# LAB of Scalable Network

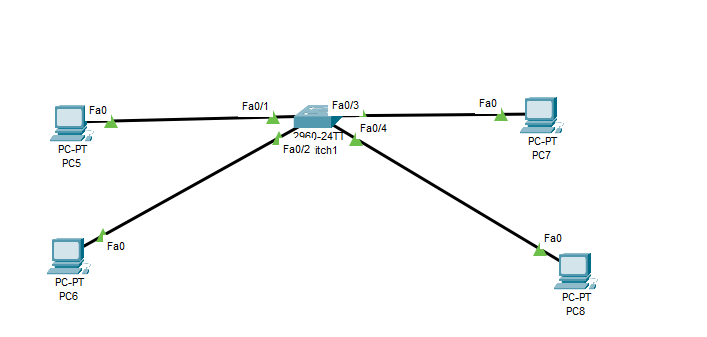


Figure 1 Vlan Design

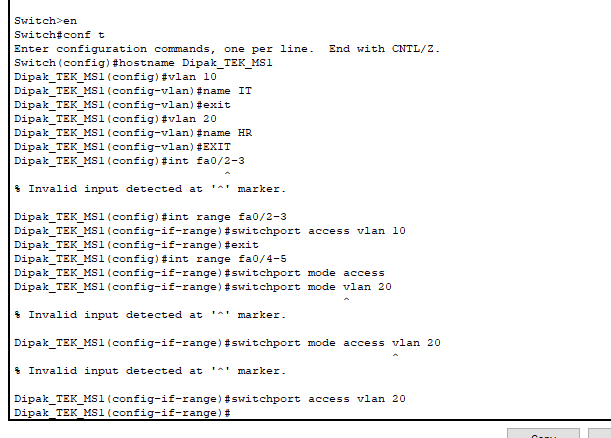


Figure 2 Vlan configuration sw1

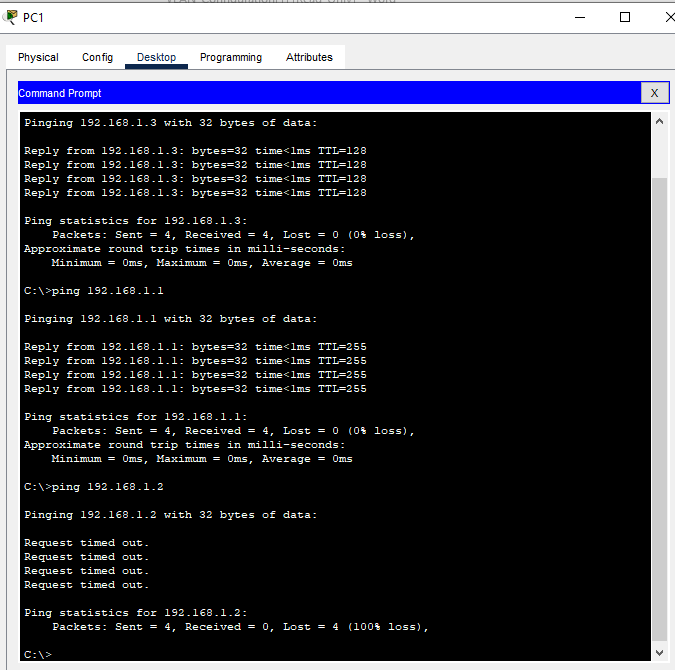


Figure 3 Vlan output

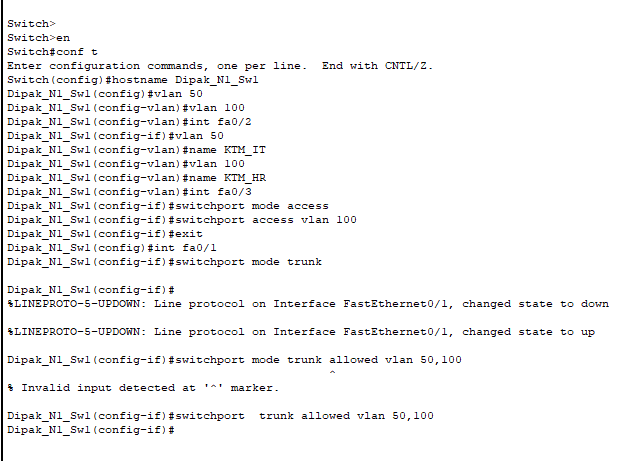


Figure 4 Vlan trunk sw1

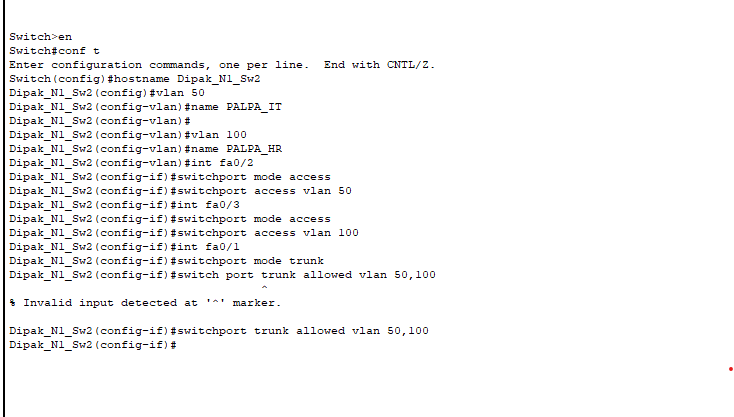


Figure 5 Vlan trunk sw2

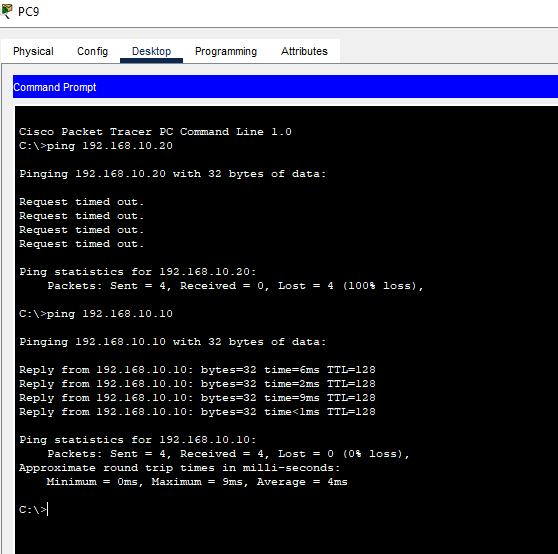


Figure 6 output Vlan trunk

# Redundancy Protocols for Scalability

Fundamental mechanisms of redundancy protocols towards high network availability, fault tolerance, and scalability. The protocols in this case are made up of multiple strategies such as fail safer, redundancy and fault tolerance mechanisms that are designed to allow continuous operation under hostile circumstances in case failures are not anticipated. In general, redundancy protocols serve as a safety measure in network architecture to allow for more traffic, change, and fault tolerance. Organizations deploy these protocols to assure not only high availability but scalability as well on the networks infrastructures, to support growing business requirements and new technology developments. Taken together, the above mentioned set of protocols constitute an underlying foundation for building a flexible, enlarged, strong network infrastructures that can withstand the vagaries of changing and emerging digital environment.

# Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP)

The heart of redundancy protocol is spanning tree protocol (STP) and its improved version Rapid Spanning Tree Protocol (RSTP). This is because STP mitigates network loops by blocking redundant paths and maintaining a loop free topology. On the other hand, it can result into improper use of available network resources. Unlike RSTP, it increases scalability by quickly adjusting for topological alterations, reducing convergence time, and fast recovery from link failure. Such protocols ensure that the network remains stable even though it was made scalable.

