

Parul University

FACULTY OF ENGINEERING AND TECHNOLOGY

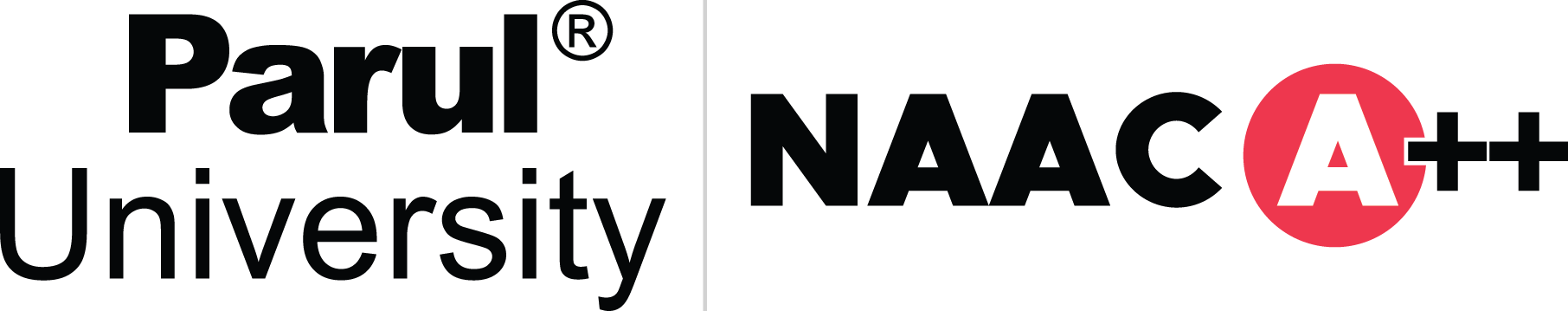
BACHELOR OF TECHNOLOGY

COMPUTER NETWORKS LABORATORY

(303105256)

IV SEMESTER

Computer Science & Engineering Department



Laboratory Manual

Session 2023-24

**COMPUTER NETWORKS PRACTICAL BOOK**

**COMPUTER SCIENCE &ENGINEERING DEPARTMENT**

**PREFACE**

It gives us immense pleasure to present the first edition of the **COMPUTER NETWORKS** Practical Book for the B.Tech . 4**rd semester** students for **PARUL UNIVERSITY**.

The **CN** theory and laboratory courses at PARUL UNIVERSITY, WAGHODIA, VADODARA are designed in such a way that students develop the basic understanding of the subject in the theory classes and then try their hands on the experiments to realize the various implementations of problems learnt during the theoretical sessions. The main objective of the **CN** laboratory course is: Learning **CN** through Experimentations. All the experiments are designed to illustrate various problems in different areas of **CN** and also to expose the students to various uses.

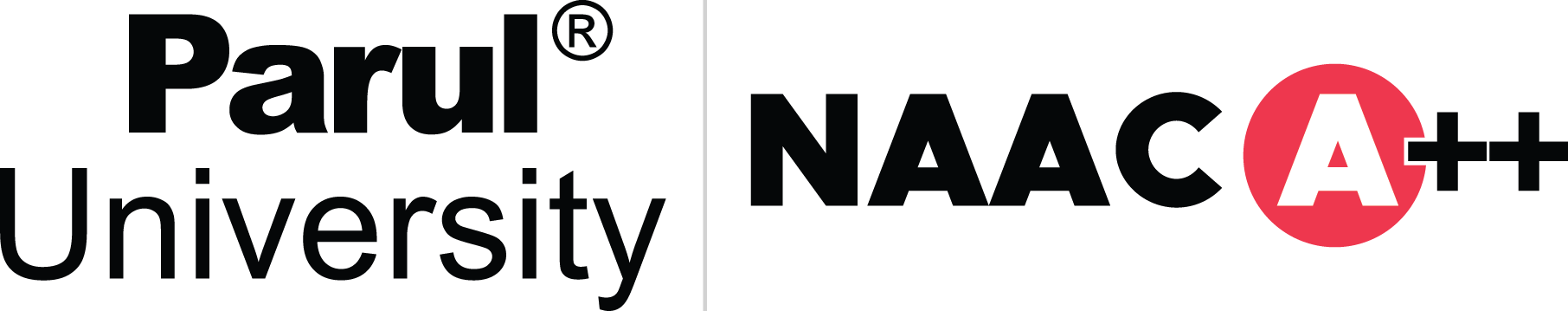
The objective of this **CN** Practical Book is to provide a comprehensive source for all the experiments included in the **CN** laboratory course. It explains all the aspects related to every experiment such as: basic underlying concept and how to analyze a problem. It also gives sufficient information on how to interpret and discuss the obtained results.

We acknowledge the authors and publishers of all the books which we have consulted while developing this Practical book. Hopefully this **CN** Practical Book will serve the purpose for which it has been developed.

**INSTRUCTIONS TO STUDENTS**

1. The main objective of the **CN** laboratory is: Learning through the Experimentation. All the experiments are designed to illustrate various problems in different areas of **CN** and also to expose the students to various problems and their uses.
2. Be prompt in arriving to the laboratory and always come well prepared for the practical.
3. Every student should have his/her individual copy of the **CN** Practical Book.
4. Every student have to prepare the notebooks specifically reserved for the **CN** practical work: ”**CN** Practical Book”
5. Every student has to necessarily bring his/her **CN** Practical Book, **CN** Practical Class Notebook and **CN** Practical Final Notebook.
6. Finally find the output of the experiments along with the problem and note results in the **CN** Practical Notebook.

The grades for the **CN** practical course work will be awarded based on our performance in the laboratory, regularity, recording of experiments in the **CN** Practical Final Notebook, lab quiz, regular viva-voce and end-term examination.



Computer Science And Engineering

Faculty of Engineering And Technology

CN(303105256) B.tech 4th Sem

Enrollment No: 2203051050620

CERTIFICATE

This is to Certify that

Mr./Ms. **VIJAY KUMAR** with enrolment no. **2203051050620** has successfully completed his/her laboratory experiments in the **COMPUTER NETWORKS** **(303105256)** from the department of **COMPUTER SCIENCE & ENGINEERING** during the academic year 2023-2024.



Head of department: ……………………….

Date of Submission : ………………………. Staff In Charge: ……………………….

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Sr. No** | **Experimental Title** | **Page No** | | **Date of Start** | **Date of Completion** | **Sign** | **Marks (out of 10)** |
| **From** | **To** |
| 1. | **Experiments on Simulation Tools: (CISCO PACKET TRACER):**  To understand environment of CISCO PACKET TRACER to design simple network and perform experiments. |  |  |  |  |  |  |
| 2. | Experiments of Packet capture tool: Wireshark. |  |  |  |  |  |  |
| 3. | To study behavior of generic devices used for networking: (CISCO PACKET TRACER). |  |  |  |  |  |  |
| 4. | Data Link Layer (Error Correction). |  |  |  |  |  |  |
| 5. | Virtual LAN |  |  |  |  |  |  |
| 6. | Wireless LAN |  |  |  |  |  |  |
| 7. | Inter networking with routers: 1: Experiment on same subnet 2: Perform Experiment across the subnet and observe functioning of Router via selecting suitable pair of Source and destination. |  |  |  |  |  |  |
| 8. | Implementation of SUBNETTING. |  |  |  |  |  |  |
| 9. | Routing at Network Layer. |  |  |  |  |  |  |
| 10. | Experiment on Transport Layer. |  |  |  |  |  |  |

**TABLE OF CONTENT**

# EXPERIMENT NO: 1

**AIM :** Experiments on Simulation Tools: (CISCO PACKET TRACER).

The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

**Workspace :**

Logical –

Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices.

