c/en/us/td/docs/net_mgmt/active_network_abstraction/3-7/reference/guide/ANARefGuide37.pdf>
6. <http://digitalcommons.uncfsu.edu/cgi/viewcontent.cgi?article=1011&context=macsc_wp>
7. <http://ieeexplore.ieee.org/document/5474509/>
8. <http://phucchau.tran.free.fr/book/O%27Reilly%20->
9. <http://www.net130.com/tutorial/cisco-pdf/routingtcpipv1.pdf>
10. <ftp://ftp.hp.com/pub/networking/software/A-C13-Adv_Routing.pdf>