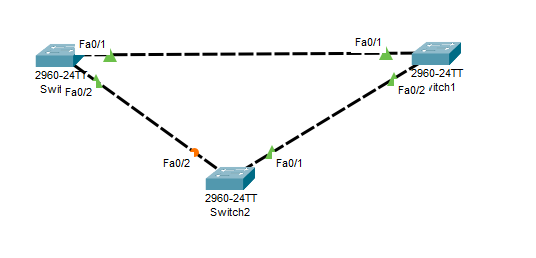


Figure 7 STP design

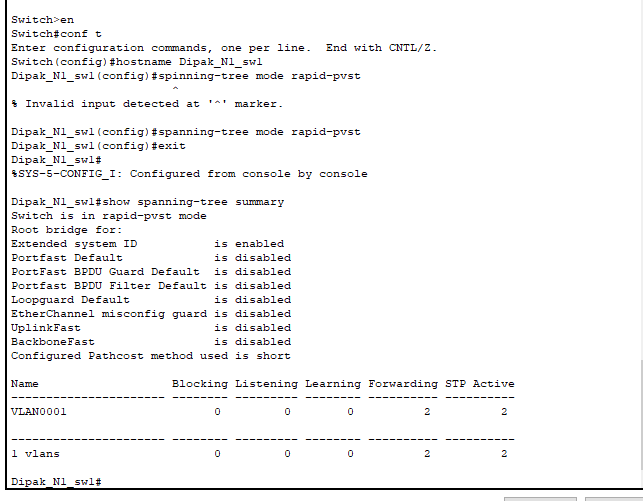


Figure 8 STP configuration sw1

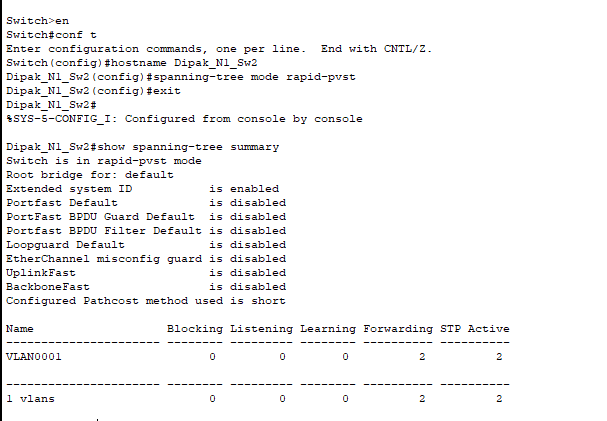


Figure 9 STP configuration sw2

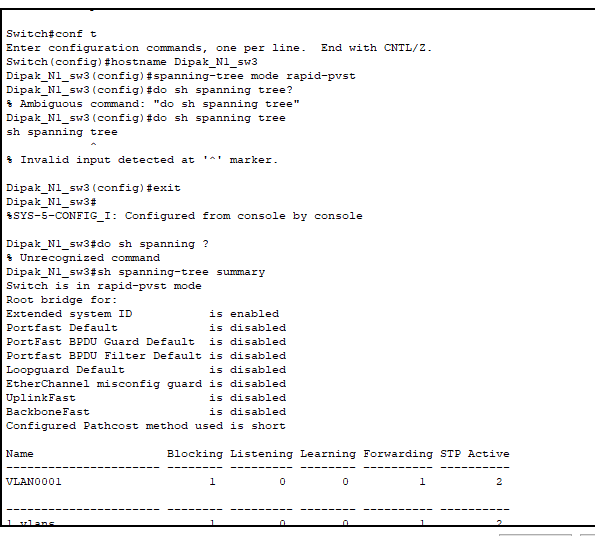


Figure 10 STP configuration sw3

# Virtual Router Redundancy Protocol (VRRP) and Hot Standby Router Protocol (HSRP)

At the routers level, the routers are introduced using the virtual router redundant protocol (VRRP) and the hot standby router protocol (HSRP). A backup router is configured to automatically step in and take over when the primary one fails so that there is no break in the connection to the network. These protocols help to improve scalability, ensuring that networks remain reliable, even when experiencing additional traffic loads and device failures; they do this by building a virtual router made up of several routers functioning concurrently.

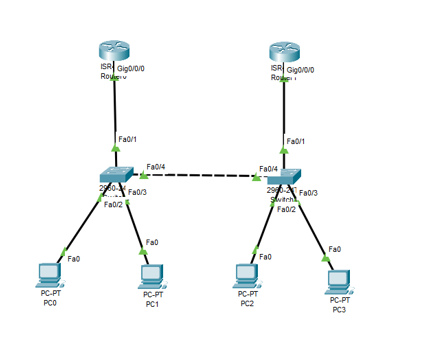


Figure 11 HSRP design

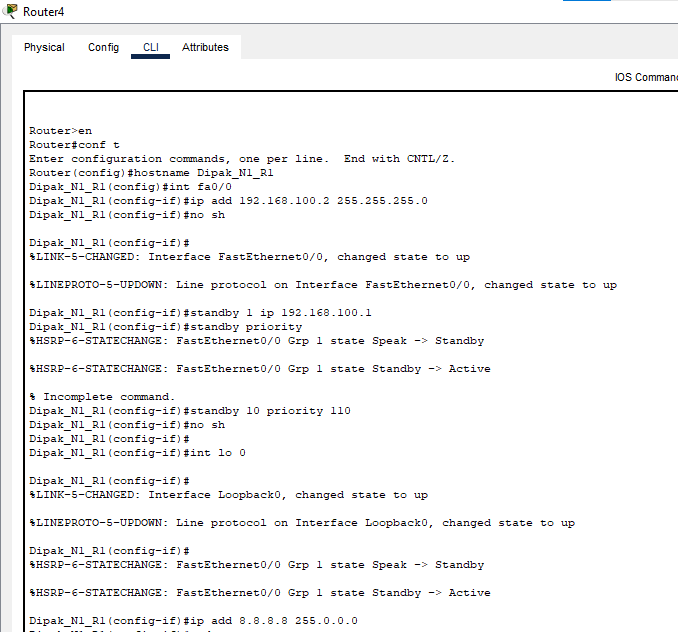


Figure 12 HSRP configuration R1

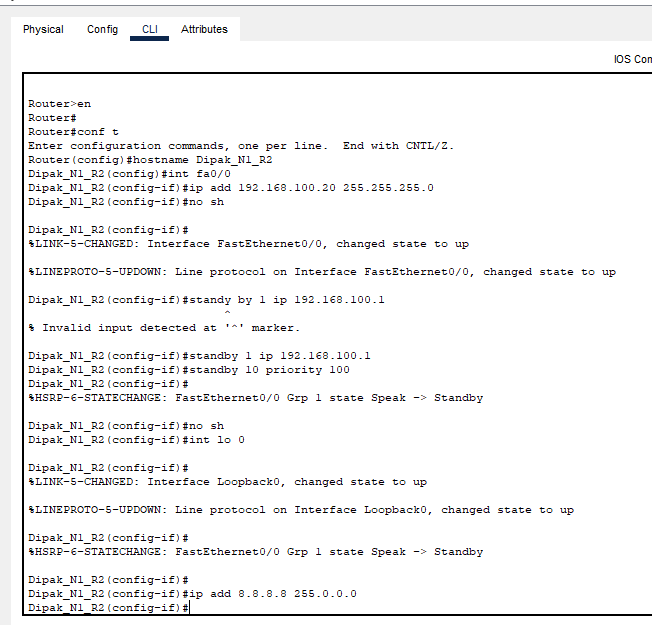


Figure 13 HSRP configuration R2

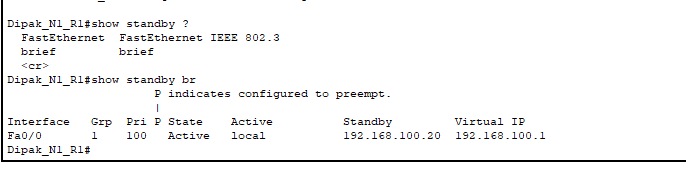


Figure 14 HSRP RESULTS

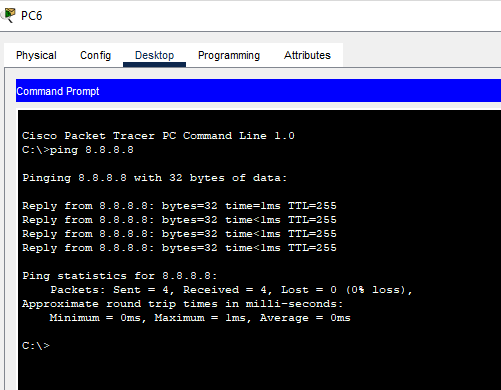


Figure 15 Ping Test HSRP

# Link aggregation protocols such as Ether Channel and Link Aggregation Control Protocol (LACP)

They address scalability through aggregating several physical links into one logical link using, for example, Ether Channel or LACP. By means of this aggregation, bandwidth and redundancy increases for uninterrupted data transmission and also improves network scalability. Moreover, dynamic routing protocols such as OSPP, EIGRP, and BGP alter routes depending upon change in a network to facilitate routing decisions and enable scaling while remaining scalable.