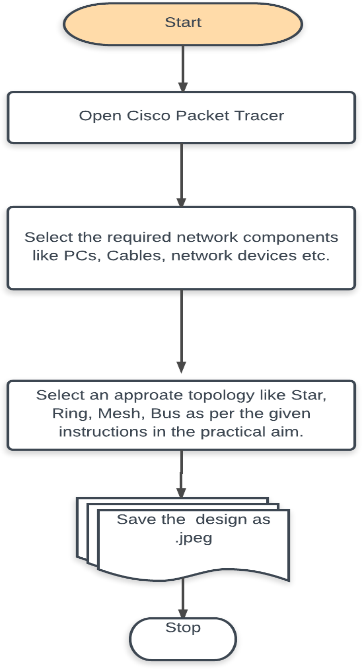
Physical –

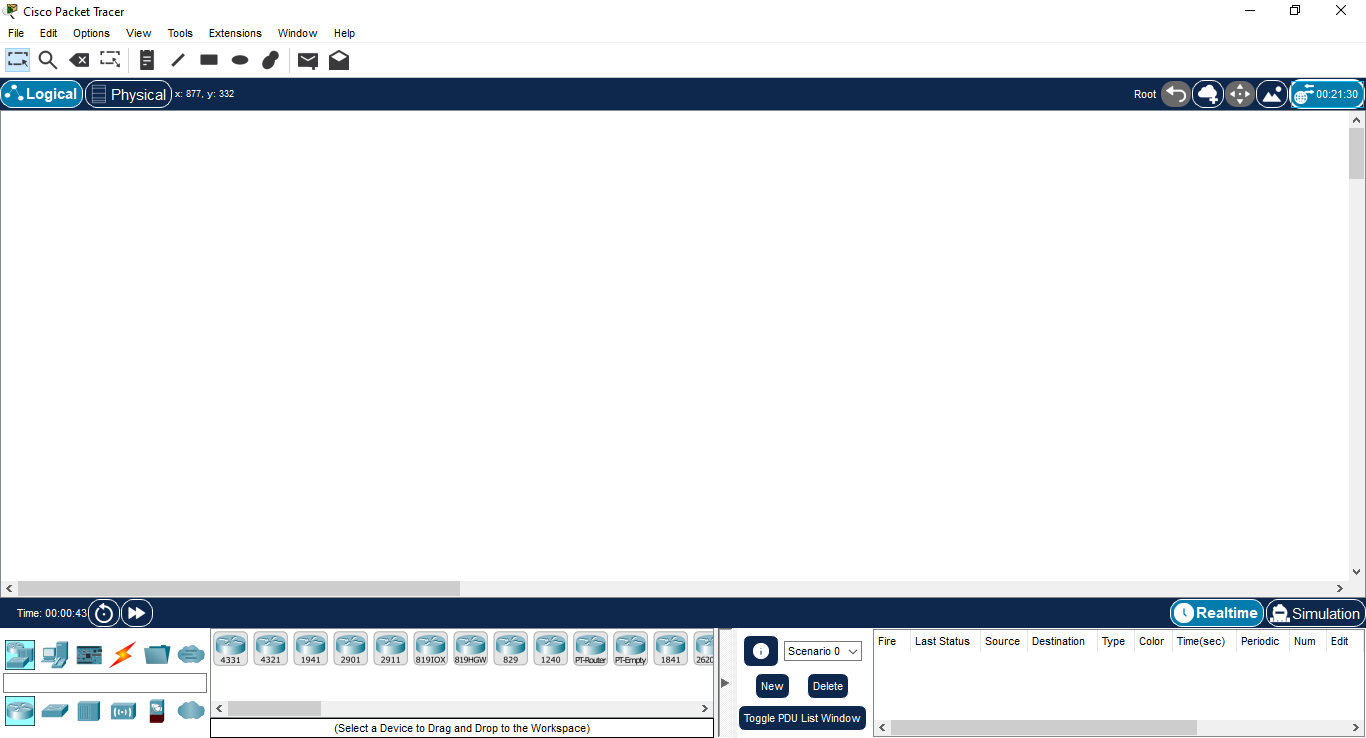
Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment. It also provides geographical representation of networks, including multiple buildings, cities and wiring closets.

**Key Features:**

* Unlimited devices
* E-learning
* Customize single/multi user activities
* Interactive Environment
* Visualizing Networks
* Real-time mode and Simulation mode
* Self-paced
* Supports majority of networking protocols
* International language support
* Cross platform compatibility

**Logical Flow:**

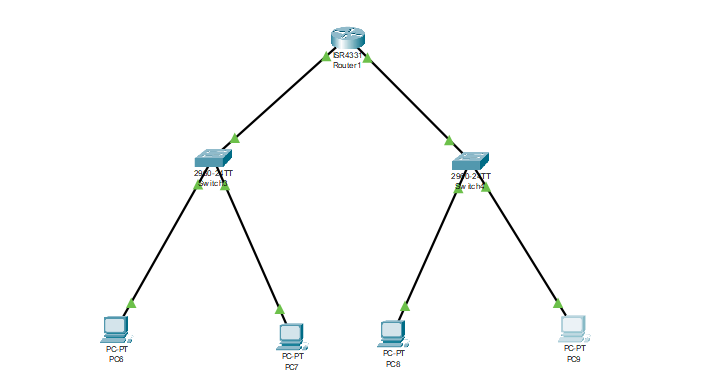


****

**Input :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **IP Address** | **Subnet Mask** | **Default Gateway IP** | **DNS Server IP** |
| 1 | PC6 | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 | 0.0.0.0 |
| 2 | PC7 | 10.0.0.3 | 255.0.0.0 | 10.0.0.1 | 0.0.0.0 |
| 3 | PC8 | 11.0.0.2 | 255.0.0.0 | 11.0.0.1 | 0.0.0.0 |
| 4 | PC9 | 11.0.0.3 | 255.0.0.0 | 11.0.0.1 | 0.0.0.0 |
| 5 | GigabitEthernet0/0/0 | 10.0.0.1 | 255.0.0.0 |  |  |
| 6 | GigabitEthernet0/0/1 | 11.0.0.1 | 255.0.0.0 |  |  |

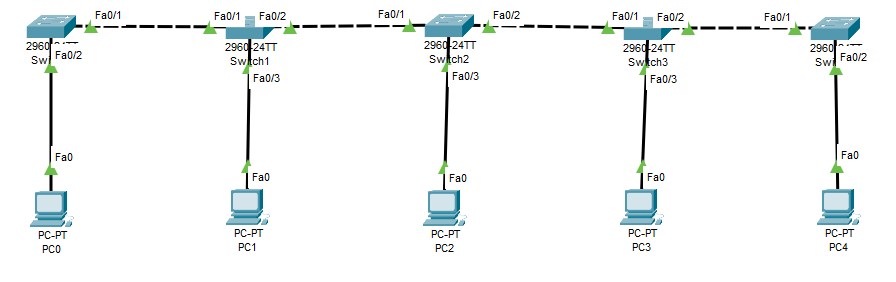
**Ip table for fig 1.2**



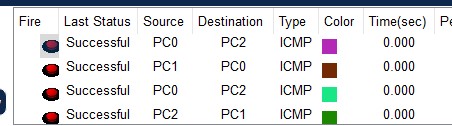
**Fig 1.1**

**Ip table for fig 1.1:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **IP Address** | **Subnet Mask** | **Default Gateway IP** | **DNS Server IP** |
| 1 | PC0 | 10.0.0.1 | 255.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| 2 | PC1 | 10.0.0.2 | 255.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| 3 | PC2 | 11.0.0.3 | 255.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| 4 | PC3 | 11.0.0.4 | 255.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| 5 | PC4 | 10.0.0.6 | 255.0.0.0 | 0.0.0.0 | 0.0.0.0 |

 **fig 1.2**

**EXPECTED OUTPUT:**



After sending the PDU from all the sources of computers they are able to communicate with each other

In both topology.

