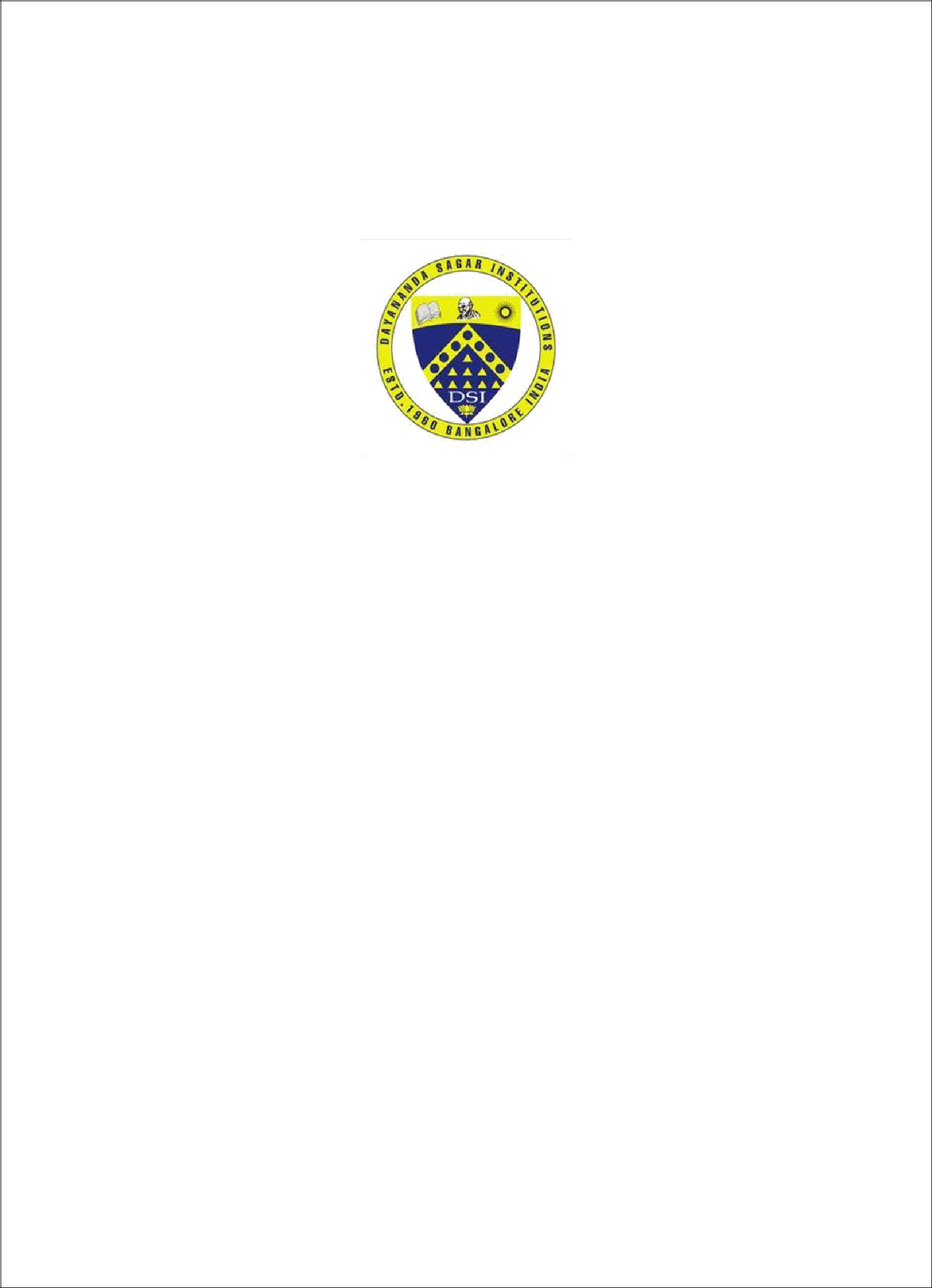
**DAYANANDA SAGAR COLLEGE OF ENGINEERING**

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with ‘A’ grade, Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078.