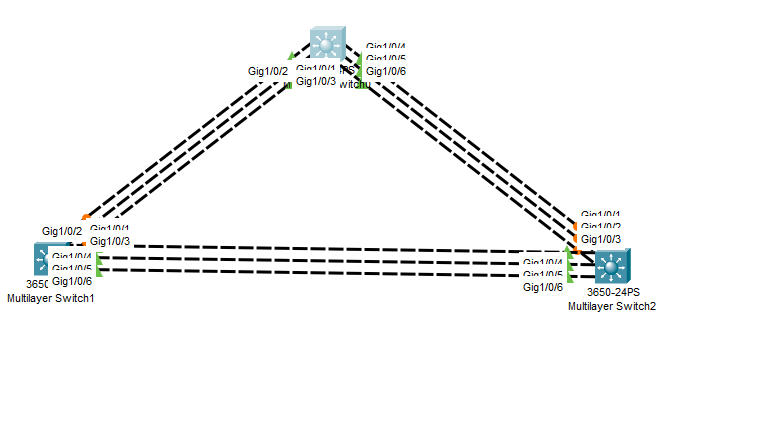


Figure 16 Ether-channel Design

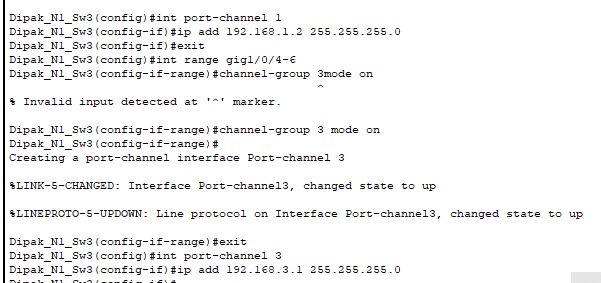


Figure 17 Switch configuration Ether-Channel

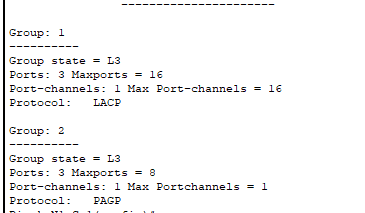


Figure 18 Showing Ether-Channel

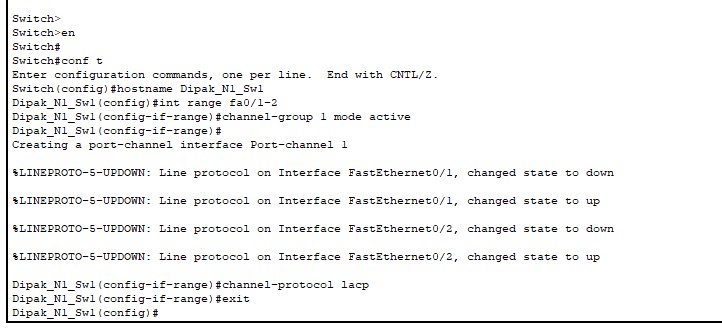


Figure 19 Link aggregation sw1

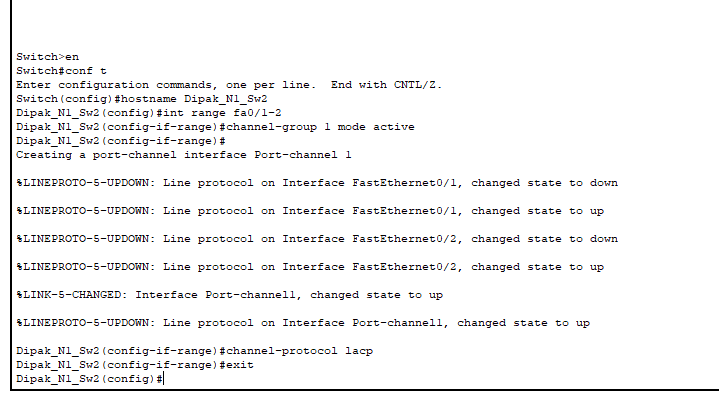


Figure 20 link aggregation 2

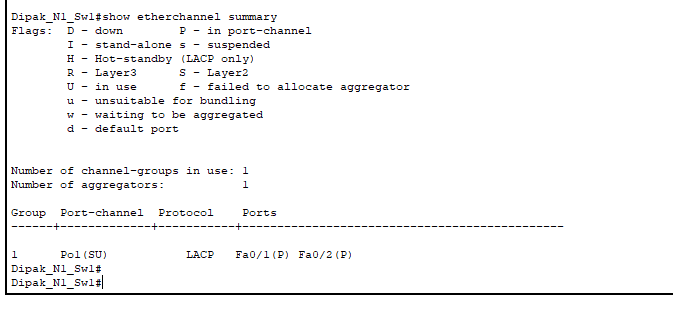


Figure 21 link aggregation output

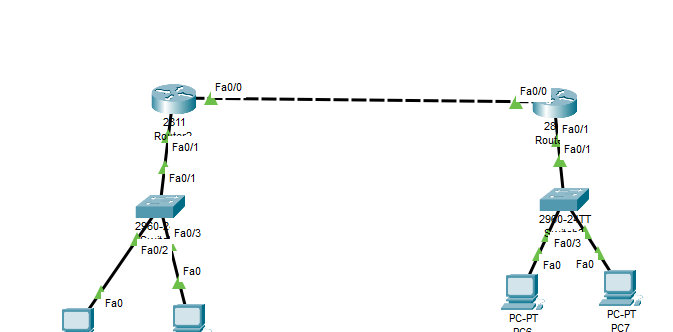


Figure 22 ipv6 design

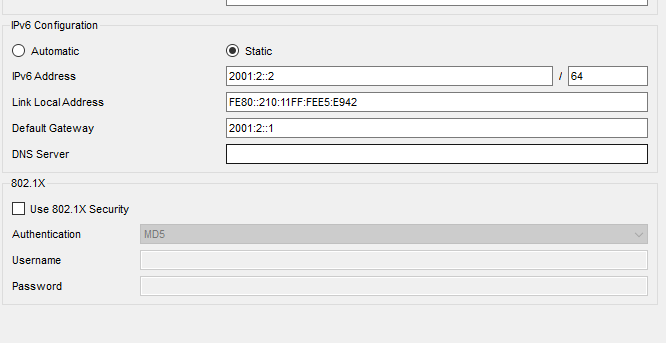


Figure 23 ipv6 into devices

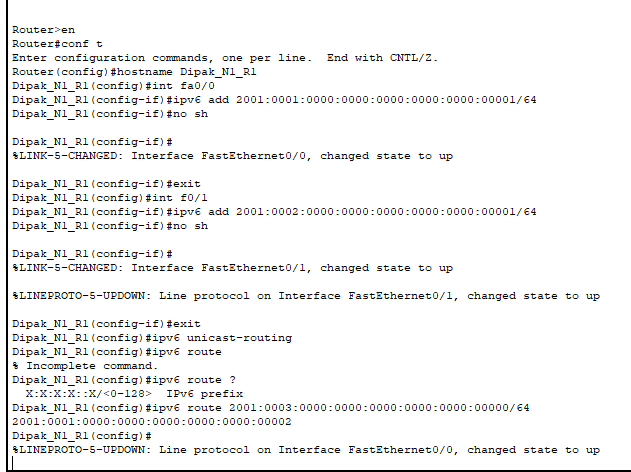


Figure 24 ipv6 Router Configuration R1

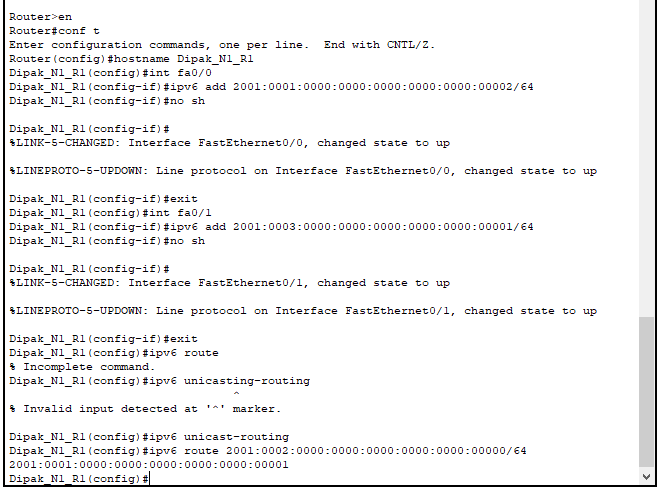


Figure 25 ipv6 Configuration R2

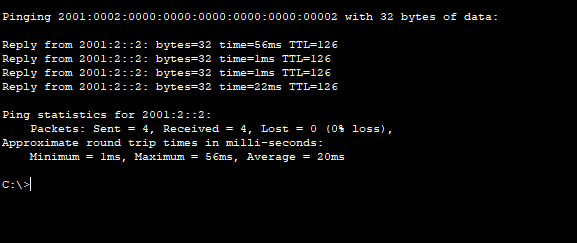


Figure 26 ipv6 output

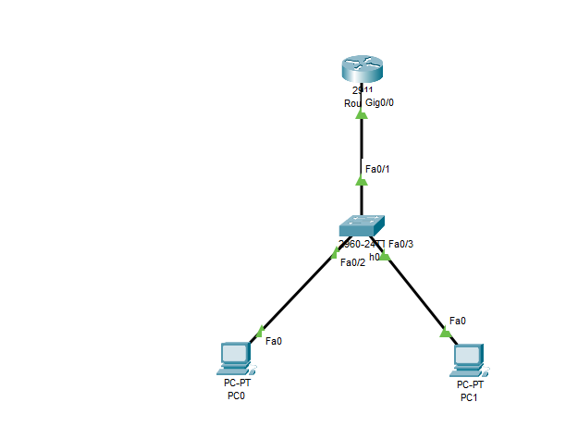


Figure 27 DHCP Design

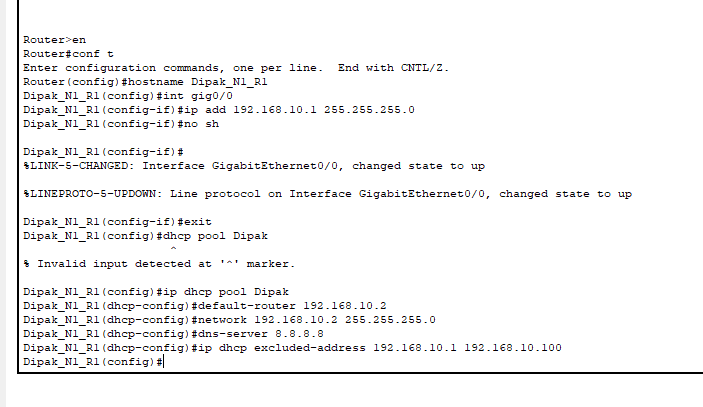


Figure 28 DHCP configuration

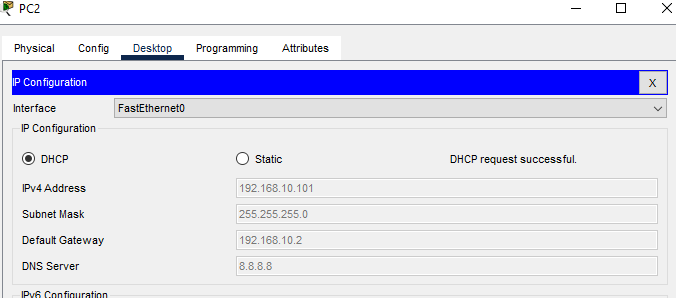


Figure 29 DHCP output

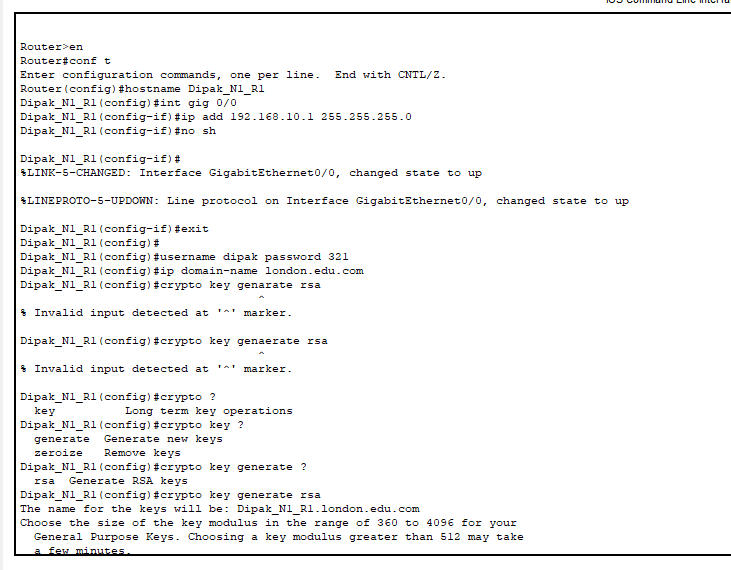


Figure 30 ssh cmd

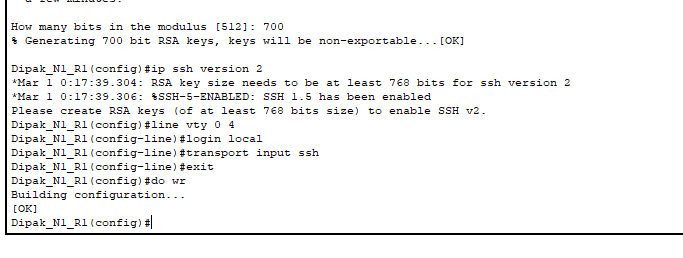


Figure 31 ssh cmd contd.