All the Computers are interconnected in a network.

The status of the Packet Transmission can be viewed in the real-time(Shift +R) and also in Simulation Mode(Shift +S). Here all the computers are communicating with each other.

**CONCLUSION:**

**Here we have studied about the use of cisco packet tracer simulation tool and our implementation**

**Done Successfully.**

# EXPERIMENT NO: 2

**Aim**: To study about WIRESHARK tool and demonstrate working of network packet analyzer using the tool.

**Theory:**

Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers. The extent of its popularity is such, that experience with Wireshark is considered as a valuable/essential trait in a computer networking-related professional.

There are many reasons why Wireshark is so popular:

1. It has a great GUI as well as a conventional CLI (T Shark).

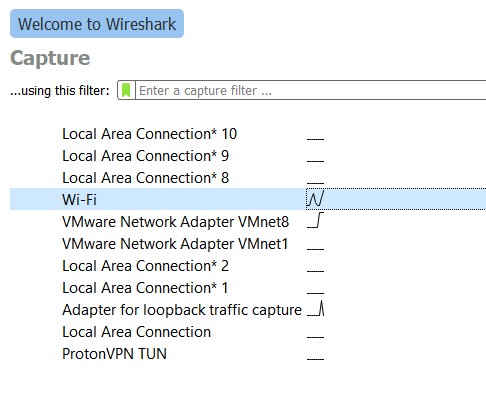
2. It offers network monitoring on almost all types of network standards (Ethernet, Wireless LAN, Bluetooth etc.)

3. It is open-source with a large community of backers and developers.

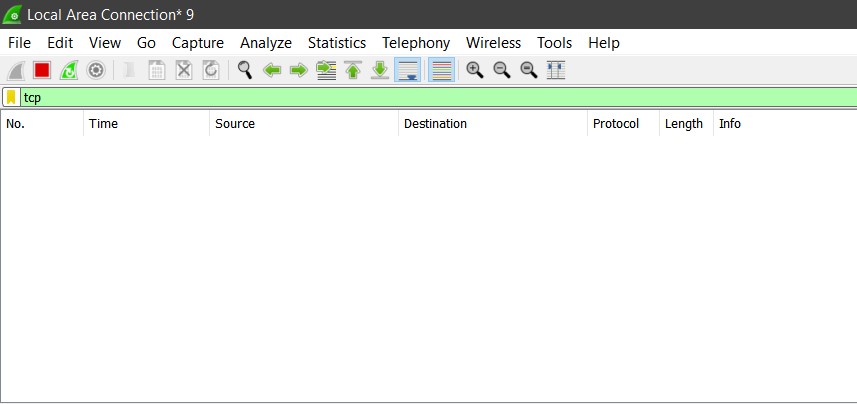
4. All the necessary components for monitoring, analyzing and documenting the network traffic are present. It is free to use.

History of Wireshark: Wireshark was started with the intention of developing a tool for closely analyzing network packets. It was started by Gerald Combez in 1997. Its initial name was Ethereal. It was initially released in July 1998 as version 0.2.0. Due to the support, it got from the developer community, it grew rapidly and was released as version 1.0 in 2008, almost two years after it was renamed to Wireshark.

**Setting Up Wireshark:**

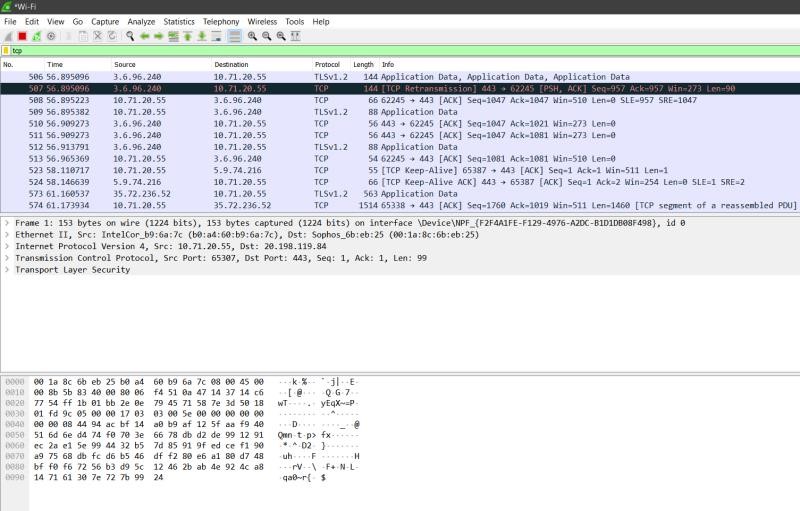


**2.1 Monitor TCP packets in a LAN connection and record your observations**

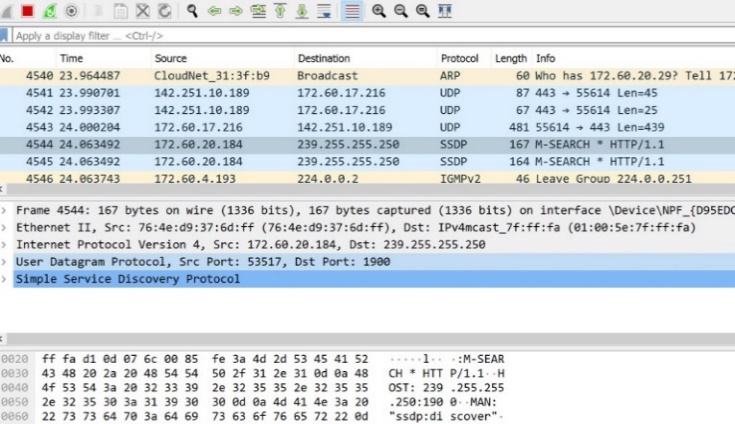


**No TCP Packets are travelled as the device is not connected to a Local Area Network.**

#### 2.2 Monitor TCP packets in a Wi-Fi connection and record your observations



#### 2.4 Monitor UDP packets in a Wi-Fi connection and record your observations



#### 2.5 Monitor SMTP packets in a Wi-Fi connection and record your observations

A screenshot of a computer

Description automatically generated

**Conclusion:**

**Here we have studied about the uses of Wireshark software and performed WIFI analysis. and our implementation Done Successfully.**

## **EXPERIMENT NO : 3**

**AIM :** To study behavior of generic devices used for networking: (CISCO PACKET TRACER).

**Theory :**

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example, Repeater, Hub, Bridge, Switch, Routers, Gateway etc.

