Tshwane University of Technology

We empower people

FACULTY
OF
INFORMATION
AND
COMMUNICATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

REQUIREMENTS DOCUMENT

COURSE: **N.DIP IT** COMMUNICATOIN NETWORKS
SUBJECT CODE: IDC30BC
PROJECT NAME: **Perfomance optimization for Gijima Technology people**

SUBMISSION DATE: 19/10/2023
PROJECT CO-ORDINATOR: MR. Z. MAPUNDU
Year 2023 2nd Semester: Final Evaluation: 28 February 2024

STUDENT DETAILS:

SURNAME & INITIALS: Mothapo H.I
SURNAME & INITIALS:

STUDENT NUMBER: 213243233
STUDENT NUMBER:

EMAIL ADDRESS: Ozzy50473@gmail.com
EMAIL ADDRESS:

CONTACT NUMBERS:072 249 2860
CONTACT NUMBERS:

TABLE OF CONTENTS

Introduction

Our project aims to identify the network challenges we are experiencing and to propose a better solution to Gauteng Department of Education infrastructure. Its going to provide less network downtime by providing redundant links and load balancing throughout the network this will help to avoid single point failure.

It is going to provide extensive security to avoid hackers or attackers, undesired network traffic which will be monitored by implementing ACLs (access lists) to prevent suspicious traffic which comes in form of IP packets to try to bridge into our network. We are going to implement most of technologies which is used in our enterprise to show the experience we have gained so far. We are also going to use Cisco packet tracer to demonstrate our project.

Project Purpose

In this project I will be introducing redundancy by adding links that will be for alternatives routes for traffic passing from ISP, to routers, core switches and access switches. We are also going to add data recovery site for data backup. Infrastructures are essential for keeping businesses function properly. If it has the capacity to prevent outages and failures; or if an infrastructure is able to operate its most important functions without interruptions or problems, an enterprise can achieve continuity.

Once this is achieved, problems related to data loss and downtimes, among others, will trickle down. Moreover, with high availability, it will be easy to avoid customer service-related problems and the negative publicity that stems from these. Also, employees will become more productive.

Every time there is downtime, an enterprise is poised to lose productivity, which, of course, affects its revenue-making capabilities. If the downtime is lower than 30 seconds, the impact can be quite small. But, if this length of time increases, the effect will also grow. Ultimately, it will create a negative impact on the enterprise. With a good high availability solution, this can be avoided.

- ACL
    - Will also be configured to block certain users from accessing certain servers. They will give permission slips indicating that a user needs to open a particular network device, file or other information.

- IPsec
    - Is a group of protocols that are used together to set up encrypted connections between devices. It helps keeps data sent over public network secure.

- Frame-relay
    - Is a standardized wide area network technology that specifies the physical and data link layers of digital telecommunications channels using packet switching metrology. Frame relay sends information in packets called frames through a shared Frame-Relay network.
- LAN connectivity and Port security
    - On the local area networks, we will also be introducing BPDU guard on the ports as a way to enhance security on the switches. Failover will be implemented on routers by configuring HSRP (Hot Standby Router Protocol). We also going to have redundancy links from our core switches to our access layer switches.
- We going have two links from each server to access switches, we will
    - Configure DHCP to assign IP addresses to end users automatically
    - Configure access points for wireless access
- Implementation of SSH
    - Configure SSH for network services to operate securely over an unsecured network.
- Implementing VLANs
    - I will also create VLANs as a form to separate the networks; this will help improve the security on the network (by reducing broadcast traffic). We will have different VLANs on all sites. On the router I will configure Router-on-stick command so that the VLANs would be able to communicate with each other.
- DHCP Snooping
    - feature performs the following activities: Validates **DHCP** messages received from untrusted sources and filters out invalid messages.

Network security will protects our company data, to businesses and individuals, data is something to be treasured and protected. If you're a business, your data might consist of marketing materials, financial data, and everything else that makes your business what it is. For individuals, you also have financial data and personal information you don't want anyone else to access.

Network security ensures your data stays yours. It also protects client data Governments and businesses store data that isn't theirs. For organizations like accounting firms and fiancés that data is very sensitive. Keeping that data secure is the responsibility of the organization. This includes backing up the data properly and ensuring hackers can't get into your system.

When Yahoo had a breach that affected its 3 billion customers, the direct costs ended up costing them around $350 million. On an individual level, attacks can leave you with a drained bank account. There's also the emotional distress of having your information stolen or sold. While good network security may cost you upfront, it more than pays for itself.

Project Scope

SonicWall's SSL VPN NetExtender

allows you to provide easy and secure access to Windows and Linux users. This transparent software enables remote users to securely connect and run any application on the company network. Users can upload and download files, mount network drives, and access resources as if they were on the local network. It is a traditional client-based VPN that can be configured either as an IPsec or SSL end-point agent.

Mobile Connect

Increasing mobile security threats pose a danger to your business. Protect corporate data and resources, while providing easy mobile access to your employees on iOS, macOS, Android, and Chrome OS devices.

This advanced thin client is both easy to use and highly configurable, allowing IT administrators to establish granular policies based on context (i.e. user, devices-in-use, and target application). Mobile Connect works in tandem with SonicWall firewall and SMA series.

The SonicWALL SSL VPN supports many common enterprise authentication methods, including two-factor authentication and one-time passwords. It also supports single-sign on capabilities. The SonicWALL SSL VPN comes with network access control features, which ensure that devices connecting to the network are safe.

Its an expensive security implementation, it needs latest and performance (CPU) .Routing is a little bit over-complicated and has different licenses which need to be renewed.

Definitions, Acronyms, and Abbreviations

VLAN- (*virtual local area network*) the technology used for security and access control, by separating traffic and blocking access or giving access to a certain group.

IPsec- (*internet protocol security*) encrypting data before transmission.

SSH- (*Secure Shell*) provides alternatives options for strong authentication.

ACL- (*access control list*) provide security for a network by permitting and denying.

Port security- secure network by preventing unknown devices from forwarding packets.

DHCP- (*dynamic host configuration protocol*) protocol for deploying IP address related configuration information to network devices.

DHCP snooping

Is a series of techniques applied to improve the security of a DHCP infrastructure.

HRSP- () is a First Hop Redundancy Protocol (FHRP) designed to allow for transparent failover of the first-hop IP device. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on networks configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active device and a standby device.

OSPF- (*open shortest path first*) is a routing protocol that determines shortest path during communication of network devices and used to advertise network to another networks.

VTP- (*vlan trunk protocol)* is protocol created by cisco that propagates the definition of VLAN on whole local area network.

Router - 2811 cisco router, a router is a device that forwards data packets along networks and is located at gateways, the places where two or more networks connect, and are the critical device that keeps data flowing between networks and keeps the networks connected to the Internet.

Switch - Cisco Catalyst 2960 Series Switches layer 2, a switch is a device that is used at the Access or OSI Layer. A switch can be used to connect multiple hosts (PCs) to the network. A switch sends a message to another host on the same network or same switch, the switch receives and decodes the frames to read the physical (MAC) address portion of the message.

Cables, Is used to connect one network device to other network devices or to connect two

or more computers to share printer, PCs etc. category 6 cabling have fewer errors for current applications. This means fewer re-transmissions of lost or corrupted data packets under certain conditions, which translates into higher reliability for category 6 networks compared to category 5e networks.
Fiber optic, cross over, straight through and RJ45

Dell server - is a computer in a LAN that is dedicated to database storage and retrieval of data.

Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols

Firewall – A sonic Firewall is a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

VPN (virtual private network**)** – is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Patch panel - Patch panels' offer the convenience of allowing technicians to quickly change the path of select signals, without the expense of dedicated switching equipment. Is a panel that contains multiple cable connections, the back of the panel has wiring or other connective cabling that runs to disparate equipment. The front of the patch panel allows easy access to connect the different equipment through the use of short patch cables.

IDPS - is used to detect and prevent who try to access our data on the network or any information that is not belonging to the network by telling the administrator with a notification.

Dell PC - Consists of two or more computing devices connected by a medium allowing the exchange of electronic information.

A PBX (private branch exchange) is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines.

Rapid STP Is a network protocol that ensures a loop-free topology for Ethernet networks.

Dynamic Routing protocol
Is a networking technique that provides optimal data routing.
VOIP telephone on LAN
Is a term used to describe technologies that use a variety of protocols to exchange voice, fax, and other forms of information, traditionally carried over the Public Switched Telephone Network (PSTN).

DHCP sever
A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.
DHCP snooping
is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers.

VPN IPsec
Is a popular set of protocols used to ensure secure and private communications over Internet Protocol (IP) networks, which is achieved by the authentication and encryption of IP packets between two endpoints.

ACLs
Is a collection of permit and deny conditions, called rules that provide security by blocking unauthorized users and allowing authorized users to access specific resources.