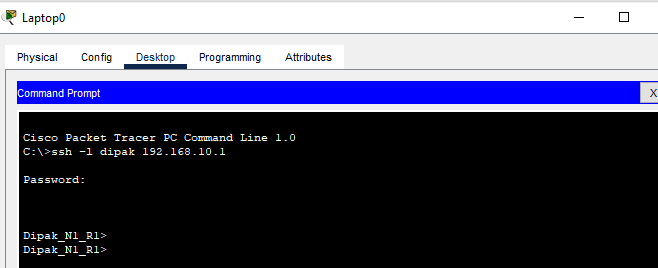


Figure 32 ssh output

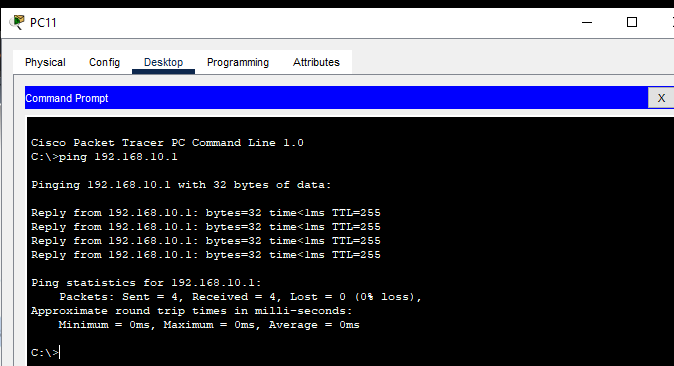


Figure 33 ssh ping configuration

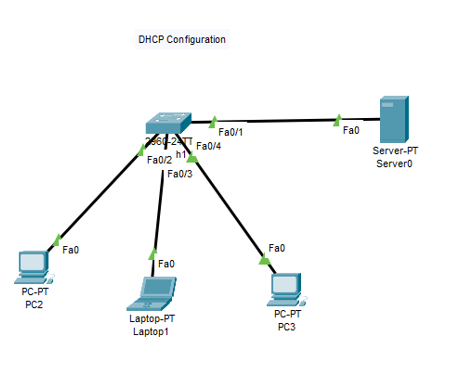


Figure 34 DHCP Server Design

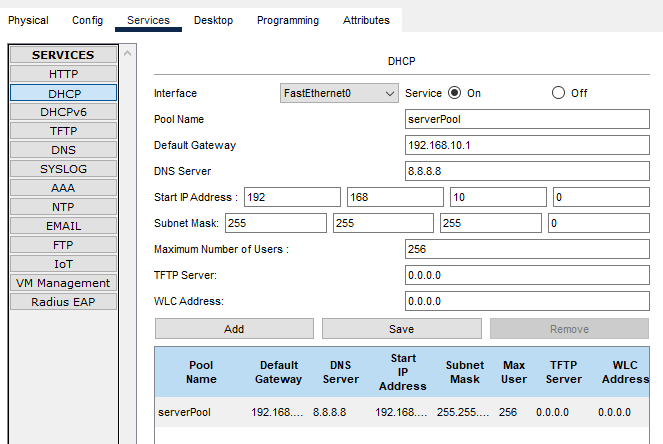


Figure 35 DHCP Server Configuration

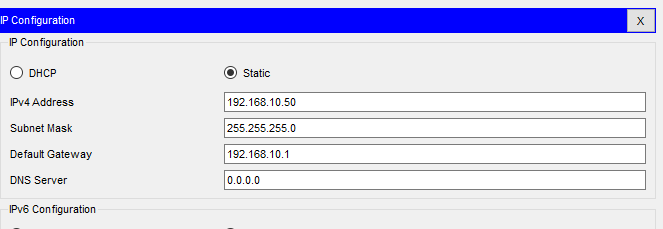


Figure 36 DHCP Server IP

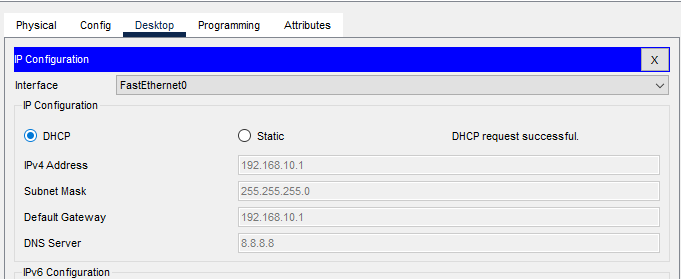


Figure 37 DHCP Server output

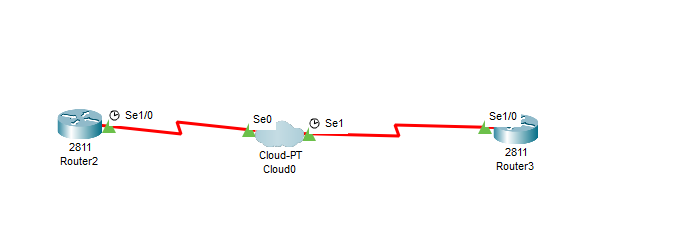


Figure 38 Frame Relay Design

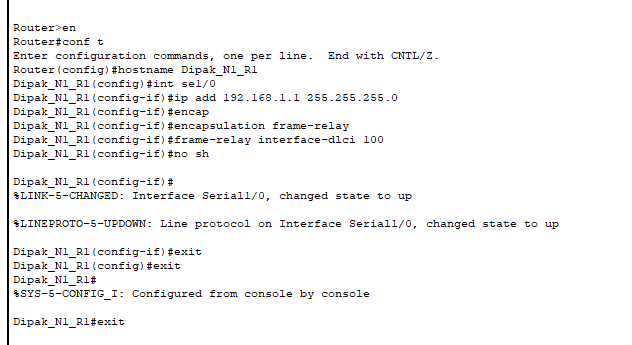


Figure 39 Frame Relay configuration R1

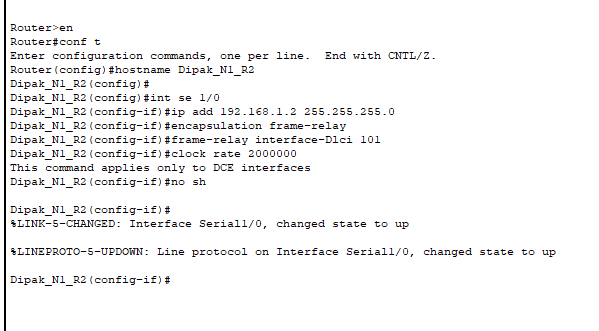


Figure 40 Frame Relay configuration R2

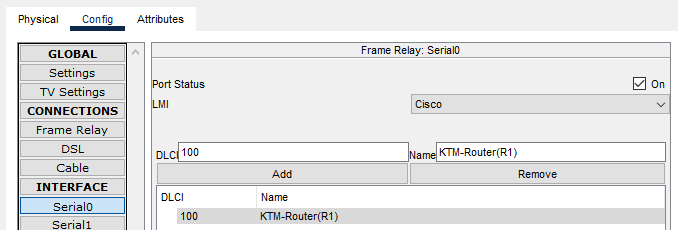


Figure 41 Frame Relay Cloud configuration 1

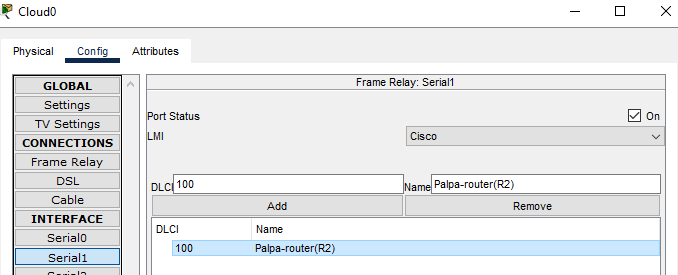


Figure 42 Frame Relay Cloud configuration 2

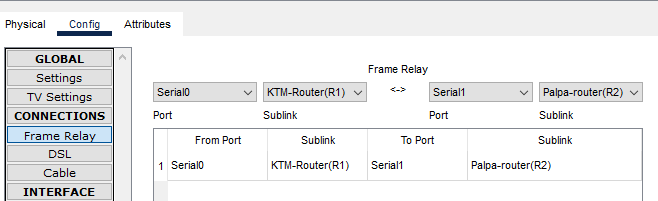


Figure 43 Frame Relay Cloud configuration 3

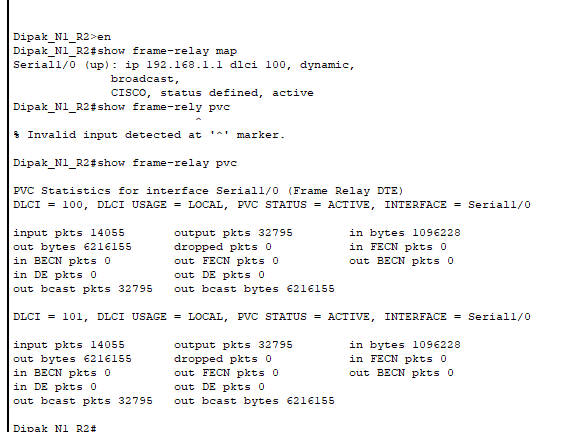


Figure 44 Frame Relay output 1

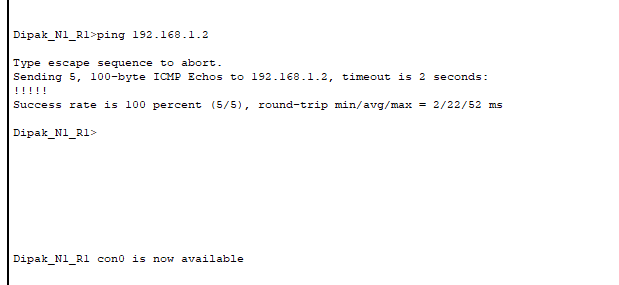


Figure 45 Frame Relay output 2

# VPN LAB

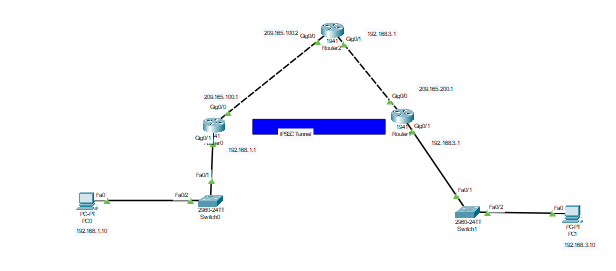


Figure 46 Design

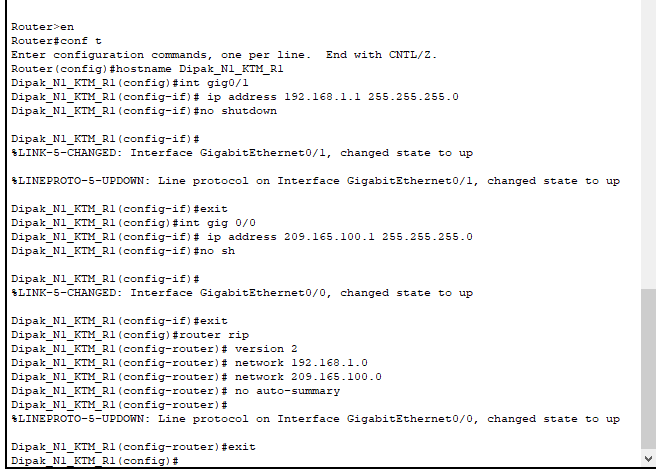


Figure 47 R1\_configuration

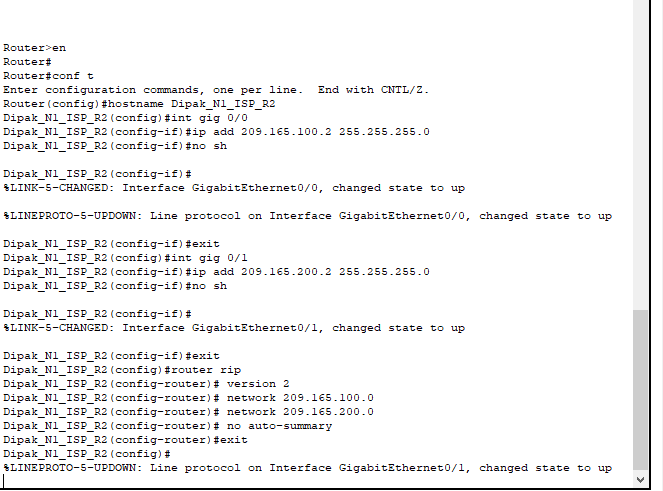


Figure 48 ISP router configuration

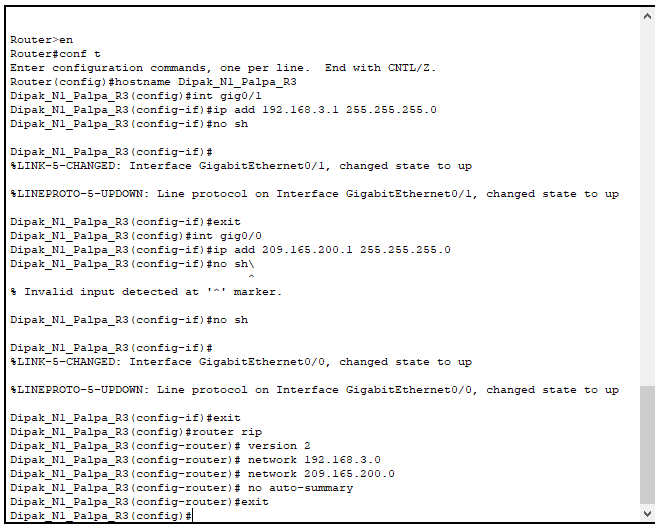


Figure 49 R3 router configuration

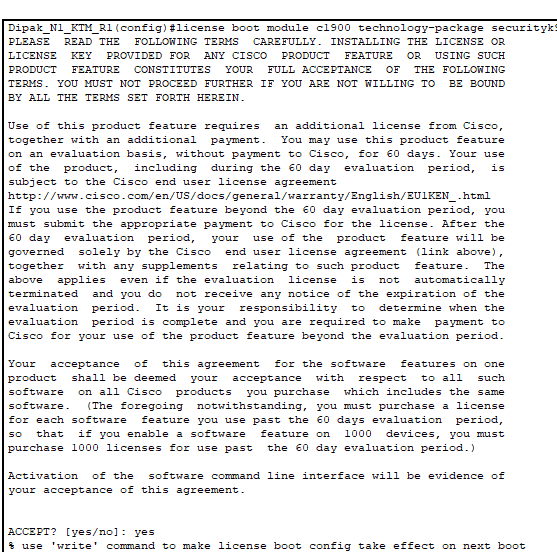


Figure 50 R1 License Agreement