**Minor Project Report**

**on**

**“Project Title”**

Submitted By

Joseph Raj Vishal-1DS20CS093

Jyothi R-1DS20CS094

K L Kalpana-1DS20CS095

**Fifth Semester B.E (CSE)**

**in**

**Computer Networks Laboratory**

**19CS5DLCNL**

Under the guidance of

**Dr. Nagaraja J.**

**Associate Professor**

**Dept. of CSE**

**DSCE, Bangalore**

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Contents** | **Page** |
| 1 | Abstract |  |
| 2  3 | Introduction  Types of SSH Encryption | 1  2 |
| 4 | Design and Configuration | 3 |
| 5    6 | Topology  Real Time and Simulation Mode Results | 8  9 |
|  |  |  |
| 7 | Conclusion and Future Enhancement | 12 |

**1.Abstract**

The secure shell protocol strives to protect the privacy of its users in several ways. On one hand, the strong encryption and authentication algorithms that it adopts provide guarantees that the data exchanged between two SSH endpoints remain private to third parties. On the other hand, the type of traffic that each SSH channel transports, such as e-mail, remote shell activity, etc., is also supposed to be hidden from any observer that does not possess the necessary keys. This paper introduces a simple but accurate model of the SSH channel which can be used to study the level of privacy that SSH-protected traffic can achieve concerning the users' activities. In this project, this project focuses on configuring routers from remote PCs using the SSH protocol.

Secure Shell (SSH) is designed to provide secure remote login and other security services in insecure network environments. When users remotely access the switch across an insecure network, SSH will automatically encrypt data before transmission and decrypt data after they reach the destination to guarantee information security and protect switches from such attacks as plain-text password interception. In addition, SSH provides powerful authentication to defend against the man-in-the-middle attacks. SSH uses the client/server mode, by which the SSH server accepts the connection requests from SSH clients and provides authentication. SSH clients can establish SSH connections and log into the SSH server through the SSH connections.

SSH also provides other functions, such as compressing the data to be transmitted to speed up the transmission speed, functioning as Telnet, and providing secure channels for FTP, PoP and even PPP.

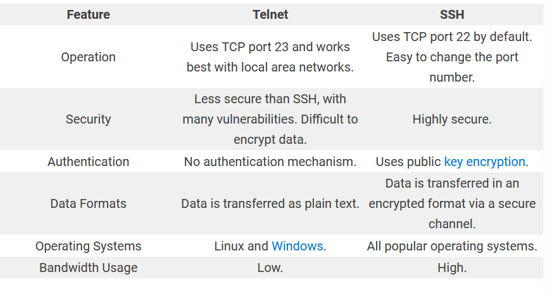
**2.Introduction**

# **SSH or Secure shell is a network communication protocol, which is the protocol that enables two computers to communicate and share data. An inherent feature of SSH is that communication is encrypted meaning that it’s suitable for use on insecure networks. It is an application layer protocol.**

# SSH is an acronym for “Secure Shell”, and is a [TCP](https://www.netburner.com/learn/tcp-vs-udp-battle-of-the-protocols/)  application protocol used to make secure connections to a remote device in order to perform file-sharing or host configuration tasks. This protocol was born as a successor to the [Telnet protocol](https://en.wikipedia.org/wiki/Telnet), which essentially serves to perform the same tasks as SSH. The only problem with Telnet is that the information was totally transparent during transmission, i.e., it had no encryption. This made it an excellent target for people who wanted to get your information. Using Telnet on the modern Internet is totally unthinkable because of all the security breaches it could cause.

# Telnet stands for**Tel**etype **Net**work. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard [**TCP/IP protocol**](https://www.geeksforgeeks.org/tcp-ip-in-computer-networking/) for virtual terminal service which is given by [**ISO**](https://www.geeksforgeeks.org/iso-full-form/).