NAT
Network address translation is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device

IPS - intrusion prevention system

OSPF - Open Shortest Path First
a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS).
SMTP, IMAP
Is part of the application layer of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks.
SSH - Secure Shell
a cryptographic network protocol for operating network services securely over an unsecured network
SNMP – Simple Network management Protocol
Is a way for different devices on a network to share information with one another.
Frame Relay
Is a standardized wide area network technology that specifies the physical and data link layer of the digital telecommunications channel using a packet switching methodology.
NAT
A method of mapping an IP address space into another by modifying network address information in the IP header of the packets while they are in transit across a trafiic routing device

Performance Requirements

Bandwidth commonly measured in bits/second is the maximum rate that information can be transferred-Our enterprise consist of about 13 floors which have plus minus 500 workers including interns.so there for the is a high demand for bandwidth and throughput

Throughput is the rate of successful message delivery over a communication channel.

Latency the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses.IT team use a BMC software to communicate with all other works so than can rich them and also help them with IT related problems so Speed is important.

Error rate the number of corrupted bits expressed as a percentage or fraction of the total sent

- **Cisco Routers 2811**
    - Simplified operations and deployment of virtual network services on any platform
    - Multi-core processing increases network services performance and availability
    - Simplify network management, deploy networks in minutes, and predict problems before they happen
    - Cloud-delivered, secure, flexible and rich services architecture that delivers the best user experience over any connection.
- **Cisco Catalyst 2960-S switches**
    - 1G Small Form-Factor Pluggable (SFP)
    - Cisco Flex Stack stacking with 20 Gbps of stack throughput (optional)
    - IEEE 802.3at-compliant PoE+ for up to 30W of power per port
    - Up to 740W of combined PoE/PoE+ budge
    - 48 Gigabit Ethernet ports
    - USB interfaces for management and file transfers
    - LAN Base or LAN Lite Cisco IOS® Software feature set
    - Smart Operations tools that simplify deployment and reduce the cost of network administration

- An enhanced limited lifetime hardware warranty (E-LLW), providing next-business-day replacement

- **Cisco Server 2012 R2**
  - Network Adapter requirements
  - An Ethernet adapter capable of at least gigabit throughput

Design Constraints

Application limitation-the applications currently used by the company can have a significant impact on a network design project like using the old operating system, the network design will have to include it.

Personnel limitation-In a case where the company have sufficient staff to allocate to a project, it is possible that the members do not have technical expertise required to implement or manage the network therefore additional training or hiring of new members will be required.

Bandwidth or media limitation-it is conceivable that certain parts of the network cannot be changed such as wireless access point therefore that must be circumvented

Existing equipment-the company may have the existing equipment that meets their needs and do not prefer to replace them but to reuse them.

Network Design, Network Cabling and Network Links

*The network will be making use of **RIP** (routing information protocol)*It's a standardized protocol that is vlsm compliant and also provide fast convergence)

Firewall - network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In our case ***ACLs*** will be configured on the interfaces to limit or block unauthorized users from accessing servers.

Technology: cisco ASA

Wireless router – This device will allow all our users to be able to connect using their personal devices and be able to move around while they are connected.

Technology: cisco

Cables are used to connect one network device to other network devices or to connect two or more computers to share printer, PCs etc. category 6 cabling have fewer errors for current applications. This means fewer re-transmissions of lost or corrupted data packets under certain conditions, which translates into higher reliability for category 6 networks compared to category 5e networks.
Fiber optic, cross over, straight through and RJ45
straight through and cross over- will be used for connecting all the devices on the network.
Fiber optic, straight through, cross-over and serial cables

Switch – it is a device that allows for the interconnections of devise in order to share data.

Server – is a computer system, which is used as the central repository of data and various programs that are shared by users in a network.

Technology: Dell

Firewall - network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Technology: cisco ASA

Wireless router – This device will allow Students to be able to connect using their personal devices and be able to move around while they are connected.

Technology: cisco

Cables (straight through and cross over) - will be used for connecting all the devices on the network.

Technology: Cisco

IP address planning.

Switch – it is a device that allows for the interconnections of devise in order to share data.

Technology: Cisco

Fiber optic, straight through, cross-over and serial cables

Server – is a computer system, which is used as the central repository of data and various programs that are shared by users in a network.

Technology: Dell

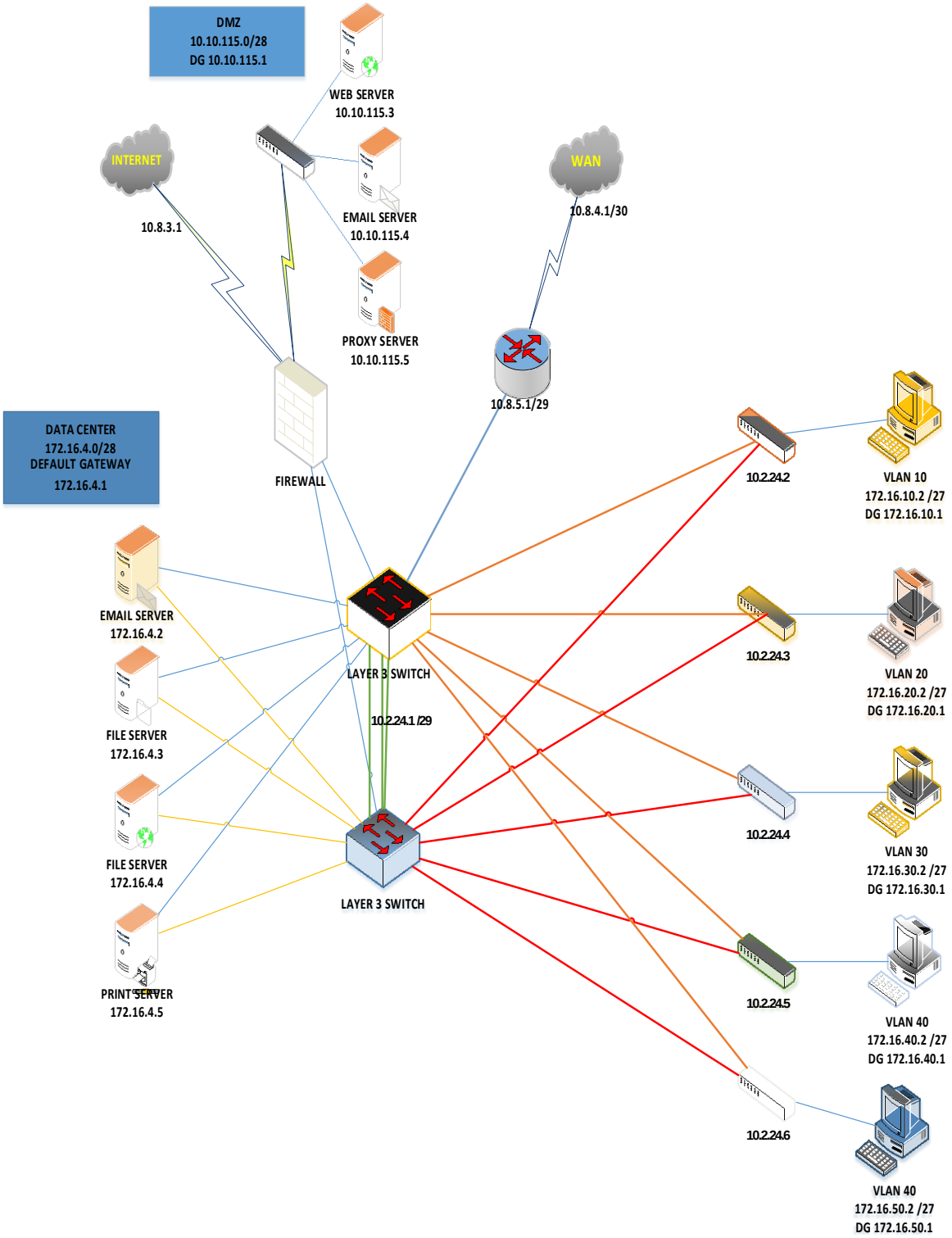
Johannesburg office

Name	Hosts Needed	Hosts Available	Network Address	Mask	Usable Range	Broadcast
Data Center VLAN 10	5	6	172.16.10.0/29	255.255.255.248	172.16.10.1 - 172.16.10.6	172.16.10.7
IT VLAN 20	15	30	172.16.20.0/27	255.255.255.224	172.16.20.1 - 172.16.20.30	172.16.20.31
HR VLAN 30	10	14	172.16.30.0/28	255.255.255.240	172.16.30.1 - 172.16.30.14	172.16.30.15
MANAGEMENT VLAN 99	8	14	172.16.99.0/28	255.255.255.240	172.16.99.1 - 172.16.99.14	172.16.99.15
VOICE VLAN 40	10	14	172.16.40.0/28	255.255.255.240	172.16.40.1 - 172.16.40.14	172.16.40.15
Routers Active/Standby WAN	8	14	192.168.25.0/28	255.255.255.240	192.168.25.1 - 192.168.25.14	192.168.25.15