**Repeater**:

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.



**Hub:** A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

**Types of Hubs:**

1. Active Hub: These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.

2. Passive Hub: These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.

3. Intelligent Hub: It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.



**USB Hub**

**Bridge:** A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.

**Types of Bridges**

1. Transparent Bridges: These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

2. Source Routing Bridges: In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.



**Switch:** A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

**Types of Switches**

1. Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.

2. Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.

3. Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.

4. Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.

5. Layer 3 switches: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.



**Router**: A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.



**Gateway:** A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter

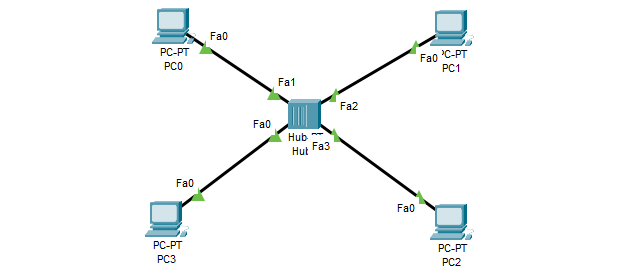


**Implementation:**

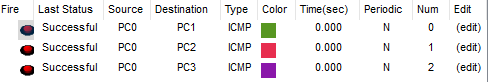
**Input:**

**Ip table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **IP Address** | **Subnet Mask** | **Default Gateway IP** | **DNS Server IP** |
| 1 | PC0 | 10.11.13.14 | 255.0.0.0 | 10.11.13.100 | 10.11.13.70 |
| 2 | PC1 | 10.11.13.15 | 255.0.0.0 | 10.11.13.100 | 10.11.13.70 |
| 3 | PC2 | 10.11.13.16 | 255.0.0.0 | 10.11.13.100 | 10.11.13.70 |
| 4 | PC3 | 10.11.13.17 | 255.0.0.0 | 10.11.13.100 | 10.11.13.70 |



**EXPECTED OUTPUT:**

****

**Conclusion:**

**Here we have studied about the behavior of generic devices in networking was achieved Successfully through Cisco Packet Tracer simulations**.

## **EXPERIMENT NO : 4**

**Aim**: To implement Error Detection Algorithm at Data Link Layer.

**Purpose:**

The experiment aims to implement error detection algorithms at the Data Link Layer to ensure the integrity and reliability of data transmission over a network. By employing techniques such as checksums or cyclic redundancy checks (CRC), the experiment seeks to detect and mitigate transmission errors, enhancing the overall robustness of the network communication protocol.

**Theory:**

Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. It is a technique developed by R.W. Hamming for error correction.

**Steps:**

1. Enter the Data to be transmitted

2. Calculate the no of redundant bits required

3. Determine the parity bits

4. Create error data for testing

5. Check for errors

Decoding a message in Hamming Code

Once the receiver gets an incoming message, it performs recalculations to detect errors and correct them.

**Hamming Code in Python.**

def calcRedundantBits(m):

for i in range(m):

if(2\*\*i >= m + i + 1):

return i

def posRedundantBits(data, r):

j = 0

k = 1

m = len(data)

res = ''

for i in range(1, m + r+1):

if(i == 2\*\*j):

res = res + '0'

j += 1

else:

res = res + data[-1 \* k]

k += 1

return res[::-1]

def calcParityBits(arr, r):

n = len(arr)

for i in range(r):

val = 0

for j in range(1, n + 1):

if(j & (2\*\*i) == (2\*\*i)):

val = val ^ int(arr[-1 \* j])

arr = arr[:n-(2\*\*i)] + str(val) + arr[n-(2\*\*i)+1:]

return arr

def detectError(arr, nr):

n = len(arr)

res = 0

for i in range(nr):

val = 0

for j in range(1, n + 1):

if(j & (2\*\*i) == (2\*\*i)):

val = val ^ int(arr[-1 \* j])

res = res + val\*(10\*\*i)

return int(str(res), 2)

data = '1011001'

m = len(data)

r = calcRedundantBits(m)

arr = posRedundantBits(data, r)

arr = calcParityBits(arr, r)

print("Data transferred is " + arr)

arr = '11101001110'

print("Error Data is " + arr)

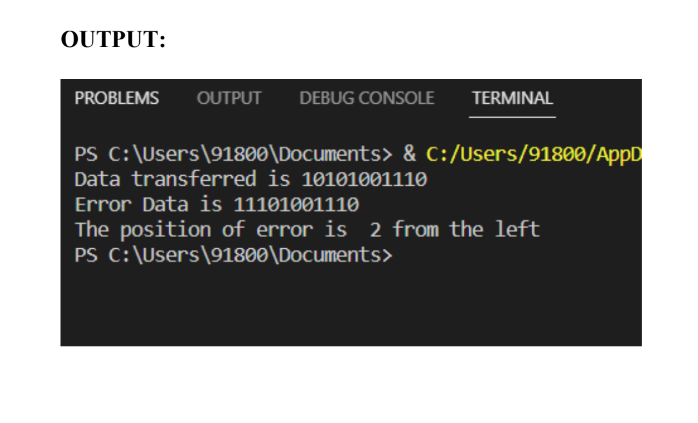
correction = detectError(arr, r)

if(correction==0):

print("There is no error in the received message.")

else:

print("The position of error is ",len(arr)-correction+1,"from the left”)



**Conclusion:**

**Here we have studied about the implementation of Error Detection Algorithm at Data Link Layer was effectively demonstrated Done Successfully.**

## **EXPERIMENT NO : 5**

**AIM :** Virtual LAN

**Theory :**

Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide the broadcast domain but the broadcast domain can be divided by switches using the concept of VLAN. A broadcast domain is a network segment in which if a device broadcast a packet, then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packets but it is limited to switches only as routers don’t forward out the broadcast packet. To forward out the packets to different VLAN (from one VLAN to another) or broadcast domains, inter VLAN routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

**Advantages:**

● Performance: The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destinations. e.g.-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain, therefore, all will receive the traffic i.e. wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.

● Formation of virtual groups: As there are different departments in every organization namely sales, finance etc., VLAN scan be very useful in order to group the devices logically according to their departments.

● Security: In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls

**Disadvantages:**

1. Complexity: VLANs can be complex to configure and manage, particularly in large or dynamic cloud computing environments.

2. Limited scalability: VLANs are limited by the number of available VLAN IDs, which can be a constraint in larger cloud computing environments.

3. Limited security: VLANs do not provide complete security and can be compromised by malicious actors who are able to gain access to the network.

4. Limited interoperability: VLANs may not be fully compatible with all types of network devices and protocols, which can limit their usefulness in cloud computing environments.

5. Limited mobility: VLANs may not support the movement of devices or users between different network segments, which can limit their usefulness in mobile or remote cloud computing environments.

**Real-Time Applications of VLAN:**

**Virtual LANs (VLANs) are widely used in cloud computing environments to improve network performance and security. Here are a few examples of real-time applications of VLANs:**

1. Voice over IP (VoIP): VLANs can be used to isolate voice traffic from data traffic, which improves the quality of VoIP calls and reduces the risk of network congestion.