Differences between Telnet and SSH :

****

**Figure 1**

1|Mini Project Computer Networks Laboratory 2022

**3.Types of SSH Encryptions**

**Symmetric encryption –shared key encryption, symmetric encryption is usually a single key or a pair of keys used for both encryption and decryption. Used to encrypt the entire session of communication. The key is calculated on agreed methods**

**Asymmetric encryption – Uses a pair of keys for encryption and decryption. These are called public and private keys. The public key is distributed private key is closely related to the public key in terms of functionality but cannot be calculated just by knowing the public key.**

# **Hashing-Hashing is the process of mapping any arbitrary size data into a fixed-length value using a hash function. This fixed-length value is known as a hash value, hash code, digest, checksum, or simply hash.**

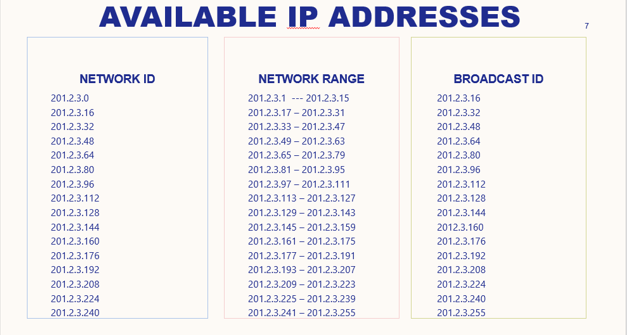
**We have subdivided the project for ease of design into 7 divisions.**

1. Configurations of IP
2. Router Name Change and Configuration
3. Domain Data and Data Encryption
4. Router User Config
5. SSH Config
6. EIGRP
7. SSH Verification

2|Mini Project Computer Networks Laboratory 2022

**4.Design and Configuration**

1. **Configurations of IP**

****

**Figure 2**

Step 1: Find out the number of bits to be borrowed from host

2^3=8

Step 2: Design new Subnet mask Find

Old= 255.255.255.00000000

New=255.255.255.11100000

Step 3: Find out Block size 🡺 2^5 = 32

Step 4: Design the IP table as shown above

**2.Router Name Change and Configuration**

**Router 0**

GigabitEthernet0/0-201.2.3.18

GigabitEthernet0/1- 201.2.3.33

GigabitEthernet0/2-201.2.3.49

Serial 0/3/0-201.2.3.65

Serial 0/3/1-201.2.3.225

**Router 1**

GigabitEthernet0/0-201.2.3.83

GigabitEthernet0/1-201.2.3.97

3|Mini Project Computer Networks Laboratory 2022

GigabitEthernet0/2-201.2.3.113

Serial 0/3/0-201.2.3.66

Serial 0/3/1-201.2.3.210

**Router 2**

GigabitEthernet0/0-201.2.3.177

GigabitEthernet0/1-201.2.3.161

Serial 0/3/0-201.2.3.209

Serial 0/3/1-201.2.3.242

**Router 3**

GigabitEthernet0/0-201.2.3.129

GigabitEthernet0/1-201.2.3.145

GigabitEthernet0/2-201.2.3.193

Serial 0/3/0-201.2.3.226

**Serial 0/3/1-201.2.3.241**

Router: Routers are networking devices operating at layer 3 or a network layer of the OSI model.

Enable: To make operational or activate through a software setting, a hardware button or a jumper.

Config: A Configuration is the arrangement or the process of making the arrangement of the parts that make up a whole.

Interface gigabitEthernet0/0: gigabitEthernet0/0 is up, line protocol is up(connected).

No Shutdown: The command “no shutdown” enable the interface to move from administration down status to UP.

**Steps to configure router**

Router # configure terminal

Router (config) # interface GigabitEthernet0/0

Router (config-if) # ip address 201.2.3.18 255.255.255.240

Router (config-if) # no shutdown

Router (config) # exit

Router (config) # hostname R1

4|Mini Project Computer Networks Laboratory 2022

**3.Domain Data and Data Encryption**

In this project domain name was changed. The domain name will be cisco.com. And after that we will encrypt the data with “crypto key generate rsa” command.

Show IP SSH: Displays SSH connections details.

Hostname R1: A Hostname is a unique name given to a device router R1on a network and is used to identify one device from another on a specific network over the internet.

IP Domain name: An IP domain name is used on a router so the router can do look ups.

**4.Router User Config**

Username admin privilege 15 secret cisco: Cisco devices use privilege levels to provide password security for different levels of switch operation

There are 5 admins one for each router and one admin who is

Router (config) # username admin privilege 15 secret cisco

**5.SSH Config**

Crypto Key generate RSA: SSH may generate an additional RSA key pair if we generate a key pair on a router having no RSA keys.