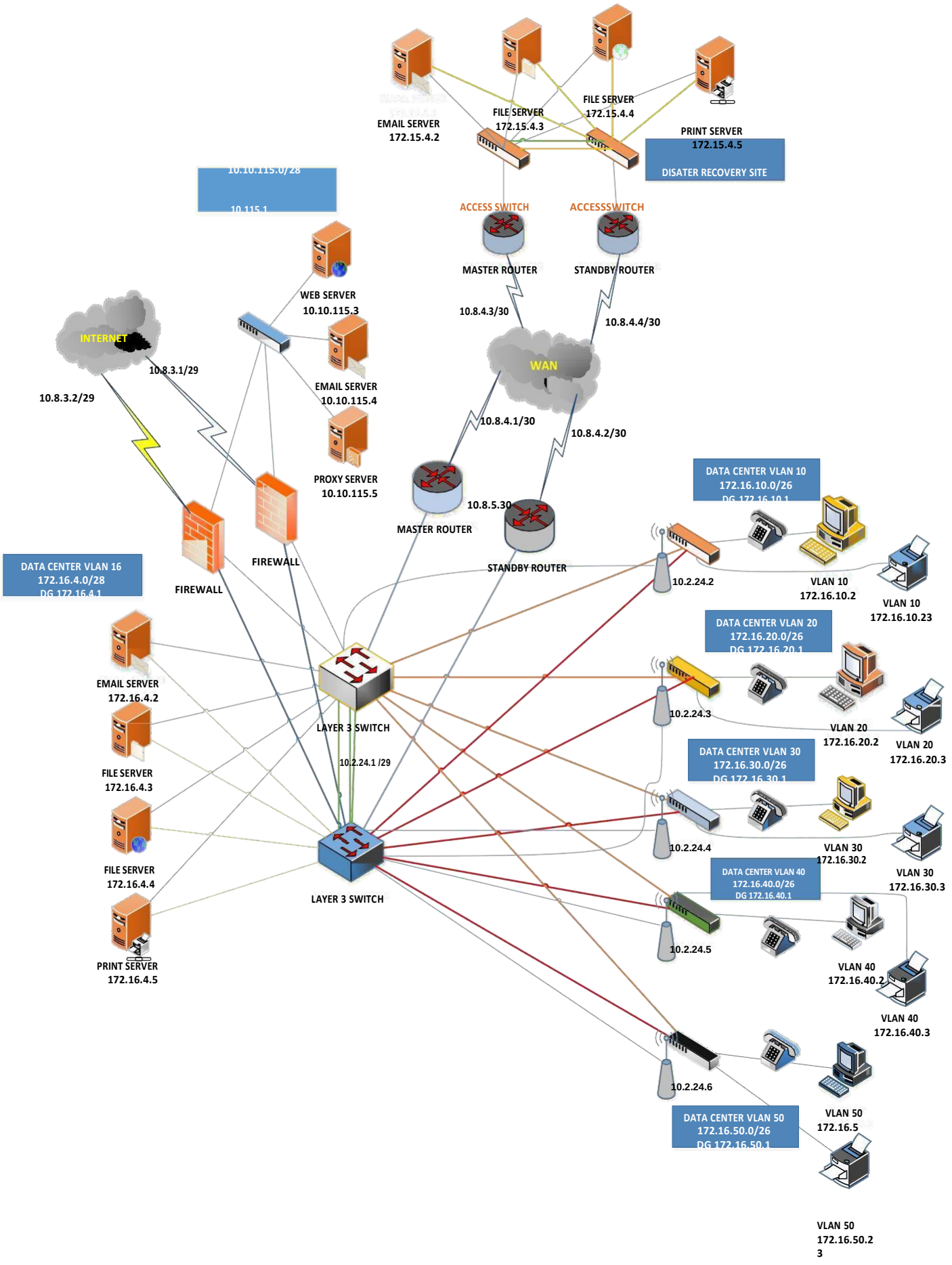
Disaster Recovery

Name	Hosts Needed	Hosts Available	Network Address	Mask	Usable Range	Broadcast
Disaster Recovery VLAN 50	10	14	172.16.50.0/20	255.255.255.240	172.16.50.1 - 172.16.50.14	172.16.50.15

Current or Existing Network Diagram



New or Proposed Network Diagram


EMAIL SERVER
172.15.4.2
FILE SERVER
172.15.4.3
FILE SERVER
172.15.4.4
PRINT SERVER
172.15.4.5
DISATER RECOVERY SITE
10.10.115.0/28
10.115.1
ACCESS SWITCH
ACCESSSWITCH
MASTER ROUTER
STANDBY ROUTER
WEB SERVER
10.10.115.3
10.8.4.3/30
10.8.4.4/30
INTERNET
10.8.3.1/29
10.8.3.2/29
EMAIL SERVER
10.10.115.4
WAN
PROXY SERVER
10.10.115.5
10.8.4.1/30
10.8.4.2/30
MASTER ROUTER
10.8.5.30
STANDBY ROUTER
DATA CENTER VLAN 10
172.16.10.0/26
DG 172.16.10.1
DATA CENTER VLAN 16
172.16.4.0/28
DG 172.16.4.1
FIREWALL
FIREWALL
10.2.24.2
VLAN 10
172.16.10.2
VLAN 10
172.16.10.23
DATA CENTER VLAN 20
172.16.20.0/26
DG 172.16.20.1
EMAIL SERVER
172.16.4.2
LAYER 3 SWITCH
10.2.24.3
VLAN 20
172.16.20.2
VLAN 20
172.16.20.3
DATA CENTER VLAN 30
172.16.30.0/26
DG 172.16.30.1
FILE SERVER
172.16.4.3
10.2.24.1 /29
10.2.24.4
VLAN 30
172.16.30.2
VLAN 30
172.16.30.3
FILE SERVER
172.16.4.4
LAYER 3 SWITCH
DATA CENTER VLAN 40
172.16.40.0/26
DG 172.16.40.1
PRINT SERVER
172.16.4.5
10.2.24.5
VLAN 40
172.16.40.2
VLAN 40
172.16.40.3
10.2.24.6
DATA CENTER VLAN 50
172.16.50.0/26
DG 172.16.50.1
VLAN 50
172.16.5
VLAN 50
172.16.50.2
3

Proposed Solution (Security Implementation Approach and Tools Used)

- **ACL**
  - Access List control will be configured on the interfaces to limit or block unauthorized users from accessing servers.
- **VLANs**
  - We will also create as a form to separate networks; this will help improve the security on the network. As we have multiple departments with different task to perform. On the router we configure router on stick so that Vlans would be able to communicate.

- **IPsec**
  - When a packet arrives at the outbound interface of the router and if it is sent down the tunnel, it is first encapsulated using GRE (Generic Routing Encapsulation) and then encrypted with IPsec. In other words, any traffic permitted to enter the GRE Tunnel is also encrypted by IPsec. The reason we will be implementing IPsec it's because we need to make sure that the data that is passing through the tunnel is secured as GRE does not provide security.

- **DMZ**
  - A perimeter network that protects the organization's LAN from untrusted traffic. Servers that provide data to public are located in the buffer zone so they will be an extra layer of security.

- **NAT**
  - A method of mapping an IP address space into another by modifying network address information in the IP header of the packets while they are in transit across a trafiic routing device
  - Our NAT device function as the default gateway for the internal host which is typically aware of the true IP address and the TCP/UDP port of the external host while external host are only aware of the public IP address .

- **SSH**
  - Secure Shell is a network communication protocol that enables two computers to communicate (http or hypertext transfer protocol, which is the protocol **used to** transfer hypertext such as web pages) and share data.

- **DHCP snooping**
  - feature performs the following activities: Validates DHCP messages received from untrusted sources and filters out invalid messages.

All in all we have introduced the VLANs to force appropriate security measures and implementation of Secure Shell to facilitates a secure communication over an unsecured network, Access Control Lists for permissions basically to permit and deny the traffic entering/leaving the network, and made use of a console password and IPsec to ensure integrity, confidentiality and authentication of data. On WIFI I implemented WPA encryption. ***This approach will protect and prevent unauthorized users from accessing the network.***

Proposed Solution (Network and System Redundancy Approach)

Below is list of network redundancy approach

Redundant system ensures continuity and avoids disruption of critical communication and data flow. Network redundancy works by creating multiple data paths within a network, between any and all locations. If a cable, switch, or router suddenly fails, another pathway will be available to maintain the communication flow.

On the Network System and redundancy, I have introduced:

- **Replication** –Having more than one copy of resources to enhance the reliability of the system. The network consists of two core router whereby the second router is a standby to avoid downtime in case of any failure on the core router.

  This is achieved by implementing **HSRP *(Hot Standby Routing Protocol)*** which is a First Hop Redundancy Protocol (FHRP) designed to allow for transparent failover of the first-hop IP device. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on networks configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active device and a standby device.

  The core switches address redundancy for fault tolerance by having redundancy of physical links whereby three link are active and one link is not active, for which it is used for back up purposes in case of a link failure

- **Disaster Recovery site** (DR) is a **facility** an organization can use to **recover** and **restore** its technology infrastructure and operations when its primary data center becomes unavailable

- **EtherChannel** is a port link aggregation technology or port-channel architecture used primarily on **Cisco** switches. It allows grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers.

  - This Means I am ***introducing redundancy*** by adding EtherChannel links between the core switches, which they will act as one logical Ethernet link for the purpose of providing fault tolerance and high-speed links between switches.
  - I will also be adding ***virtual router redundancy protocol*** where this will increase the availability and reliability of routing paths via automatic default gateway selections on the router with high priority.