2. Video Conferencing: VLANs can be used to prioritize video traffic and ensure that it receives the bandwidth and resources it needs for high-quality video conferencing.

3. Remote Access: VLANs can be used to provide secure remote access to cloud-based applications and resources, by isolating remote users from the rest of the network.

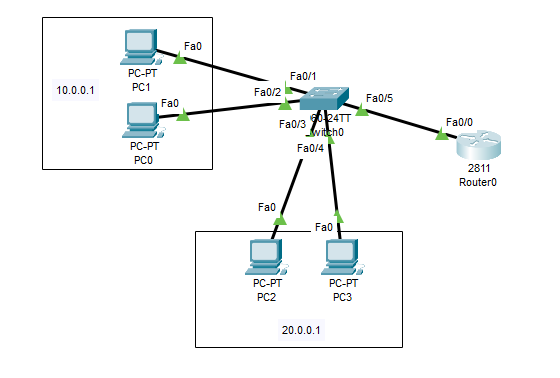
4. Cloud Backup and Recovery: VLANs can be used to isolate backup and recovery traffic, which reduces the risk of network congestion and improves the performance of backup and recovery operations.

5. Gaming: VLANs can be used to prioritize gaming traffic, which ensures that gamers receive the bandwidth and resources they need for a smooth gaming experience.

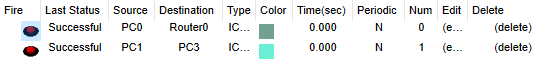
6. IoT: VLANs can be used to isolate Internet of Things (IoT) devices from the rest of the network, which improves security and reduces the risk of network congestion

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **IP Address** | **Subnet Mask** | **Default Gateway IP** | **DNS Server IP** |
| 1 | PC0 | 10.0.0.3 | 255.0.0.0 | 10.0.0.1 | 10.11.13.70 |
| 2 | PC1 | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 | 10.11.13.70 |
| 3 | PC2 | 20.0.0.2 | 255.0.0.0 | 20.0.0.1 | 10.11.13.70 |
| 4 | PC3 | 20.0.0.2 | 255.0.0.0 | 20.0.0.1 | 10.11.13.70 |
|  | **COMMAND TO BE GIVEN ON SWITCH**  enable  config terminal  vlan 10  name HR  vlan 20  name IT  int fa0/1  switchport mode access  switchport access vlan10  int fa0/2  switchport mode access  switchport access vlan10  int fa0/3  switchport mode access  switchport access vlan20  int fa0/4  switchport mode access  switchport access vlan20  int fa0/5  switchport mode trunk |  |  | **COMMAND TO BE GIVEN ON ROUTER**  no  en  conf t  int fa0/0  no sh  int fa0/0.10  encapsulation dot1q 10  ip add 10.0.0.1 255.0.0.0  int fa0/0.20  encapsulation dot1q 20  ip add 20.0.0.1 255.0.0.0v |  |

**Input:**



**EXPECTED OUTPUT:**



**Conclusion:**

**Here we have studied about the vlan and we created vlan virtually in cisco packet tracer and our vlan network run Successfully**

## **EXPERIMENT NO : 6**

**Aim**: To implement WLAN.

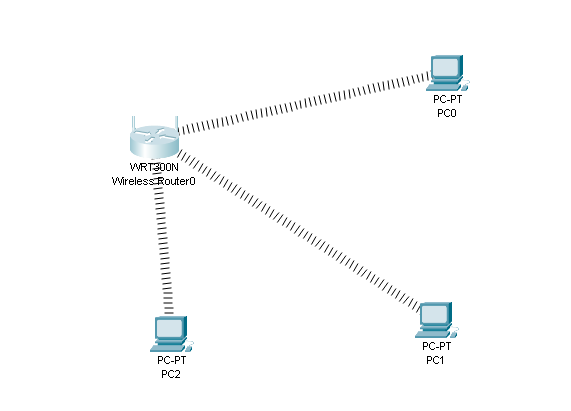
**Theory:**

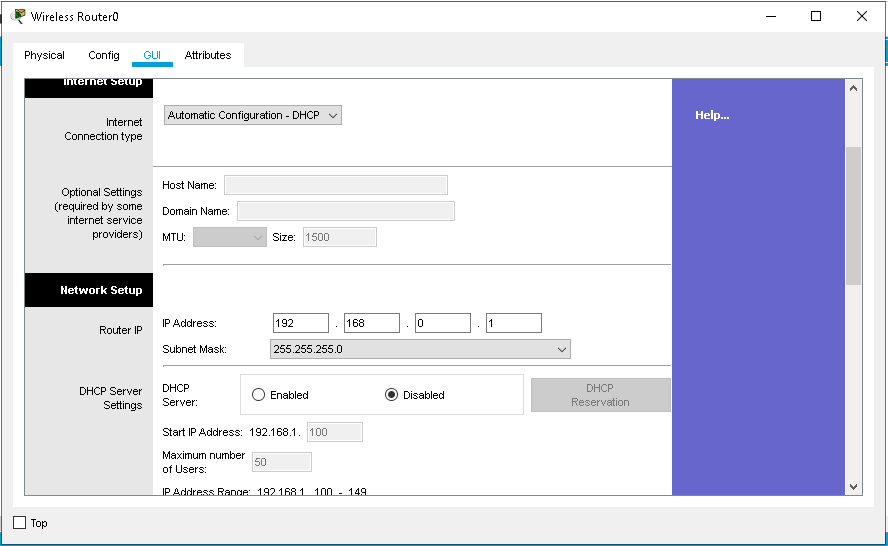
WLAN stands for Wireless Local Area Network. WLAN is a local area network that uses radio communication to provide mobility to the network users while maintaining the connectivity to the wired network. A WLAN basically, extends a wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter which is similar in function to an ethernet adapter. It is also called a LAWN is a Local area wireless network. The performance of WLAN is high compared to other wireless networks. The coverage of WLAN is within a campus or building or that tech park. It is used in the mobile propagation of wired networks. The standards of WLAN are HiperLAN, Wi-Fi, and IEEE 802.11. It offers service to the desktop laptop, mobile application, and all the devices that work on the Internet. WLAN is an affordable method and can be set up in 24 hours. WLAN gives users the mobility to move around within a local coverage area and still be connected to the network. Latest brands are based on IEE 802.11 standards, which are the WI-FI brand name.