Modulus 1024: Command prompt crypto key generate modulus 1024.

IP SSH Version 2: SSH Version 2 Configuration, the SSH protocol is a method

for secure remote login from one device to other.

Line vty 0 15: It is kind of range command, we are giving range of vty(virtual terminal line) from 0 to 15.

Transport input SSH: We use the cisco ‘transport input’ command to set which protocols are allowed to access the virtual terminal lines.

Router (config) # ip ssh version 2

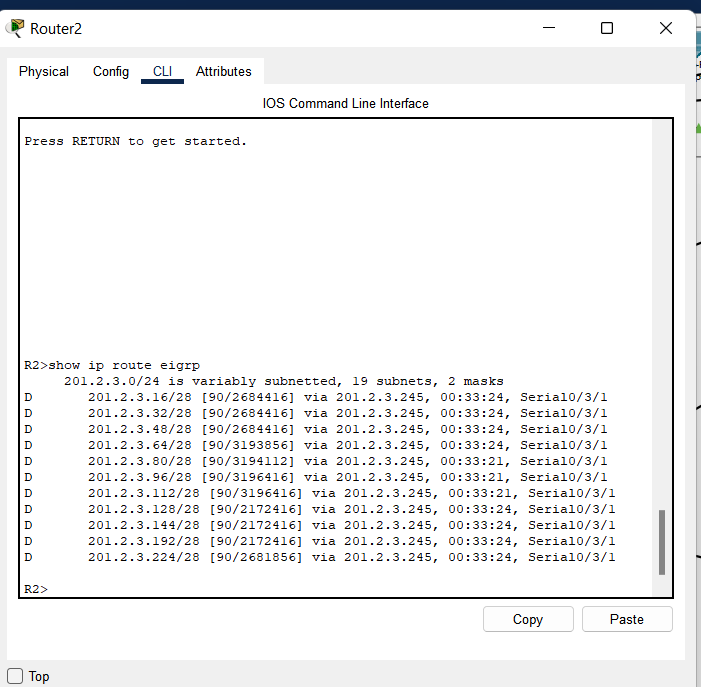
Router (config) # crypto key generate rsa general-keys modulus 1024

Router (config) # line vty 0 15

Router (config-line) # transport input ssh

5|Mini Project Computer Networks Laboratory 2022

**6.EIGRP:** The Enhanced Interior Gateway Routing Protocol is a network routing protocol which promotes an efficient information exchange between the routers. This routing protocol is developed by Cisco and is compatible only with Cisco hardware (routers) and not with other vendors. EIGRP is an advanced distance vector protocol version of RIP.

****

**Figure 3 (EIGRP Routing Protocols for Router 2)**

**7.SSH Verification**

Login local: Login local command is used to ensure the secure remote login by telnet

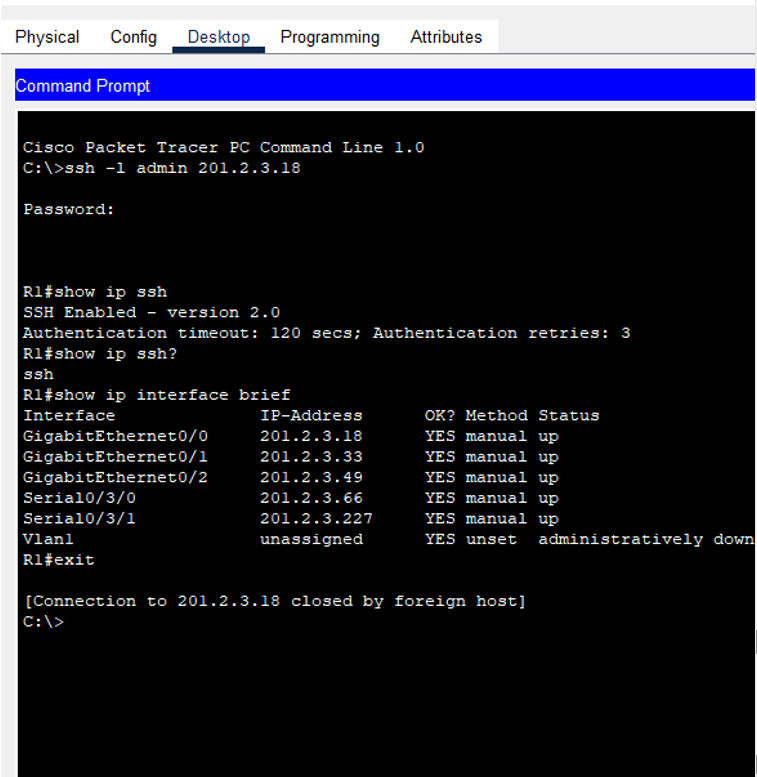
and it is also used to store the information about that remote users in the database.