- I will also implement ***frame relay*** so that the branches will also be able to communicate as we have an organization that has branches that need to be connected from different geographical places.
- I will also implement ***disaster recovery site*** which have our backup servers in case the current severs in the main brunch fails.

Proposed Solution (Configuration Steps) or Screen Dumb

//configurations on CORE_SWITCH1

CORE_SWITCH1

//configuring vtp server mode on the switches so that the vlans maybe configured on the access switches to save time

```
vtp mode server
vtp domain niselagroupholding.co.za
vtp password admin
```

//Assigning trunk ports on the interfaces

```
interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport mode trunk

interface FastEthernet0/5
 switchport mode trunk

interface FastEthernet0/6
 switchport mode trunk

interface FastEthernet0/7
 switchport mode trunk

interface FastEthernet0/8
 switchport mode trunk
```

//creating VLANS

```
vlan 10
```

```
name DATA_CENTER

vlan 20
name IT

vlan 30
name HR

vlan 40
name Management

vlan 60
name VOICE

//Assigning Access ports on the interfaces

interface FastEthernet0/13
 switchport access vlan 20

interface FastEthernet0/14
 switchport access vlan 20

interface FastEthernet0/15
 switchport access vlan 20

interface FastEthernet0/16
 switchport access vlan 20

interface FastEthernet0/17
 switchport access vlan 30

interface FastEthernet0/18
 switchport access vlan 30

interface FastEthernet0/19
 switchport access vlan 30

interface FastEthernet0/20
 switchport access vlan 30

interface FastEthernet0/21
 switchport access vlan 40

interface FastEthernet0/22
 switchport access vlan 40

interface FastEthernet0/23
 switchport access vlan 40

interface FastEthernet0/24
 switchport access vlan 40
exit
```

```
interface Vlan1
 no ip address
 shutdown
exit

line con 0
line vty 0 4
 login
line vty 5 15
 login
end

//configurations on CORE_SWITCH2

hostname CORE_SWITCH2

//configuring vtp server mode on the switches so that the vlans maybe configured on the access switches to save time

vtp mode server
vtp domain niselagroupholding.co.za
vtp password admin

//Assigning trunk ports on the interfaces

interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport mode trunk

interface FastEthernet0/5
 switchport mode trunk

interface FastEthernet0/6
 switchport mode trunk

interface FastEthernet0/7
 switchport mode trunk

interface FastEthernet0/8
 switchport mode trunk

//creating VLANS

vlan 10
name DATA_CENTER
```

```
vlan 20
name IT

vlan 30
name HR

vlan 40
name Management

vlan 60
name VOICE


//Assigning Access ports on the interfaces

interface FastEthernet0/13
 switchport access vlan 20

interface FastEthernet0/14
 switchport access vlan 20

interface FastEthernet0/15
 switchport access vlan 20

interface FastEthernet0/16
 switchport access vlan 20

interface FastEthernet0/17
 switchport access vlan 30

interface FastEthernet0/18
 switchport access vlan 30

interface FastEthernet0/19
 switchport access vlan 30

interface FastEthernet0/20
 switchport access vlan 30

interface FastEthernet0/21
 switchport access vlan 40

interface FastEthernet0/22
 switchport access vlan 40

interface FastEthernet0/23
 switchport access vlan 40

interface FastEthernet0/24
 switchport access vlan 40

line con 0
```

```
line vty 0 4
 login
line vty 5 15
 login
end

//configurations on DATA_SWITCH1 on VLAN 10

hostname DATA_SWITCH1

vtp mode client
vtp domain niselagroupholding.co.za
vtp password admin

//Assigning trunk ports on the interfaces

interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport mode trunk

interface FastEthernet0/5
 switchport mode trunk

interface FastEthernet0/6
 switchport mode trunk

interface FastEthernet0/7
 switchport mode trunk

interface FastEthernet0/8
 switchport mode trunk

//Assigning Access ports on the interfaces and configuring port security

interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000C.CF3C.81AB

interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
```

```
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00D0.D3E4.2988

interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000D.BDB3.740D

interface GigabitEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky

interface GigabitEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky

line con 0
line vty 0 4
 login
line vty 5 15
 login
end

//configuring dhcp snooping

ip dhcp snooping

ip dhcp snooping vlan 10-60

interface ra FastEthernet0/1-2

ip dhcp snooping trust

//configurations on DATA_SWITCH2 on VLAN 10

hostname DATA_SWITCH2

vtp mode client
vtp domain niselagroupholding.co.za
vtp password admin

//Assigning trunk ports on the interfaces
```

```
interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport mode trunk

interface FastEthernet0/5
 switchport mode trunk

interface FastEthernet0/6
 switchport mode trunk

interface FastEthernet0/7
 switchport mode trunk

interface FastEthernet0/8
 switchport mode trunk

//Assigning Access ports on the interfaces and configuring port security

interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000C.CF3C.81AB

interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00D0.D3E4.2988

interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000D.BDB3.740D

interface GigabitEthernet0/1
 switchport access vlan 10
 switchport mode access
```

```
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0003.E4CB.7085

interface GigabitEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky

line con 0
line vty 0 4
 login
line vty 5 15
 login
end

//configuring dhcp snooping

ip dhcp snooping

ip dhcp snooping vlan 10-60

interface ra FastEthernet0/1-2

ip dhcp snooping trust


//configurations on ACCESS_SWITCH1 on VLAN 20

hostname ACCESS_SWITCH1

vtp mode client
vtp domain niselagroupholding.co.za
vtp password admin

//Assigning trunk ports on the interfaces

interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport mode trunk

interface FastEthernet0/5
 switchport mode trunk
```

```
interface FastEthernet0/6
 switchport mode trunk

interface FastEthernet0/7
 switchport mode trunk

interface FastEthernet0/8
 switchport mode trunk

//Assigning Access & Voice ports on the interfaces and configuring port security

interface FastEthernet0/12
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00E0.F900.7D65

interface FastEthernet0/13
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.5CC7.E020

interface FastEthernet0/14
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0000.0C0A.D58B
 switchport port-security mac-address sticky 00D0.5886.B6DA

interface FastEthernet0/15
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.C95B.74B9

line con 0
line vty 0 4
 login
line vty 5 15
```

```
 login
end

//configuring dhcp snooping

ip dhcp snooping

ip dhcp snooping vlan 10-60

interface ra FastEthernet0/1-2

ip dhcp snooping trust


//configurations on ACCESS_SWITCH2 on VLAN 30

hostname ACCESS_SWITCH2

vtp mode client
vtp domain niselagroupholding.co.za
vtp password admin

//Assigning trunk ports on the interfaces

interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport mode trunk

interface FastEthernet0/5
 switchport mode trunk

interface FastEthernet0/6
 switchport mode trunk

interface FastEthernet0/7
 switchport mode trunk

interface FastEthernet0/8
 switchport mode trunk

//Assigning Access & Voice ports on the interfaces and configuring port security

interface FastEthernet0/16
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 60
```

```
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky

interface FastEthernet0/17
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0030.F29D.2C2B
 switchport port-security mac-address sticky 0090.2B33.3753

interface FastEthernet0/18
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000A.F352.5CE4

interface FastEthernet0/19
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.4721.43C5

interface FastEthernet0/20
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky

line con 0
line vty 0 4
 login
line vty 5 15
 login
end

//configuring dhcp snooping

ip dhcp snooping

ip dhcp snooping vlan 10-60
```

```
interface ra FastEthernet0/1-2

ip dhcp snooping trust


//configurations on ACCESS_SWITCH3 on VLAN 40

hostname ACCESS_SWITCH3

vtp mode client
vtp domain niselagroupholding.co.za
vtp password admin

//Assigning trunk ports on the interfaces

interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport mode trunk

interface FastEthernet0/5
 switchport mode trunk

interface FastEthernet0/6
 switchport mode trunk

interface FastEthernet0/7
 switchport mode trunk

interface FastEthernet0/8
 switchport mode trunk

//Assigning Access & Voice ports on the interfaces and configuring port security

interface FastEthernet0/21
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0003.E417.519E

interface FastEthernet0/22
 switchport access vlan 40
 switchport mode access
```

```
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0005.5E7C.072D

interface FastEthernet0/23
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00D0.9747.1402

interface FastEthernet0/24
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 60
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.2F9E.4913

line con 0
line vty 0 4
 login
line vty 5 15
 login
end

//configuring dhcp snooping

ip dhcp snooping

ip dhcp snooping vlan 10-60

interface ra FastEthernet0/1-2

ip dhcp snooping trust


//configurations on DRS_SWITCH1 (Disaster Recovery)

hostname DRS_SWITCH1

spanning-tree mode pvst
spanning-tree extend system-id

//Assigning trunk ports on the interfaces

interface FastEthernet0/1
 switchport mode trunk
```

```
interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport mode trunk

//creating VLAN

vlan 50
name DRS

//Assigning Access ports on the interfaces

interface FastEthernet0/5
 switchport access vlan 50

interface FastEthernet0/6
 switchport access vlan 50

interface FastEthernet0/7
 switchport access vlan 50

interface FastEthernet0/8
 switchport access vlan 50

interface FastEthernet0/9
 switchport access vlan 50

interface FastEthernet0/10
 switchport access vlan 50

interface FastEthernet0/11
 switchport access vlan 50

interface FastEthernet0/12
 switchport access vlan 50

interface FastEthernet0/13
 switchport access vlan 50

interface FastEthernet0/14
 switchport access vlan 50

interface FastEthernet0/15
 switchport access vlan 50

line con 0

line vty 0 4
 login
```

```
line vty 5 15
 login
end
```