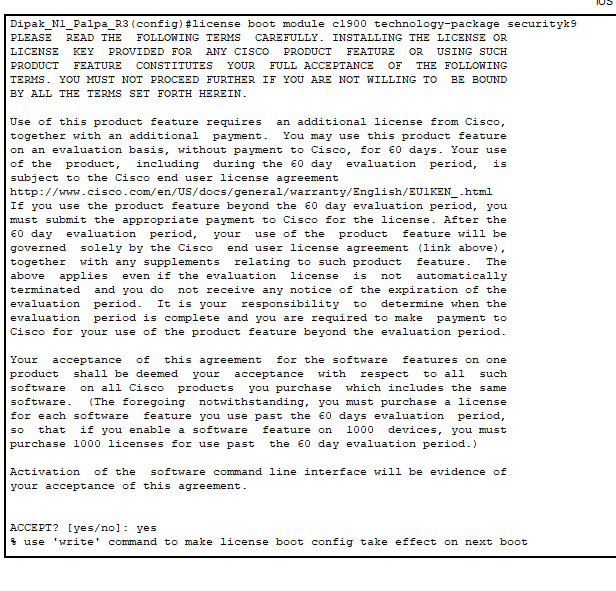


Figure 51 R3 license agreement

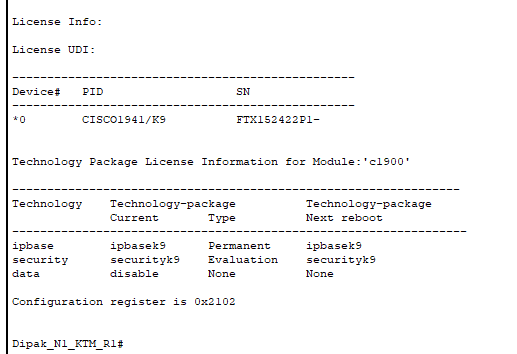


Figure 52 R1 license info

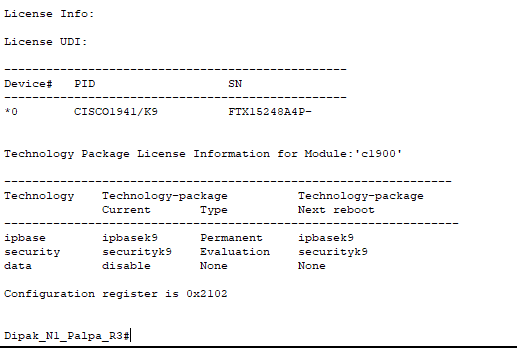


Figure 53 R3 license info

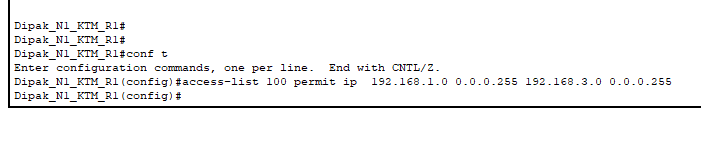


Figure 54 ACL define in R1

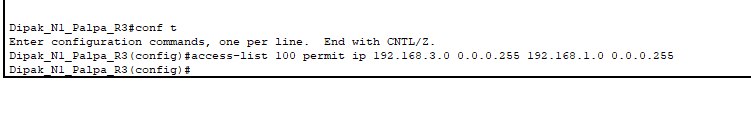


Figure 55 ACL Define in R3

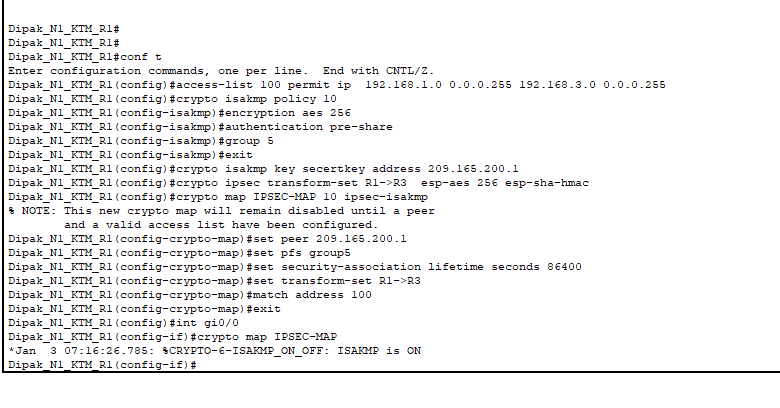


Figure 56 crypto/Map configuration R1

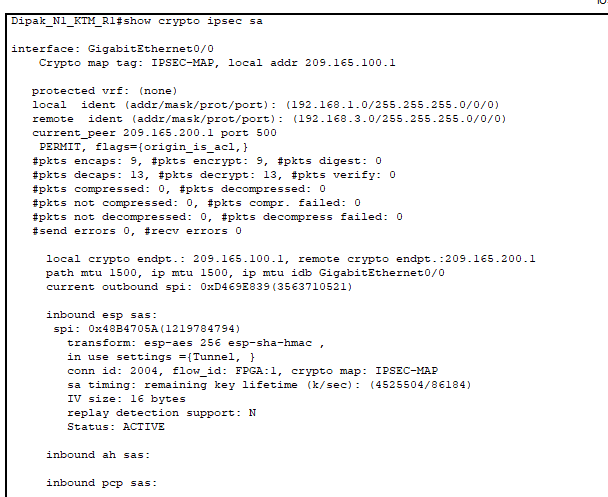


Figure 57 Showing Crypto ipsec sa R1

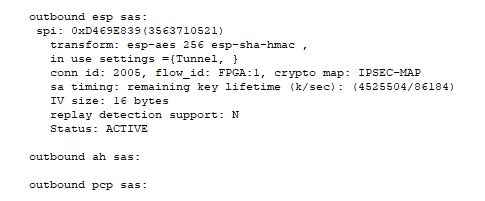


Figure 58 outbound esp R1

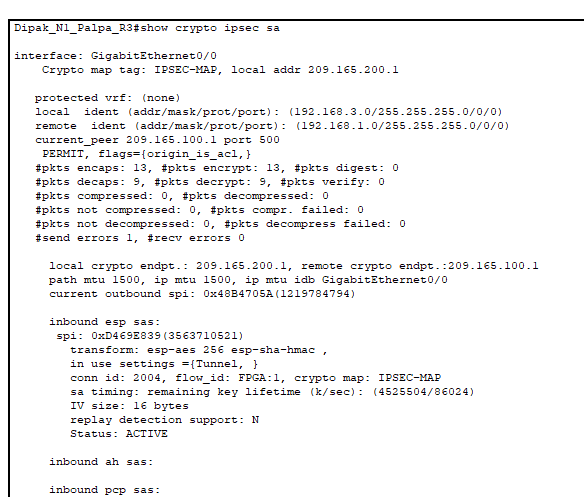


Figure 59 Showing Crypto ipsec sa R3

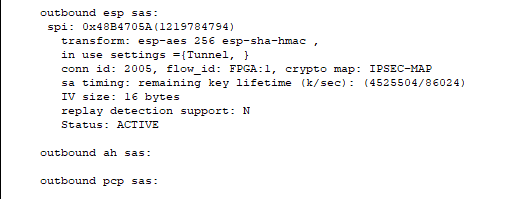


Figure 60 outbound esp R3

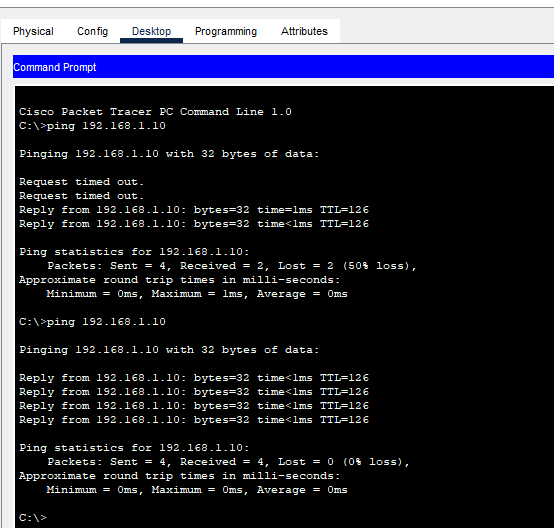


Figure 61 Ping Successfully

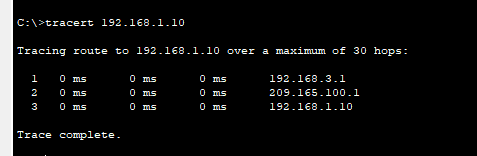


Figure 62 track

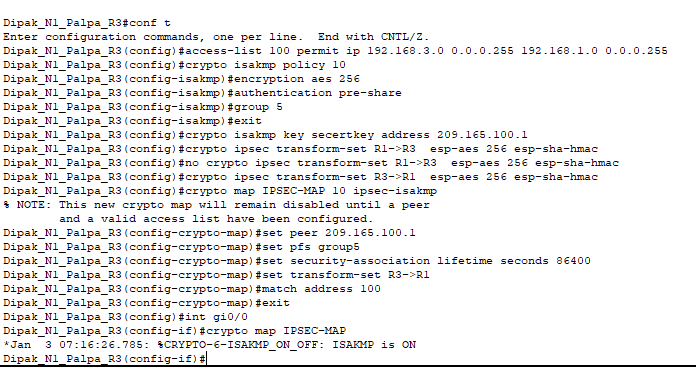


Figure 63 crypto/map configuration R3

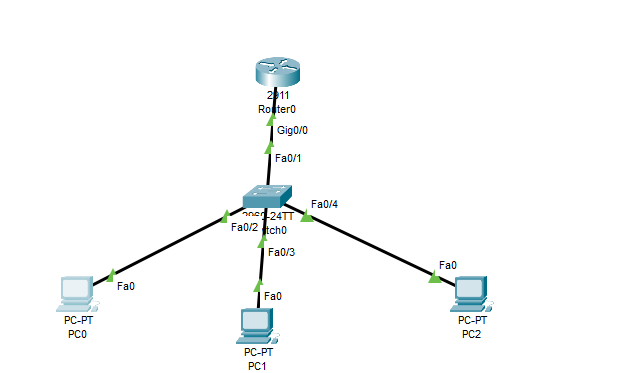


Figure 66 SNMP Design

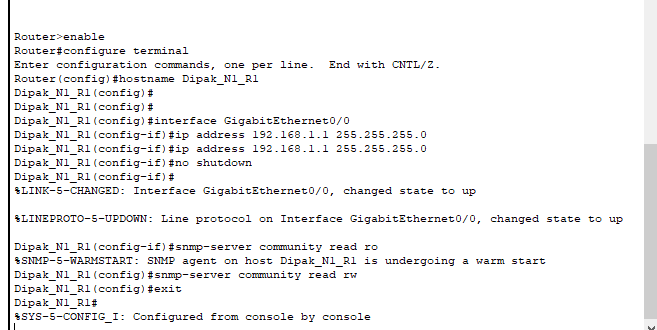


Figure 67 SNMP router conf

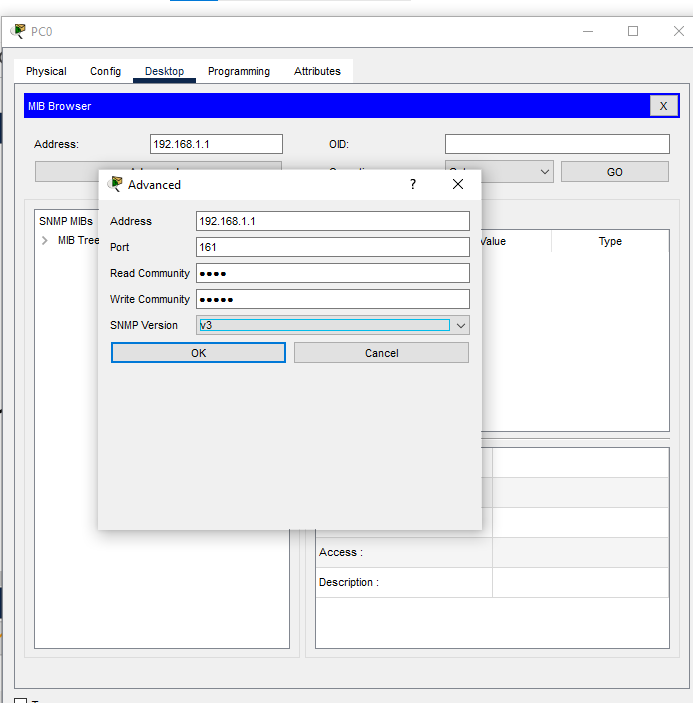


Figure 68 Setting SNMP

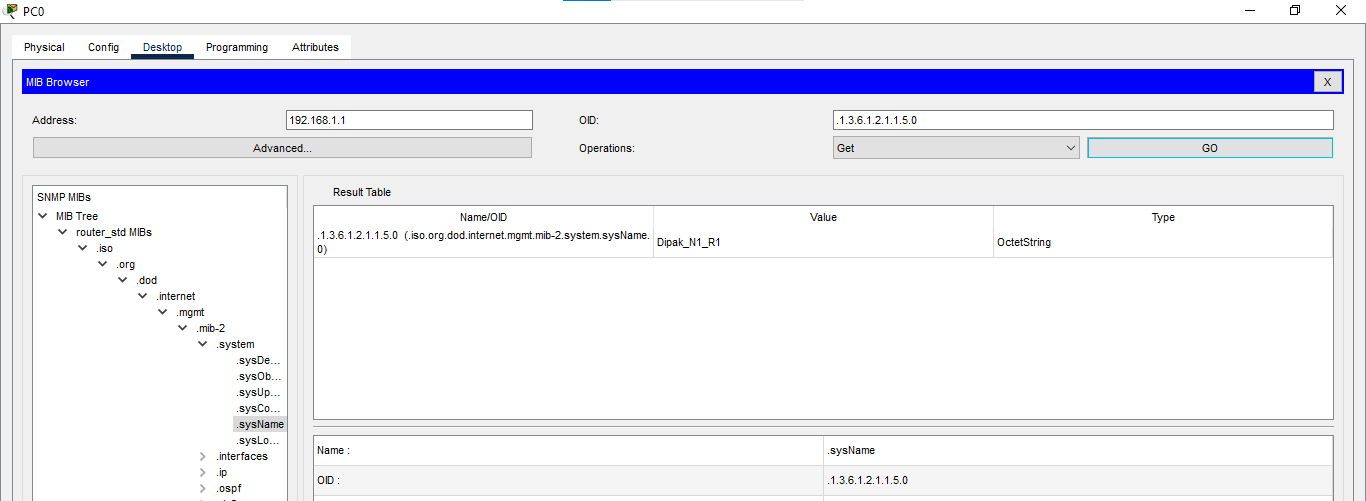


Figure 69 SNMP OUTPUT

# Lab of syslog and NTP

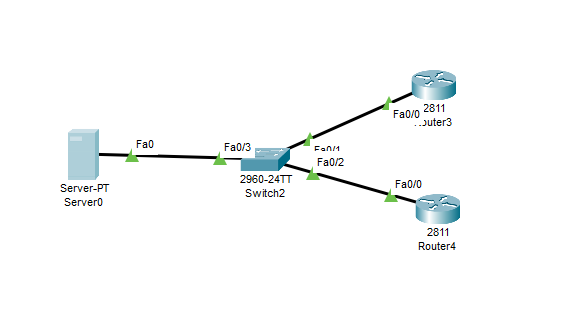


Figure 70 Syslog NTP design

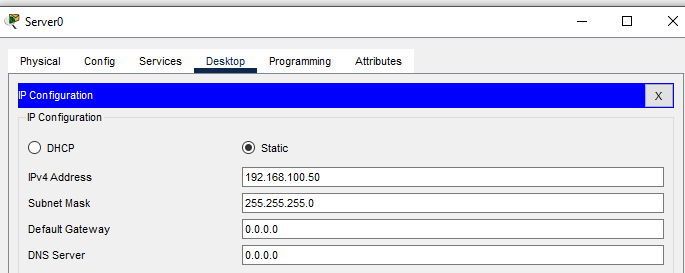


Figure 71 ADDING IP TO SERVER

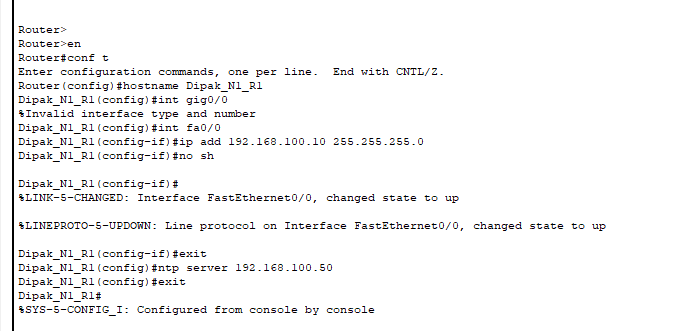


Figure 72 R1 configuration