To verify we can try to connect via SSH from PC to the router.

PC0>ssh -l admin 201.2.3.18

R1#

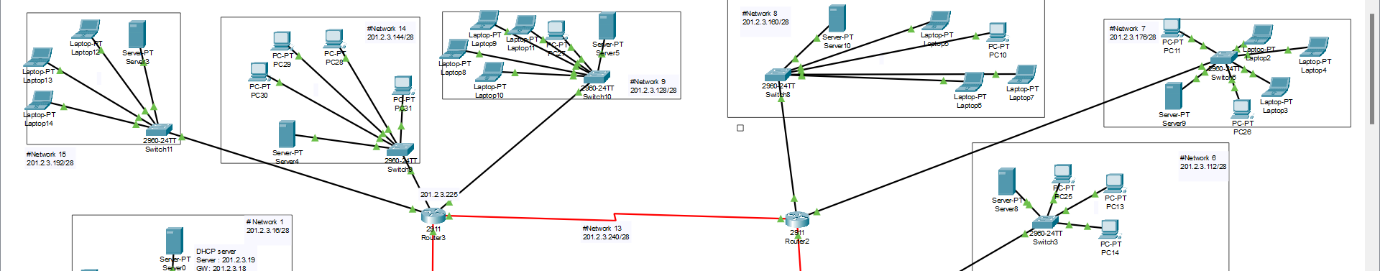
6|Mini Project Computer Networks Laboratory 2022