//configuring dhcp snooping

```
ip dhcp snooping

ip dhcp snooping vlan 10-60

interface ra FastEthernet0/1-2

ip dhcp snooping trust
```

//configurations on DRS_SWITCH2 (Disaster Recovery)

```
hostname DRS_SWITCH2

spanning-tree mode pvst
spanning-tree extend system-id
```

//Assigning trunk ports on the interfaces

```
interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport mode trunk
```

//creating VLAN

```
vlan 50
name DRS
```

//Assigning Access ports on the interfaces

```
interface FastEthernet0/5
 switchport access vlan 50

interface FastEthernet0/6
 switchport access vlan 50

interface FastEthernet0/7
 switchport access vlan 50

interface FastEthernet0/8
```

```
 switchport access vlan 50

interface FastEthernet0/9
 switchport access vlan 50

interface FastEthernet0/10
 switchport access vlan 50

interface FastEthernet0/11
 switchport access vlan 50

interface FastEthernet0/12
 switchport access vlan 50

interface FastEthernet0/13
 switchport access vlan 50

interface FastEthernet0/14
 switchport access vlan 50

interface FastEthernet0/15
 switchport access vlan 50

line con 0
line vty 0 4
 login
line vty 5 15
 login
end

//configuring dhcp snooping

ip dhcp snooping

ip dhcp snooping vlan 10-60

interface ra FastEthernet0/1-2

ip dhcp snooping trust


//configuring the ACTIVE_ROUTER

hostname ACTIVE_ROUTER

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1

// excluding ip addresses to be used as static before creating dhcp pools

ip dhcp excluded-address 172.16.40.1 172.16.40.5
ip dhcp excluded-address 172.16.30.1 172.16.30.5
ip dhcp excluded-address 172.16.20.1 172.16.20.5

// creating dhcp pools for 3 departments
```

```
ip dhcp pool management
 network 172.16.40.0 255.255.255.240
 default-router 172.16.40.1
 dns-server 172.16.10.2

ip dhcp pool HR
 network 172.16.30.0 255.255.255.240
 default-router 172.16.30.1
 dns-server 172.16.10.2

ip dhcp pool IT
 network 172.16.20.0 255.255.255.224
 default-router 172.16.20.1
 dns-server 172.16.10.2

ip dhcp pool VOICE
 network 172.16.60.0 255.255.255.240
 default-router 172.16.60.1
 option 150 ip 172.16.60.1
 dns-server 172.16.10.2

//configuring shh

username student password 0 cisco

license udi pid CISCO2811/K9 sn FTX10172V7A-

crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2

ip ssh authentication-retries 2
ip ssh time-out 15
ip domain-name niselagroupholding.co.za

spanning-tree mode pvst

ip ips config location ipsBranch retries 1

//configuring router on a stick and HSRP

interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.10.1 255.255.255.248
 standby 1 ip 172.16.10.1
 standby 1 priority 150
 standby 1 preempt
 standby 1 track Serial0/3/0

interface FastEthernet0/0.20
 encapsulation dot1Q 20
```

```
 ip address 172.16.20.1 255.255.255.224
 standby 1 ip 172.16.20.1
 standby 1 priority 150
 standby 1 preempt
 standby 1 track Serial0/3/0

interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.30.1 255.255.255.240
 standby 1 ip 172.16.30.1
 standby 1 priority 150
 standby 1 preempt
 standby 1 track Serial0/3/0

interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.40.1 255.255.255.240
 standby 1 ip 172.16.40.1
 standby 1 priority 150
 standby 1 preempt
 standby 1 track Serial0/3/0

interface FastEthernet0/0.60
 encapsulation dot1Q 60
 ip address 172.16.60.1 255.255.255.240

//confoguring frame relay and the public link ip address

interface Serial0/3/0
 ip address 192.168.10.1 255.255.255.248
 encapsulation frame-relay
 frame-relay map ip 192.168.10.2 102 broadcast
 frame-relay map ip 192.168.10.3 103 broadcast
 frame-relay map ip 192.168.10.4 104 broadcast
 frame-relay lmi-type ansi
 ip nat outside
 clock rate 72000



//configuring ospf

router ospf 1
 log-adjacency-changes
 network 172.16.10.0 0.0.0.7 area 0
 network 172.16.20.0 0.0.0.31 area 0
 network 172.16.30.0 0.0.0.15 area 0
 network 172.16.40.0 0.0.0.15 area 0
 network 172.16.50.0 0.0.0.15 area 0

//gonfiguring ip routes

ip classless
```

```
ip route 0.0.0.0 0.0.0.0 192.168.10.4
ip route 0.0.0.0 0.0.0.0 192.168.10.3
ip route 0.0.0.0 0.0.0.0 192.168.10.2

//configuring telephony service and directory number

telephony-service
 max-ephones 3
 max-dn 3
 ip source-address 172.16.60.1 port 2000
 auto assign 1 to 3

//configuring the phone extentions

ephone-dn 1
 number 111

ephone-dn 2
 number 222

ephone-dn 3
 number 333

//configuring ephone buttons

ephone 1
 device-security-mode none
 mac-address 0090.2B33.3753
 type 7960
 button 1:1

ephone 2
 device-security-mode none
 mac-address 000A.F352.5CE4
 type 7960
 button 1:2

ephone 3
 device-security-mode none
 mac-address 0003.E417.519E
 type 7960
 button 1:3

line con 0
 password cisco
 login

line aux 0
line vty 0 4
 password cisco
 login
 transport input ssh
end
```

```
//configuring the STANDBY_ROUTER

hostname STANDBY_ROUTER

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1

// excluding ip addresses to be used as static before creating dhcp pools

ip dhcp excluded-address 172.16.40.1 172.16.40.5
ip dhcp excluded-address 172.16.30.1 172.16.30.5
ip dhcp excluded-address 172.16.20.1 172.16.20.5

// creating dhcp pools for 3 departments

ip dhcp pool management
 network 172.16.40.0 255.255.255.240
 default-router 172.16.40.1
 dns-server 172.16.10.2

ip dhcp pool HR
 network 172.16.30.0 255.255.255.240
 default-router 172.16.30.1
 dns-server 172.16.10.2

ip dhcp pool IT
 network 172.16.20.0 255.255.255.224
 default-router 172.16.20.1
 dns-server 172.16.10.2

ip dhcp pool VOICE
 network 172.16.60.0 255.255.255.240
 default-router 172.16.60.1
 option 150 ip 172.16.60.1
 dns-server 172.16.10.2

//configuring shh

username student password 0 cisco

license udi pid CISCO2811/K9 sn FTX10172FXC-

crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2

ip ssh authentication-retries 2
ip ssh time-out 15
ip domain-name niselagroupholding.co.za

spanning-tree mode pvst
ip ips config location ipsBranch retries 1
```

```
//configuring router on a stick and HSRP

interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.10.1 255.255.255.248
 standby 1 ip 172.16.10.1
 standby 1 preempt
 standby 1 track Serial0/3/0

interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.20.1 255.255.255.224
 standby 1 ip 172.16.20.1
 standby 1 preempt
 standby 1 track Serial0/3/0

interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.30.1 255.255.255.240
 standby 1 ip 172.16.30.1
 standby 1 preempt
 standby 1 track Serial0/3/0

interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.40.1 255.255.255.240
 standby 1 ip 172.16.40.1
 standby 1 preempt
 standby 1 track Serial0/3/0

interface FastEthernet0/0.60
 encapsulation dot1Q 60
 ip address 172.16.60.1 255.255.255.240

//confoguring frame relay and the public link ip address

interface Serial0/3/0
 ip address 192.168.10.2 255.255.255.248
 encapsulation frame-relay
 frame-relay map ip 192.168.10.1 201 broadcast
 frame-relay map ip 192.168.10.3 203 broadcast
 frame-relay map ip 192.168.10.4 204 broadcast
 frame-relay lmi-type ansi
 ip nat outside

//configuring ospf

router ospf 1
 log-adjacency-changes
 network 172.16.10.0 0.0.0.7 area 0
 network 172.16.20.0 0.0.0.31 area 0
 network 172.16.30.0 0.0.0.15 area 0
```

```
 network 172.16.40.0 0.0.0.15 area 0
 network 172.16.50.0 0.0.0.15 area 0

//gonfiguring ip routes/ NAT

ip classless
ip route 0.0.0.0 0.0.0.0 192.168.10.4
ip route 0.0.0.0 0.0.0.0 192.168.10.3
ip route 0.0.0.0 0.0.0.0 192.168.10.1

ip flow-export version 9

access-list 10 deny 172.16.30.0 0.0.0.15
access-list 10 deny 172.16.40.0 0.0.0.15
access-list 10 permit any

//configuring telephony service and directory number

telephony-service
 max-ephones 3
 max-dn 3
 ip source-address 172.16.60.1 port 2000
 auto assign 1 to 3

//configuring the phone extention numbers

ephone-dn 1
 number 111

ephone-dn 2
 number 222

ephone-dn 3
 number 333

//configuring ephone buttons

ephone 1
 device-security-mode none
 mac-address 00D0.5886.B6DA
 type 7960
 button 1:1

ephone 2
 device-security-mode none
 mac-address 000A.F352.5CE4
 type 7960
 button 1:2

ephone 3
 device-security-mode none
 mac-address 0003.E417.519E
 type 7960
```

```
 button 1:3

line con 0
 password cisco
 login

line aux 0
line vty 0 4
 password cisco
 login
 transport input ssh
end

//configuring the DRS_ACTIVE_ROUTER (disaster recovery)

hostname DRS_ACTIVE_ROUTER

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1

//configuring shh

username student password 0 cisco

crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2

ip ssh authentication-retries 2
ip ssh time-out 15
ip domain-name niselagroupholding.co.za

spanning-tree mode pvst

// configuring ips

ip ips config location ipsBranch retries 1
ip ips name iosips
ip ips signature-category
  category all
   retired true
  category ios_ips basic
   retired false

//configuring access list

access-list 10 deny 172.16.30.0 0.0.0.15
access-list 10 deny 172.16.40.0 0.0.0.15
access-list 10 permit any

//configuring router on a stick and HSRP

interface FastEthernet0/0.50
```

```
 encapsulation dot1Q 50
 ip address 172.16.50.1 255.255.255.240
 standby 1 ip 172.16.50.1
 standby 1 priority 150
 standby 1 preempt
 standby 1 track Serial0/3/0

//confoguring frame relay and the public link ip address

interface Serial0/3/0
 ip address 192.168.10.3 255.255.255.248
 encapsulation frame-relay
 frame-relay map ip 192.168.10.1 301 broadcast
 frame-relay map ip 192.168.10.2 302 broadcast
 frame-relay map ip 192.168.10.4 304 broadcast
 frame-relay lmi-type ansi
 ip access-group 10 in
 ip nat outside

//configuring ospf

router ospf 1
 log-adjacency-changes
 network 172.16.10.0 0.0.0.7 area 0
 network 172.16.20.0 0.0.0.31 area 0
 network 172.16.30.0 0.0.0.15 area 0
 network 172.16.40.0 0.0.0.15 area 0
 network 172.16.50.0 0.0.0.15 area 0


//gonfiguring ip routes/NAT

ip classless
ip route 0.0.0.0 0.0.0.0 192.168.10.2
ip route 0.0.0.0 0.0.0.0 192.168.10.4
ip route 0.0.0.0 0.0.0.0 192.168.10.1

line con 0
 password cisco
 login

line aux 0
line vty 0 4
 password cisco
 login
 transport input ssh
end

//configuring the DRS_STANDBY_ROUTER(disaster recovery)

hostname RouterStandby
!
!
```

```
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
ip dhcp excluded-address 172.16.10.1 172.16.10.5
ip dhcp excluded-address 172.16.20.1 172.16.20.5
ip dhcp excluded-address 172.16.30.1 172.16.30.5
ip dhcp excluded-address 172.16.40.1 172.16.40.5
ip dhcp excluded-address 172.16.50.1 172.16.50.5
!
ip dhcp pool EXAM
network 172.16.10.0 255.255.255.192
default-router 172.16.10.1
dns-server 172.16.16.4
ip dhcp pool HOD
network 172.16.20.0 255.255.255.192
default-router 172.16.20.1
dns-server 172.16.16.4
ip dhcp pool HR
network 172.16.30.0 255.255.255.192
default-router 172.16.30.1
dns-server 172.16.16.4
ip dhcp pool STAFF
network 172.16.40.0 255.255.255.192
default-router 172.16.40.1
dns-server 172.16.16.4
ip dhcp pool IT
network 172.16.50.0 255.255.255.192
default-router 172.16.50.1
dns-server 172.16.16.4
ip dhcp pool PHONES
network 172.16.60.0 255.255.255.192
default-router 172.16.60.1
option 150 ip 172.16.60.1
!
!
!
no ip cef
no ipv6 cef
!
!
!
username student password 0 cisco
!
!
license udi pid CISCO2811/K9 sn FTX10173N63-
!
!
!
crypto isakmp policy 1
encr aes
authentication pre-share
group 2
```

```
!
ip ssh authentication-retries 2
ip ssh time-out 15
ip domain-name gpe.gov.za
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 172.16.10.3 255.255.255.192
standby 1 ip 172.16.10.1
standby 1 priority 140
standby 1 preempt
standby 1 track Serial0/0/0
!
interface FastEthernet0/0.16
encapsulation dot1Q 16
ip address 172.16.16.3 255.255.255.240
standby 1 ip 172.16.16.1
standby 1 priority 140
standby 1 preempt
standby 1 track Serial0/0/0
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 172.16.20.3 255.255.255.192
standby 1 ip 172.16.20.1
standby 1 priority 140
standby 1 preempt
standby 1 track Serial0/0/0
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 172.16.30.3 255.255.255.192
standby 1 ip 172.16.30.1
standby 1 priority 140
standby 1 preempt
standby 1 track Serial0/0/0
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 172.16.40.3 255.255.255.192
```

```
standby 1 ip 172.16.40.1
standby 1 priority 140
standby 1 preempt
standby 1 track Serial0/0/0
!
interface FastEthernet0/0.50
encapsulation dot1Q 50
ip address 172.16.50.3 255.255.255.192
standby 1 ip 172.16.50.1
standby 1 priority 140
standby 1 preempt
standby 1 track Serial0/0/0
!
interface FastEthernet0/0.60
encapsulation dot1Q 60
ip address 172.16.60.3 255.255.255.192
standby 1 ip 172.16.60.1
standby 1 priority 150
standby 1 preempt
standby 1 track Serial0/0/0
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 2.168.1.5 255.255.255.252
ip access-group 5 out
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2/1
no ip address
```