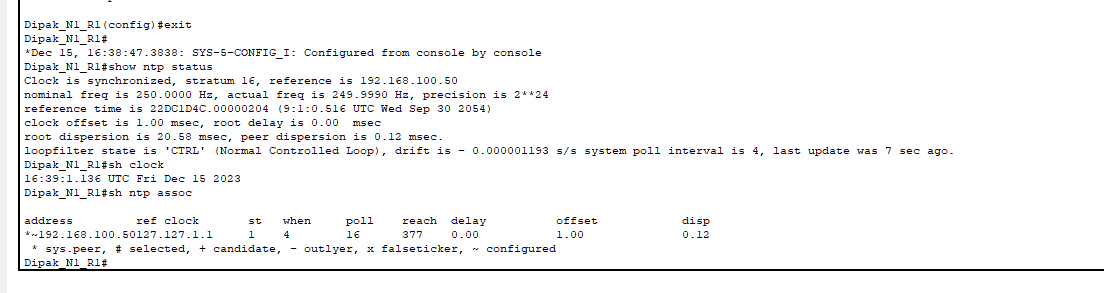


Figure 73 NTP status of R1

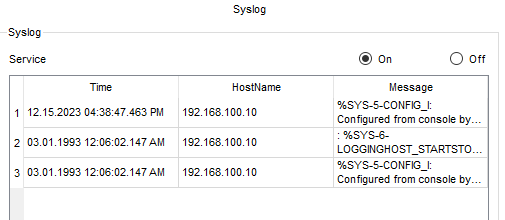


Figure 74 syslog msg For R1

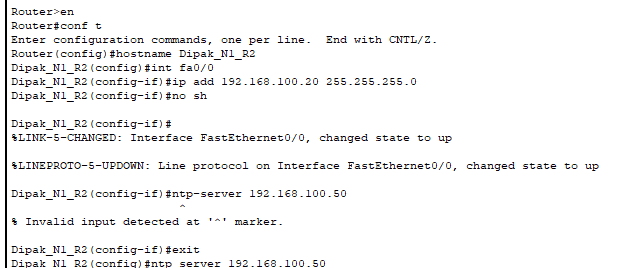


Figure 75 R2 configuration



Figure 76 r2 service timestamps

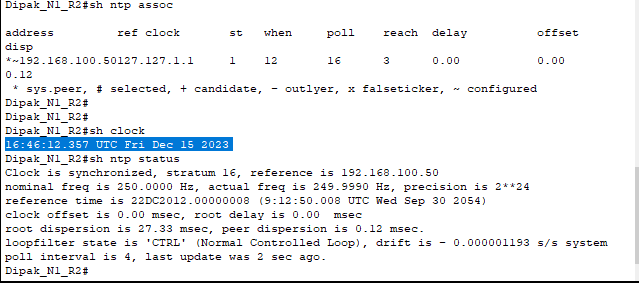


Figure 77 NTP status

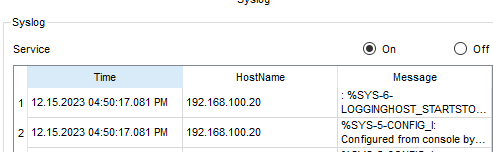
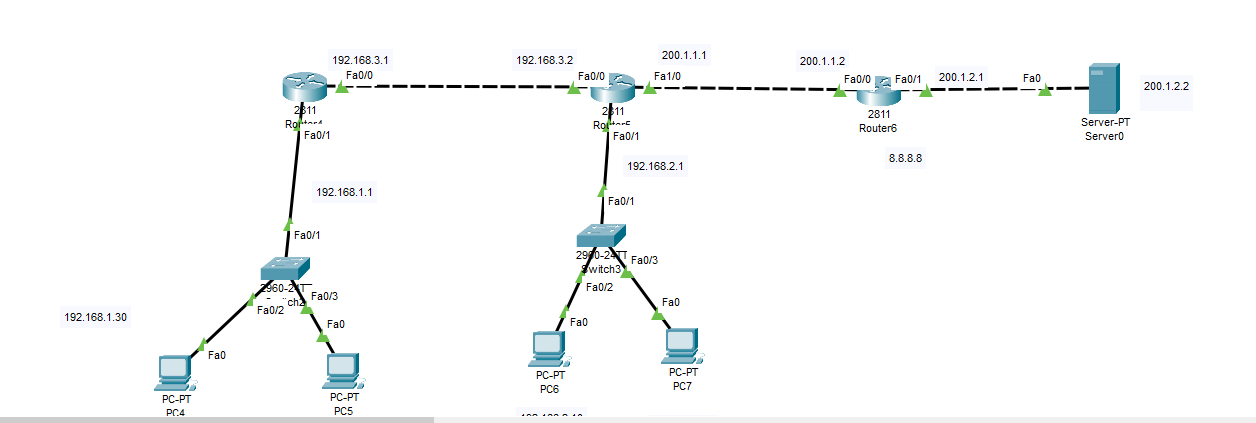


Figure 78 Syslog server message for R2



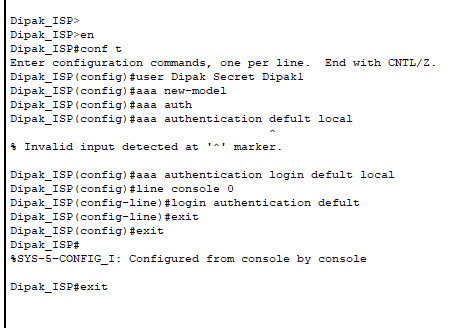


Figure 79 AAA configuration

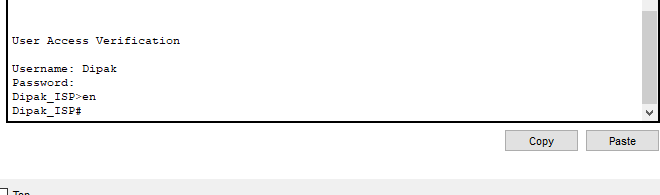


Figure 80 AAA output



Figure 81 Access-list configuration



Figure 82 NAT Configuration

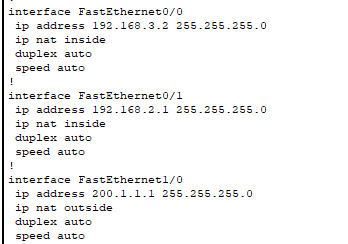


Figure 83 NAT Details

# Network troubleshooting

Network troubleshooting entails utilizing numerous procedures to find, separate, and solve problems disrupting the function of a network. Therefore, these methods are commonly used on various protocols in the network layer’s stack for efficient diagnosis. Let's explore troubleshooting methods and their application at different network layers, specifically for addressing potential networking issues at Landon College:

# Troubleshooting Methods:

* Identifying Symptoms: Collect information on reported problems like slow network connection, disconnection now and then, or application problem.
* Isolation: Find out if it is isolated to an individual device, segment, or involving the whole network.