**Input:**

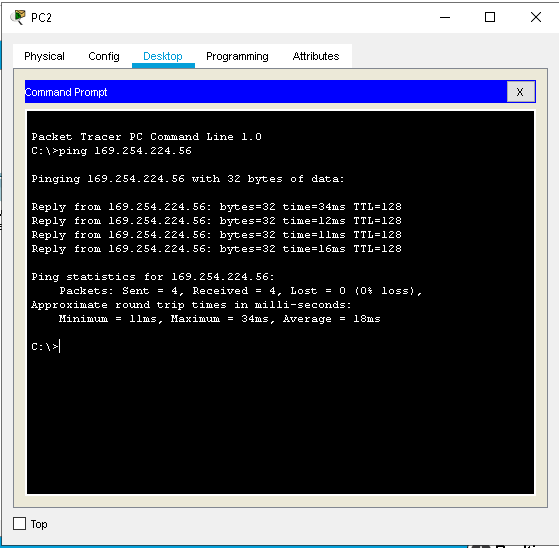
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **IP Address** | **Subnet Mask** | **Default Gateway IP** |
| 1 | PC0 | 192.168.0.102 | 255.255.255.0 | 192.168.0.101 |
| 2 | PC1 | 192.168.0.103 | 255.255.255.0 | 192.168.0.101 |
| 3 | PC2 | 192.168.0.104 | 255.255.255.0 | 192.168.0.101 |

**Implementation:**





**EXPECTED OUTPUT:**



**Conclusion:**

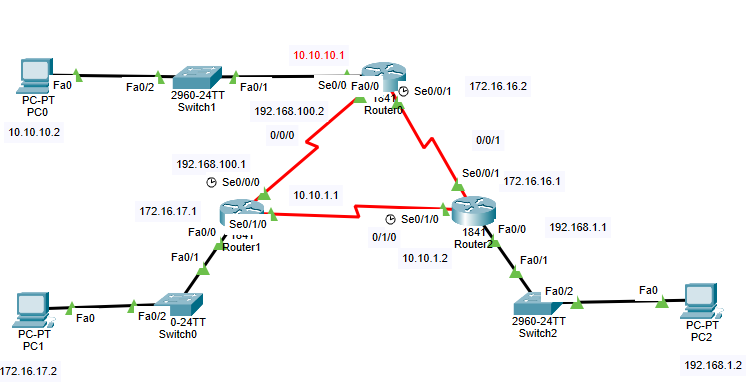
**Here we have studied about the implementation of Wireless Local Area Network and our implementation done Successfully**

## **EXPERIMENT NO : 7**

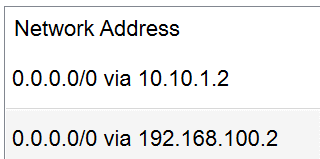
**AIM :** Inter networking with routers: 1: Experiment on same subnet 2: Perform Experiment across the subnet and observe functioning of Router via selecting suitable pair of Source and destination.

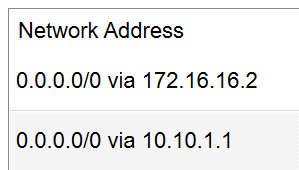
**Input:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **interface** | **IP Address** | **Subnet Mask** | **Default Gateway IP** | **DNS Server IP** |
| 1 | PC0 | Fa0 | 10.10.10.2 | 255.0.0.0 | 10.10.10.1 | 0.0.0.0 |
| 2 | PC1 | Fa0 | 172.16.17.2 | 255.255.0.0 | 172.16.17.1 | 0.0.0.0 |
| 3 | PC2 | Fa0 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | 0.0.0.0 |
| 4 | ROUTER 1 | Fa0/0 | 172.16.17.1 | 255.0.0.0 | 0.0.0.0 | 0.0.0.0 |
| 5 | ROUTER 1 | Se0/1/0 | 10.10.1.1 |  |  |  |
| 6 | ROUTER 1 | Se0/0/0 | 192.168.100.1 |  |  |  |
| 7 | ROUTER 2 | Fa0/0 | 192.168.1.1 |  |  |  |
| 8 | ROUTER 2 | Se0/1/0 | 10.10.1.2 |  |  |  |
| 9 | ROUTER 2 | Se0/0/0 | 172.16.16.1 |  |  |  |
| 10 | ROUTER 0 | Fa0/0 | 10.10.1.1 |  |  |  |
| 11 | ROUTER 0 | Se0/0/1 | 172.16.16.2 |  |  |  |
| 12 | ROUTER 0 | Se0/0/0 | 192.168.100.2 |  |  |  |

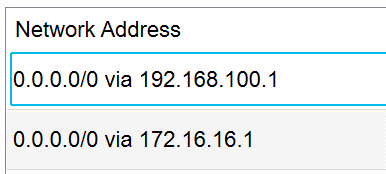
**Implementation:**

Static Routes configuration

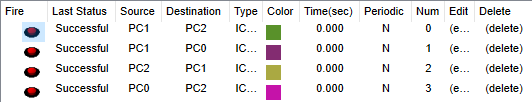


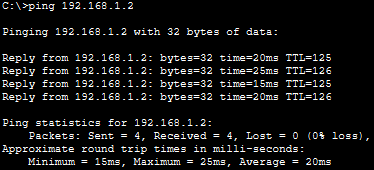


Router 0 Router 1 Router 2



**EXPECTED OUTPUT:**





**Conclusion:**

**Here we have studied about Inter networking with routers: 1: Experiment on same subnet 2: Perform Experiment across the subnet and observe functioning of Router via selecting suitable pair of Source and destination. And our implementation done Successfully**

## **EXPERIMENT NO : 8**

**AIM: Implementation of SUBNETTING.**

**Theory:**

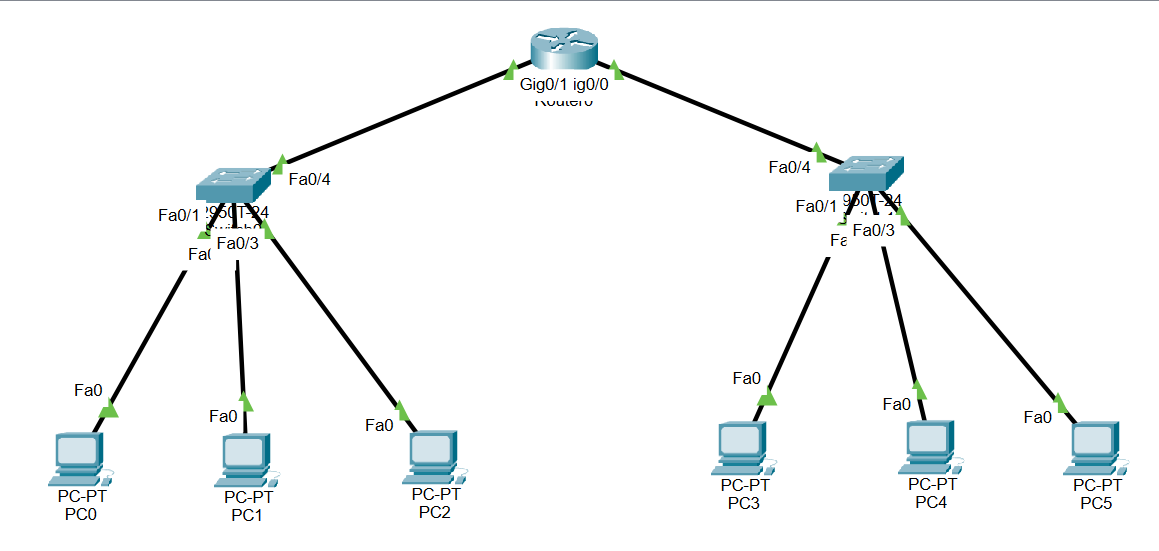
A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination

1. Subnetting is the practice of dividing up a network into two or more networks. Common advantages of subnetting include enhancing routing efficiency, network management control, and improving network security. While these are just a few of the benefits that subnetting provides, they are the most noticeable after immediately implementing a subnet system.
2. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. Addresses help to identify the pieces of hardware connected to your network. To locate a particular device you would need to organize the IP addresses in a logical way. This is where subnetting excels as a tool to help you maintain efficiency across your network.