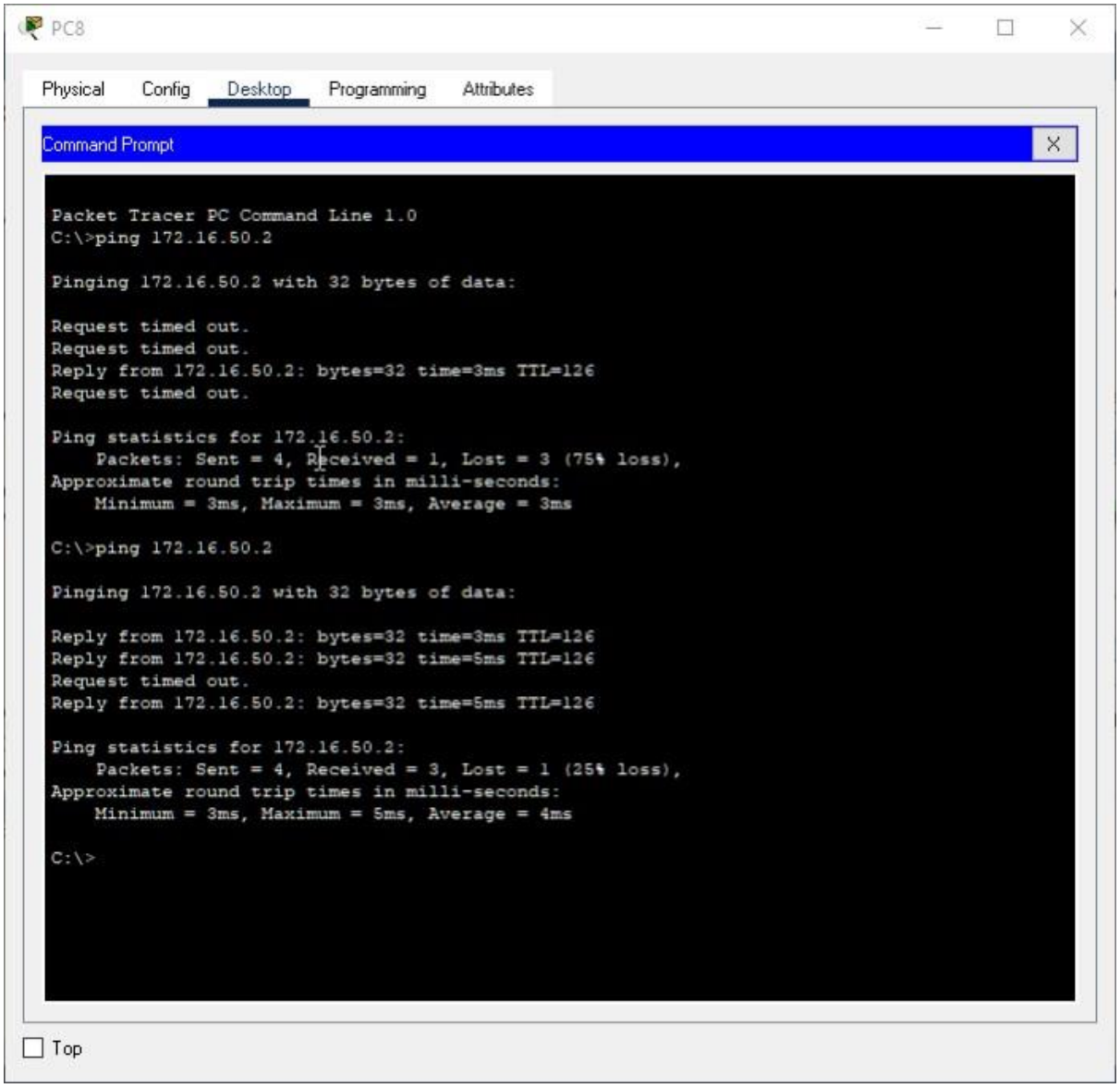
```
clock rate 2000000
shutdown
!
interface Serial0/3/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router          rip
version          2
network 2.0.0.0
network 172.16.0.0
!
ip classless
!
ip flow-export version 9
!
!
access-list 5 deny 172.16.10.0 0.0.0.63
access-list 5 deny 172.16.20.0 0.0.0.63
access-list 5 deny 172.16.30.0 0.0.0.63
access-list 5 deny 172.16.40.0 0.0.0.63
access-list 5 permit any
!
!
!
!
!
!
telephony-service
max-ephones 5
max-dn 5
ip source-address 172.16.60.1 port 2000
auto assign 1 to 5
!
ephone-dn 1
number 1000
!
ephone-dn 2
number 1001
!
ephone-dn 3
number 1002
!
```

```
ephone-dn 4
number 1003
!
ephone-dn 5
number 1004
!
ephone 1
device-security-mode none
mac-address 0001.96A6.EB13
type 7960
button 1:1
!
ephone 2
device-security-mode none
mac-address 0006.2A6E.9A99
type 7960
button 1:2
!
ephone 3
device-security-mode none
mac-address 00E0.F73B.59B2
type 7960
button 1:3
!
ephone 4
device-security-mode none
mac-address 0001.43B0.39A5
type 7960
button 1:4
!
ephone 5
device-security-mode none
mac-address 0007.ECEE.52AB
type 7960
button 1:5
!
line con 0
!
line aux 0
!
line vty 0 4
password admin
login
transport input ssh
!
!
!
end
hostname DRS_STANDBY_ROUTER

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1

//configuring shh
```