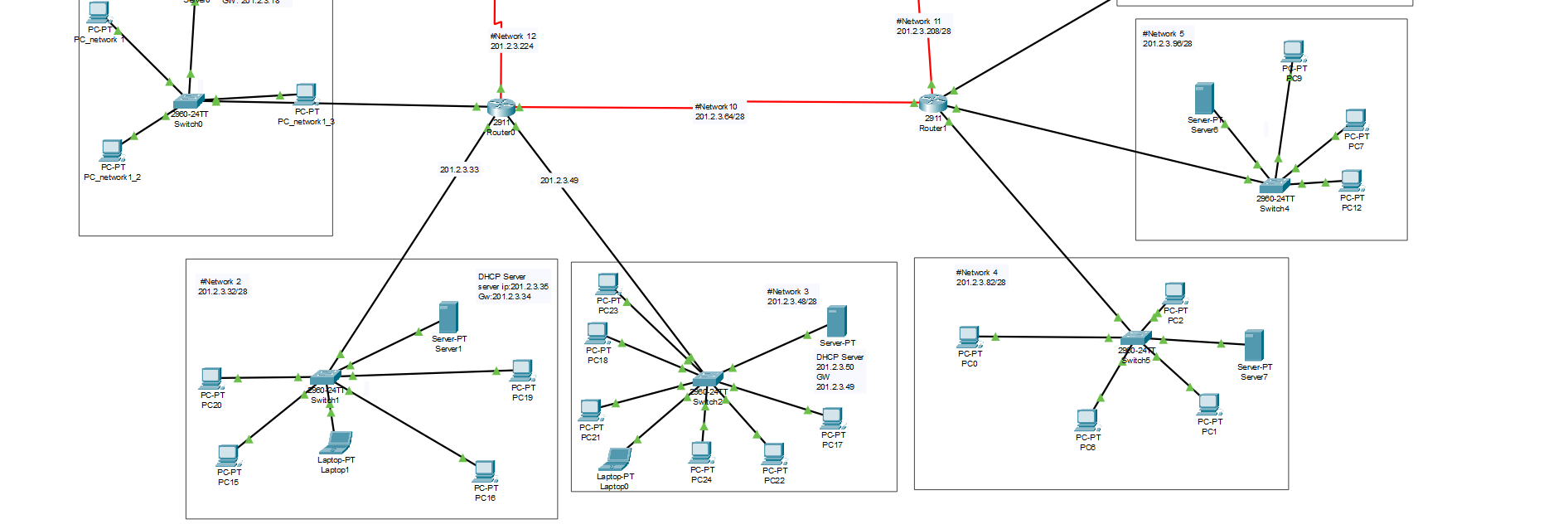
****

**Figure 4 (SSH Verification)**

7|Mini Project Computer Networks Laboratory 2022

**5.Topology:**

****

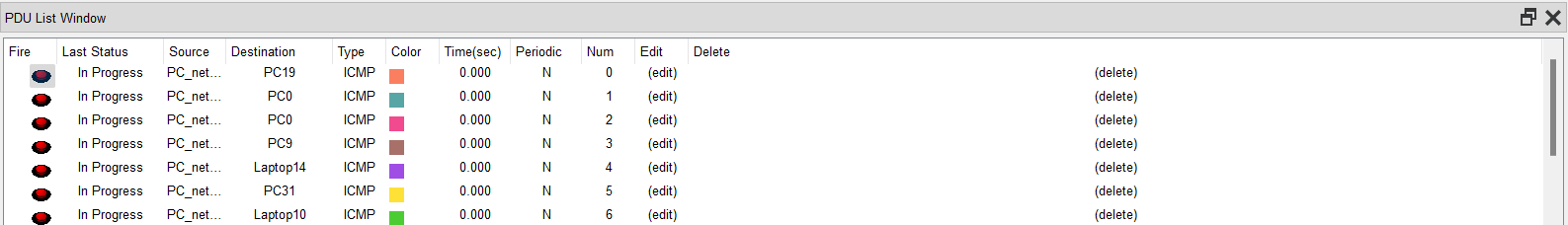
****

The Topology is made up of simple components such as 2911 Routers   
( 4 in number), PT-Switches for each Router, and 11 DHCP server.

There are 4 networks between each router and 11 networks.

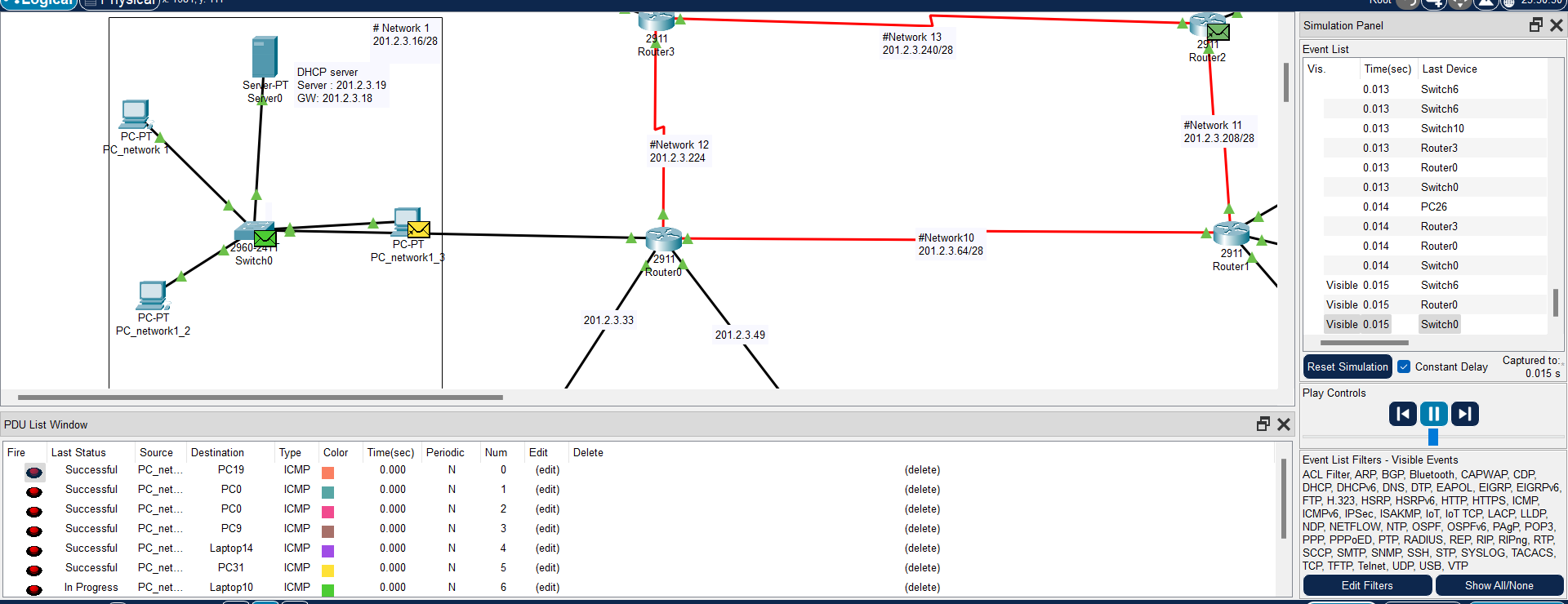
8|Mini Project Computer Networks Laboratory 2022