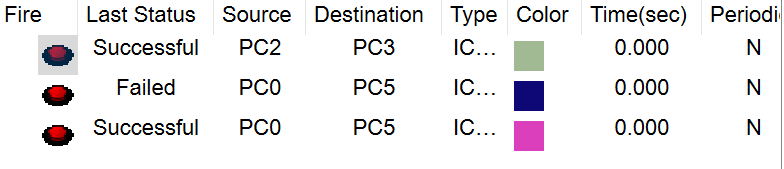
**Input:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **interface** | **IP Address** | **Subnet Mask** | **Default Gateway IP** | **DNS Server IP** |
| 1 | PC0 | Fa0 | 192.168.10.1 | 255.255.255.128 | 192.168.10.4 | 0.0.0.0 |
| 2 | PC1 | Fa0 | 192.168.10.2 | 255.255.255.128 | 192.168.10.4 | 0.0.0.0 |
| 3 | PC2 | Fa0 | 192.168.10.3 | 255.255.255.128 | 192.168.10.4 | 0.0.0.0 |
| 4 | PC3 | Fa0 | 192.168.10.129 | 255.255.255.128 | 192.168.10.132 | 0.0.0.0 |
| 5 | PC4 | Fa0 | 192.168.10.130 | 255.255.255.128 | 192.168.10.132 | 0.0.0.0 |
| 6 | PC5 | Fa0 | 192.168.10.131 | 255.255.255.128 | 192.168.10.132 | 0.0.0.0 |
| 7 | ROUTER 0 | G0/0 | 192.168.10.132 | 255.255.255.128 |  |  |
| 8 | ROUTER 0 | G0/1 | 192.168.10.4 | 255.255.255.128 |  |  |

**Implementation of Static Subnetting:**



**EXPECTED OUTPUT:**

****

**Conclusion:**

**Here we have studied about subnetting and their uses, we also implemented subnetting in cisco packet tracer and our implementation done Successfully**

## **EXPERIMENT NO : 9**

**AIM: Routing at Network Layer.**

**Theory:**

Routing is a procedure of making decisions in which the router (which is a hardware device used in networking to receive and send data in the form of packets on a network) selects the best path to make data transfer from source to destination. A router exists in the network layer in the OSI as well as TCP/IP model.

**Some functions of a router are:**

1. Building an optimal path on a network to reach its destination (in which static and dynamic routing take place).
2. Taking routing decisions.
3. Balancing load.

**Types of Routing:**

1. **Static routing:** Static routing is a process in which we have to manually add routes to the routing table. No routing overhead for the router CPU which means a cheaper router can be used to do routing. It adds security because only an only administrator can allow routing to particular networks only.
2. **Dynamic routing:** Dynamic routing is known as a technique of finding the best path for the data to travel over a network in this process a router can transmit data through various different routes and reach its destination on the basis of conditions at that time of communication circuits.

We will implement here about static routing and dynamic routing both

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **interface** | **IP Address** | **Subnet Mask** | **Default Gateway IP** | **DNS Server IP** |
| 1 | PC0 | Fa0 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | 0.0.0.0 |
| 2 | PC1 | Fa0 | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | 0.0.0.0 |
| 3 | PC2 | Fa0 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 | 0.0.0.0 |
| 4 | PC3 | Fa0 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | 0.0.0.0 |
| 5 | ROUTER 0 | G0/0 | 192.168.1.1 | 255.255.255.0 |  |  |
| 6 | ROUTER 0 | Set0/1/0 | 10.10.10.1 | 255.0.0.0 |  |  |
| 7 | ROUTER 1 | G0/1 | 192.168.2.1 | 255.255.255.0 |  |  |
| 8 | ROUTER 1 | Set0/1/0 | 10.10.11.1 | 255.0.0.0 |  |  |

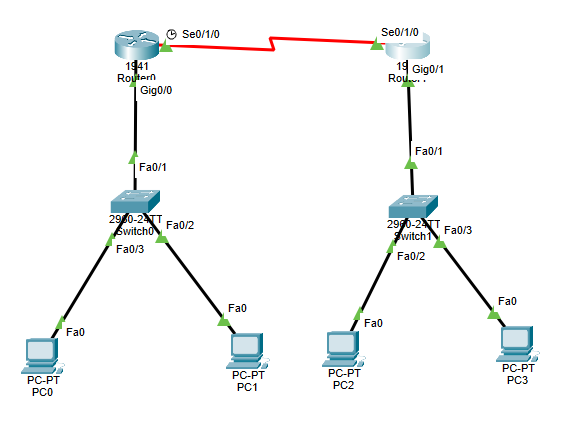
**Implementation of Static Routing:**

**Input:**

**On both routers before connecting the topology :**

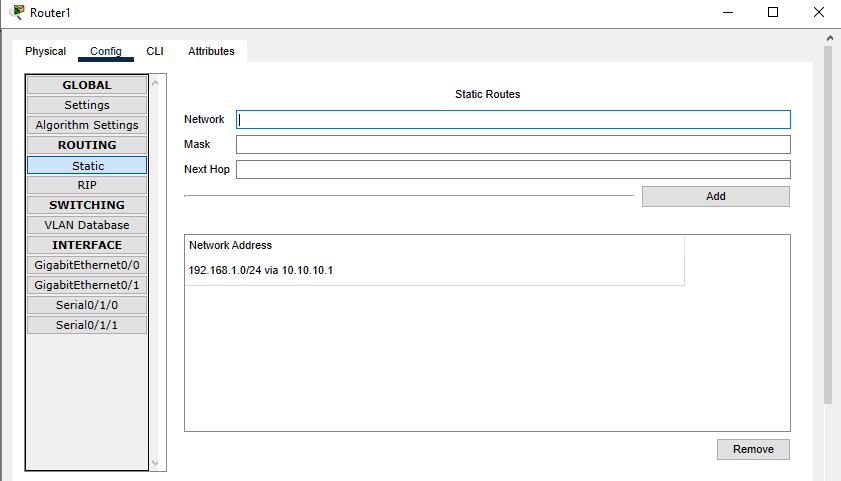
* **On routers go to physical tab then HWIC-2T tab then turn of the router**
* **Drag and drop the additional element as shown in picture below**
* **Then turn on the routers again to enable serial port**



****

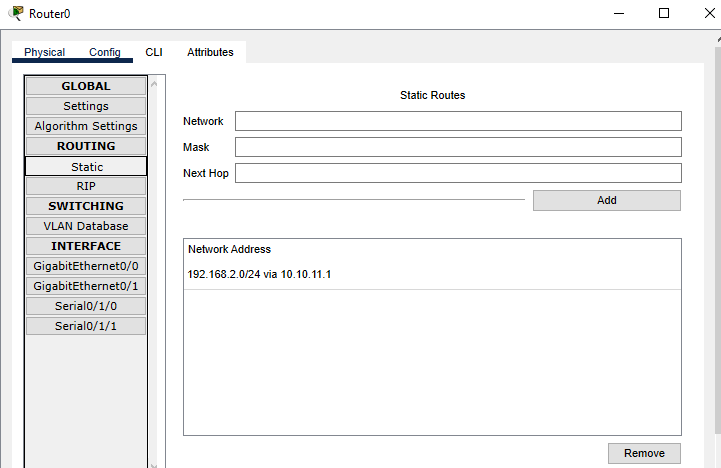
**On router 1:**

* **Configure router as given in picture below**
* **Go to settings tab and then save the settings**