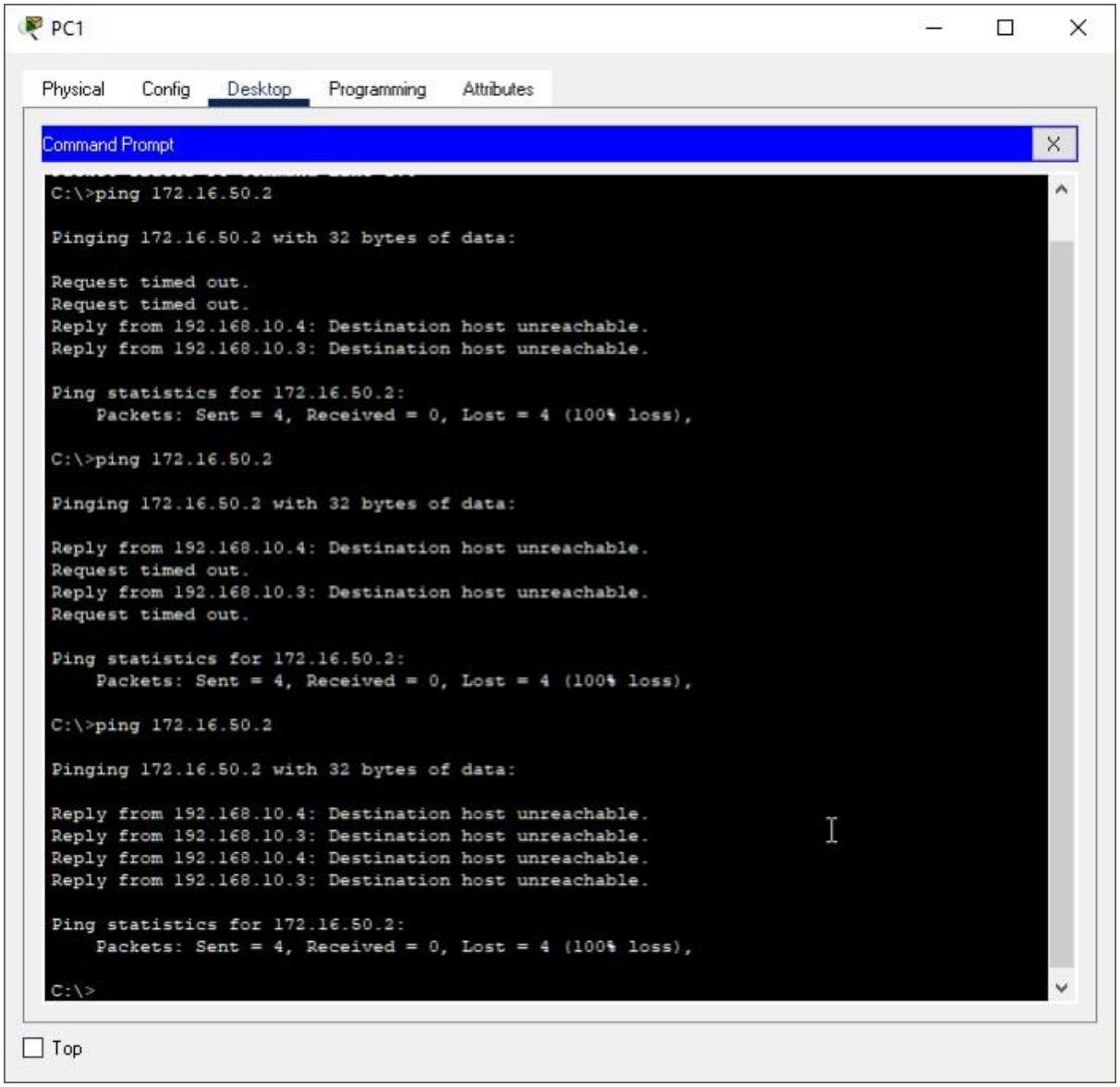
```
username student password 0 cisco

crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2

ip ssh authentication-retries 2
ip ssh time-out 15
ip domain-name niselagroupholding.co.za

spanning-tree mode pvst

// configuring ips

ip ips config location ipsBranch retries 1
ip ips name iosips
ip ips signature-category
  category all
   retired true
  category ios_ips basic
   retired false

//configuring access list

access-list 10 deny 172.16.30.0 0.0.0.15
access-list 10 deny 172.16.40.0 0.0.0.15
access-list 10 permit any

//configuring router on a stick and HSRP

interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 172.16.50.1 255.255.255.240
 standby 1 ip 172.16.50.1
 standby 1 preempt
 standby 1 track Serial0/3/0

//confoguring frame relay and the public link ip address

interface Serial0/3/0
 ip address 192.168.10.4 255.255.255.248
 encapsulation frame-relay
 frame-relay map ip 192.168.10.1 401 broadcast
 frame-relay map ip 192.168.10.2 402 broadcast
 frame-relay map ip 192.168.10.3 403 broadcast
 frame-relay lmi-type ansi
 ip access-group 10 in
 ip nat outside

//configuring ospf
```