**6.Real Time and Simulation Mode**

****

**Figure 6 (Real Time Simulation Mode)**

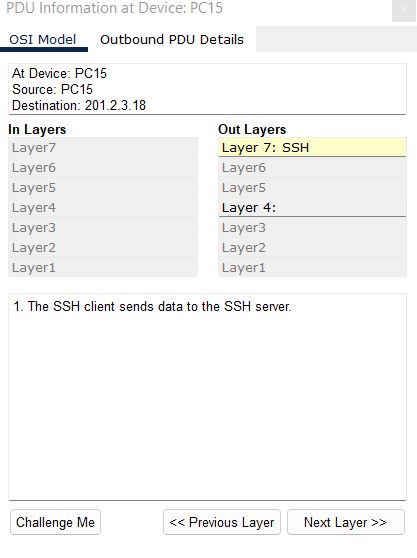
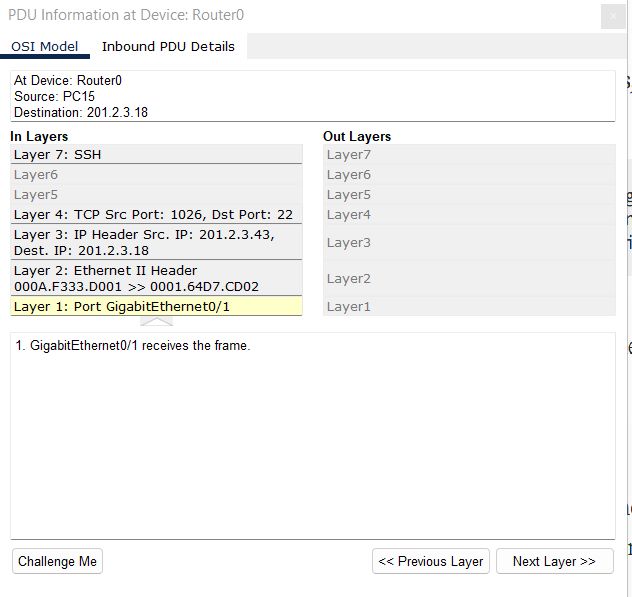
**Simulation Mode Results**

****

**Figure 7 (Shows Simulation mode)**

9|Mini Project Computer Networks Laboratory 2022

**Inbound and outbound PDU details of router and switch**

****

**Figure 8.1 and 8.2**

**(From clockwise Device 15 outbound info , Router 0 inbound PDU details , Switch inbound PDU details ,**

**OSI Model of switch 1 showing SSH Figure on be left Protocols of Router 0 , Protocols of PC15 on right)**

10|Mini Project Computer Networks Laboratory 2022

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

11|Mini Project Computer Networks Laboratory 2022

**7.Conclusion and Future Enhancements**

We wish to enhance our project by configuration of DNS servers in each network, adding a multi way switch and hubs.

12|Mini Project Computer Networks Laboratory 2022