* Gathering Information: Collect network performance, error and device status data using diagnostic tools, logs and network monitoring solutions.
* Testing and Validation: Conduct ping test, traceroute, and connectivity tests to pinpoint a possible failure point.
* Implementing Solutions: Fix or provide workaround for any identified issues that should be undertaken in a manner where these activities do not interfere with the normal functioning of the network.

# Troubleshooting Network at Different Layers:

# Physical Layer (Layer 1):

* Issues: Cable faults, defective connectors, and faulty equipment.
* Troubleshooting: Check or look at cable connections, check physical hardware, and do cable tester test in order to detect problems.

# Data Link Layer (Layer 2):

* Issues: Spanning tree protocol errors VLAN configuration problems as well as MAC address problems.
* Troubleshooting: Mac address verification, checking switch port configuration, and watching out for STP discrepancies.

# Network Layer (Layer 3):

* Issues: Causes of these problems may include incorrect IP addresses, routing issues, or Subnetting errors.
* Troubleshooting: Verify Subnetting, perform a thorough routing analysis, and check the basic IP configuration.

# Transport Layer (Layer 4):

* Issues: TCP/UDP communication problems, transport layer failures, and packet drops.
* Troubleshooting: Identify anomalies by analyzing transport protocol settings, checking for firewall rules, and performing packet captures.

# Application Layer (Layer 7):

* Issues: For instance, problems related to applications, DNS, and also protocols.
* Troubleshooting: test application connectivity, check DNS settings and inspect error-related items in application logs.

# Troubleshooting Landon College's Networking Issues:

* Symptom Identification: You may also get first hand student feedback on reported issues such as slow internet speed, sporadic WIFI in some parts of the campus, and trouble with various websites and other resources.
* Isolation: Find out whether problems affect particular locations, specified sets of equipment, or the whole infrastructure of the company’s operation system.
* Gathering Information: Gather information on Wi-Fi levels through network monitoring, bandwidth usage, speed, and other key network performance indicators.
* Testing and Validation: Carry out tests such as Wi-Fi signal tests, bandwidth tests, and connectivity tests toward identifying potential trouble spots.
* Implementing Solutions: Handle topics pertaining to a specific level of the network; for instance, fixing Wi-Fi issues by changing the position of access points or dealing with bandwidth problems by modifying network settings.

Landon college should use systematic troubleshooting techniques at different network layers in order to pinpoint the numerous networking issues that it faces and help resolve them while maintaining a steady and dependable network backbone capable of serving students, faculty and staff.