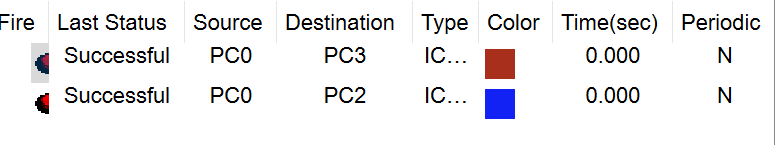
****

**On router 0:**

* **Configure router as given in picture below**
* **Go to settings tab and then save the settings**



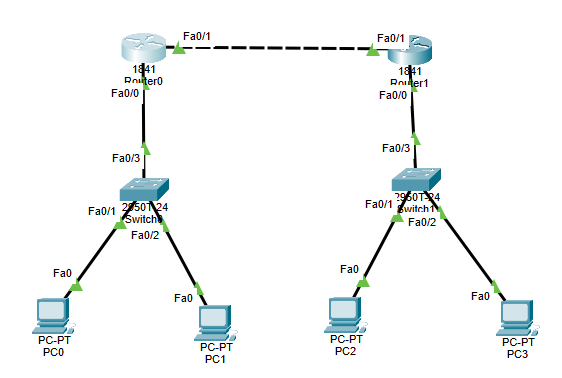
**EXPECTED OUTPUT:**

****

**Implementation of Dynamic Routing:**

**Input:**

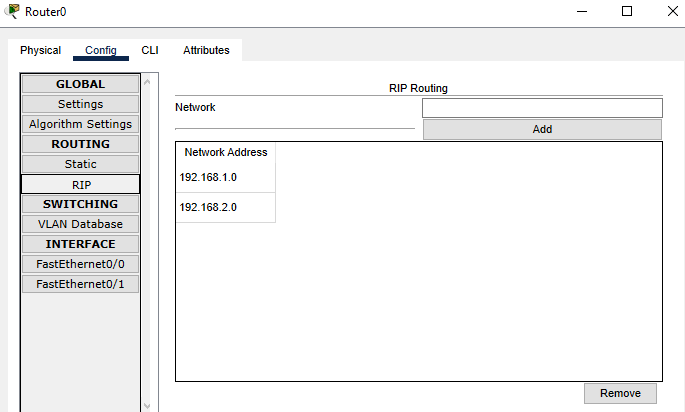
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **interface** | **IP Address** | **Subnet Mask** | **Default Gateway IP** | **DNS Server IP** |
| 1 | PC0 | Fa0 | 192.168.2.7 | 255.255.255.0 | 192.168.2.3 | 0.0.0.0 |
| 2 | PC1 | Fa0 | 192.168.2.8 | 255.255.255.0 | 192.168.2.3 | 0.0.0.0 |
| 3 | PC2 | Fa0 | 192.168.3.5 | 255.255.255.0 | 192.168.3.3 | 0.0.0.0 |
| 4 | PC3 | Fa0 | 192.168.3.7 | 255.255.255.0 | 192.168.3.3 | 0.0.0.0 |
| 5 | ROUTER 0 | Fa0/0 | 192.168.2.3 | 255.255.255.0 |  |  |
| 6 | ROUTER 0 | Fa0/1 | 192.168.1.2 | 255.255.255.0 |  |  |
| 7 | ROUTER 1 | Fa0/0 | 192.168.3.3 | 255.255.255.0 |  |  |
| 8 | ROUTER 1 | Fa0/1 | 192.168.1.4 | 255.255.255.0 |  |  |



**On router 0:**

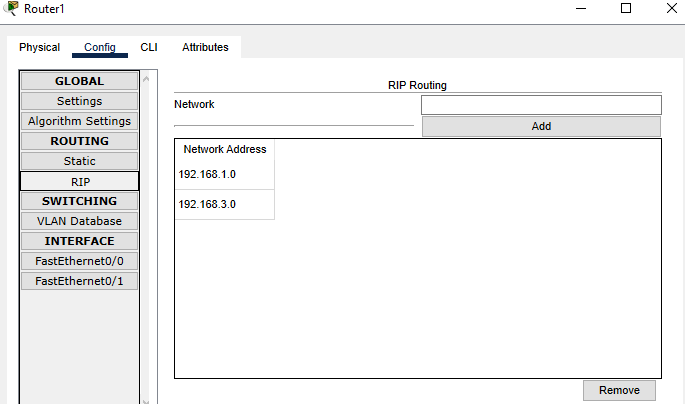
* **Configure router as given in picture below**

**Go to settings tab and then save the settings**



**On router 1:**

* **Configure router as given in picture below**
* **Go to settings tab and then save the settings**



EXPECTED OUTPUT:



**Conclusion:**

**Here we have studied about implementation and study routing at Network layer**

**We also created static and dynamic routing and our implementation done successfully**

## **EXPERIMENT NO : 10**

**AIM: Experiments on Transport Layer**

**Theory:**

FTP (File Transfer Protocol) is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Although many file transfers can be conducted using Hypertext Transfer Protocol (HTTP) -- another protocol in the TCP/IP suite -- FTP is still commonly used to transfer files behind the scenes for other applications, such as banking services

FTP is a client-server protocol that relies on two communications channels between the client and server: a command channel for controlling the conversation and a data channel for transmitting file content

Here is how a typical FTP transfer works:

• A user typically needs to log on to the FTP server, although some servers make some or all of their content available without a login, a model known as anonymous FTP.

• The client initiates a conversation with the server when the user requests to download a file.

• Using FTP, a client can upload, download, delete, rename, move and copy files on a server.

FTP sessions work in active or passive modes:

1. Active mode. After a client initiates a session via a command channel request, the server creates a data connection back to the client and begins transferring data.

2. Passive mode. The server uses the command channel to send the client the information it needs to open a data channel. Because passive mode has the client initiating all connections, it works well across firewalls and network address translation gateways.

**Implementation**

**INPUT:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Name of Components/Device** | **interface** | **IP Address** | **Subnet Mask** | **Default Gateway IP** | **DNS Server IP** |
| 1 | PC0 | Fa0 | 192.168.0.1 | 255.255.255.0 | 0.0.0.0 | 192.168.0.5 |
| 2 | PC1 | Fa0 | 192.168.0.2 | 255.255.255.0 | 0.0.0.0 | 192.168.0.5 |
| 3 | PC2 | Fa0 | 192.168.0.3 | 255.255.255.0 | 0.0.0.0 | 192.168.0.5 |
| 4 | PC3 | Fa0 | 192.168.0.4 | 255.255.255.0 | 0.0.0.0 | 192.168.0.5 |
| 5 | Server-PT | Fa0/0 | 192.168.0.5 | 255.255.255.0 | 0.0.0.0 | 192.168.0.5 |

A diagram of a network

Description automatically generated

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

**DNS Client**

**A screenshot of a computer

Description automatically generated A screenshot of a computer program

Description automatically generated**

**EMAIL Client**

**A computer screen shot of a computer screen

Description automatically generated A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated**

**FTP Client**

**A screenshot of a computer

Description automatically generated A screenshot of a computer program

Description automatically generated A computer screen shot of a black screen

Description automatically generated**

**Conclusion**:

**Here We have conducted an experiment and gained a thorough understanding of transport layer concepts. Our implementation was successful.**