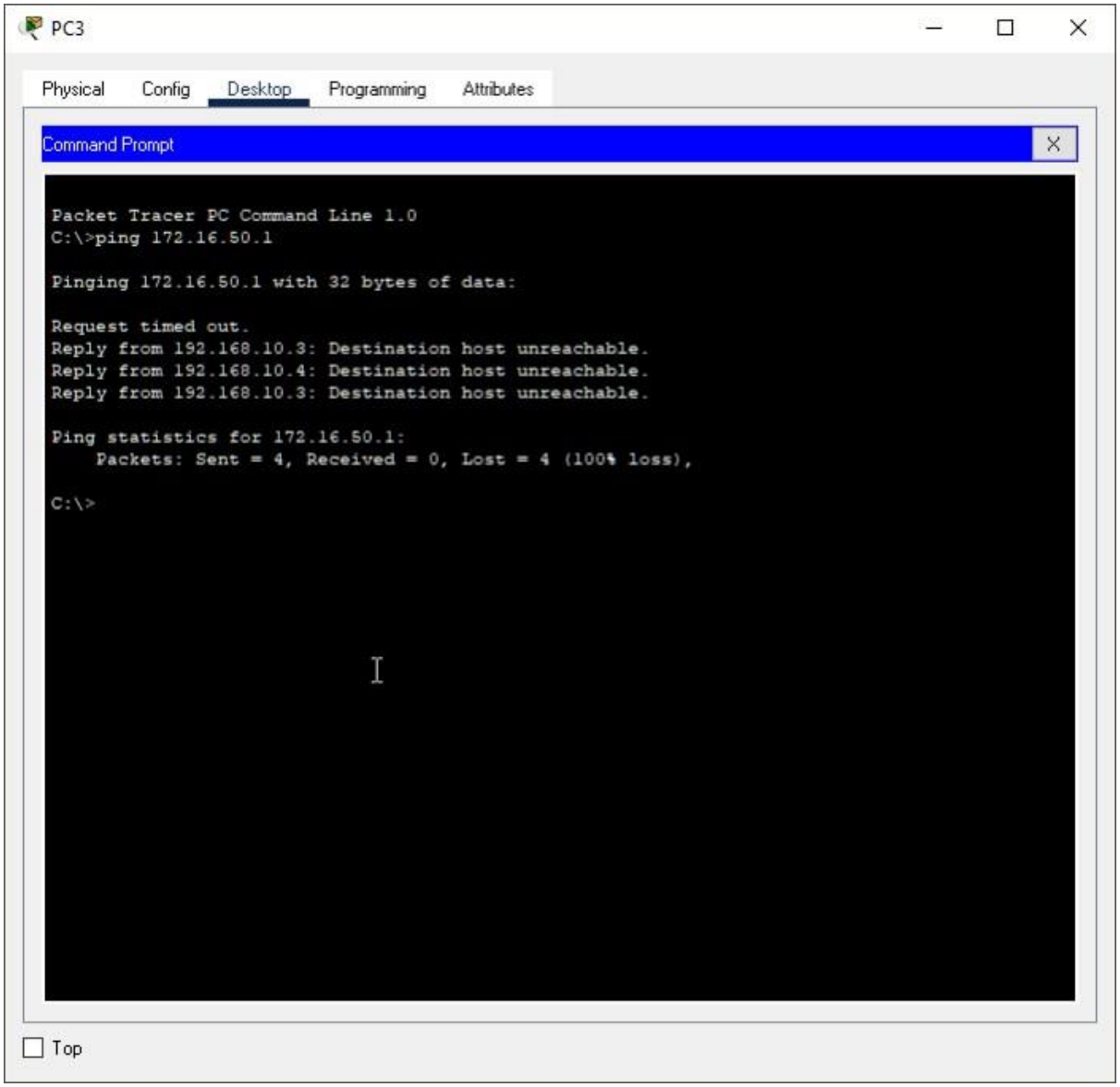
```
router ospf 1
 log-adjacency-changes
 network 172.16.10.0 0.0.0.7 area 0
 network 172.16.20.0 0.0.0.31 area 0
 network 172.16.30.0 0.0.0.15 area 0
 network 172.16.40.0 0.0.0.15 area 0
 network 172.16.50.0 0.0.0.15 area 0

//gonfiguring ip routes/NAT

ip classless
ip route 0.0.0.0 0.0.0.0 192.168.10.2
ip route 0.0.0.0 0.0.0.0 192.168.10.3
ip route 0.0.0.0 0.0.0.0 192.168.10.1

line con 0
 password cisco
 login

line aux 0
line vty 0 4
 password cisco
 login
 transport input ssh
end

//Ping Disaster recovery server from VLAN 20 the IT department
```

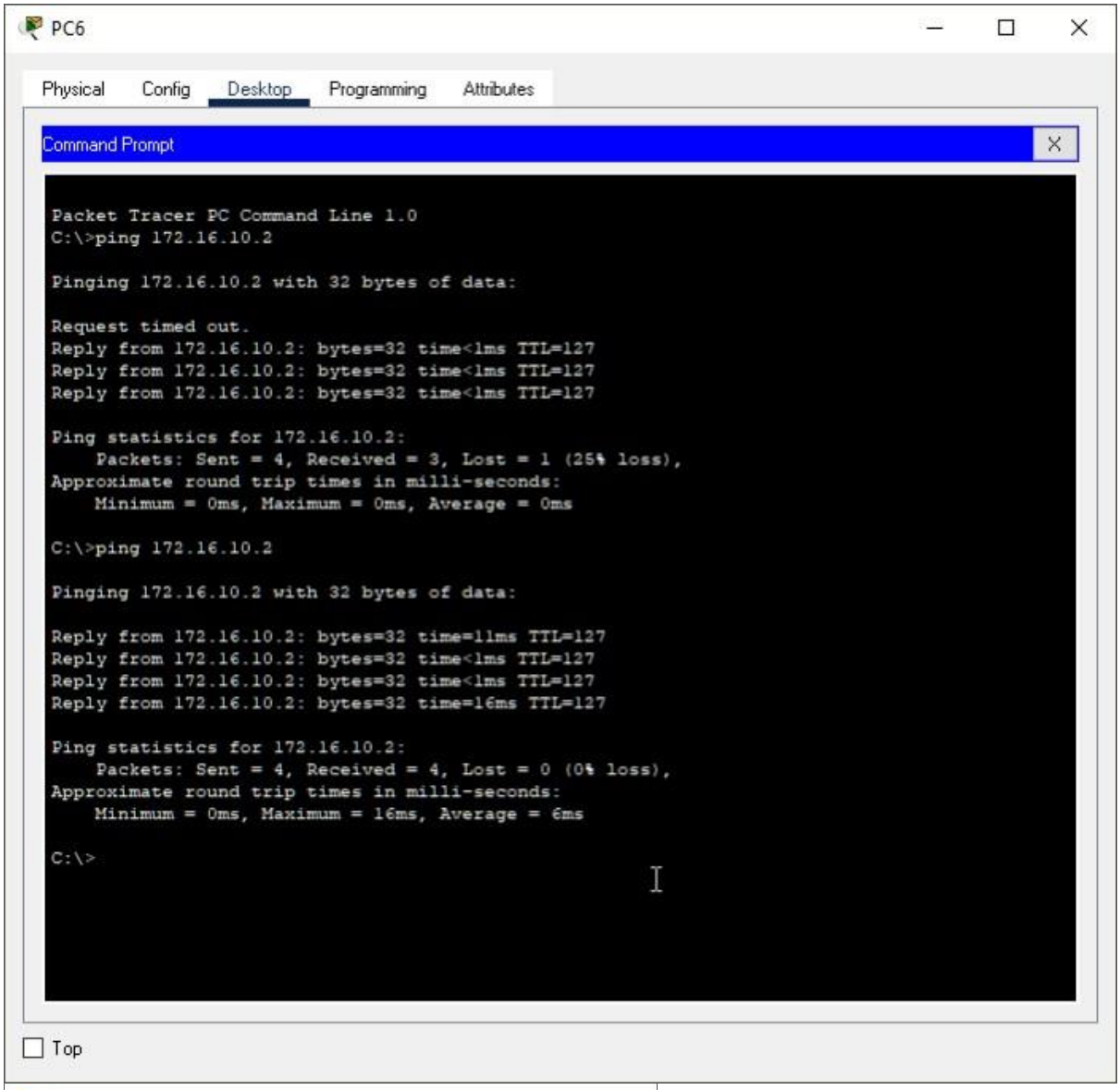
Overall Outcomes or Results



//Ping Disaster recovery server from VLAN 40 the Management department

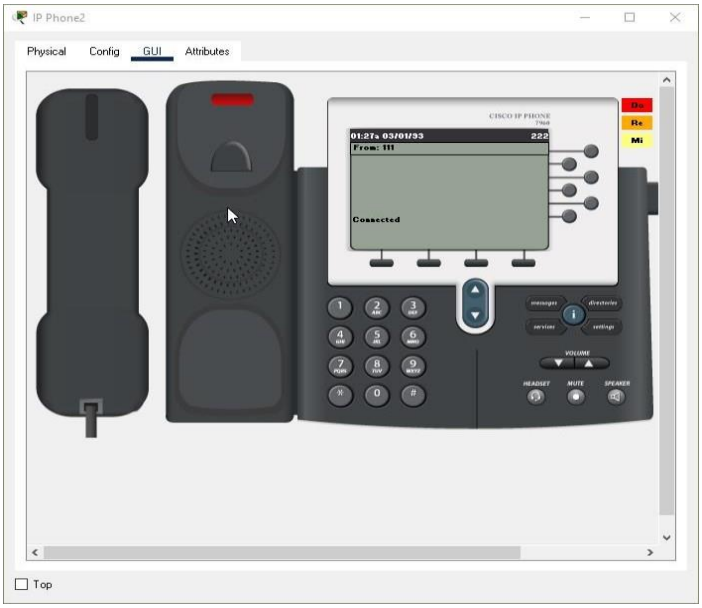

PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 172.16.50.2
Pinging 172.16.50.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.10.4: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Ping statistics for 172.16.50.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.16.50.2
Pinging 172.16.50.2 with 32 bytes of data:
Reply from 192.168.10.4: Destination host unreachable.
Request timed out.
Reply from 192.168.10.3: Destination host unreachable.
Request timed out.
Ping statistics for 172.16.50.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.16.50.2
Pinging 172.16.50.2 with 32 bytes of data:
Reply from 192.168.10.4: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.4: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Ping statistics for 172.16.50.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top


PC3
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.50.1
Pinging 172.16.50.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.4: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Ping statistics for 172.16.50.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top

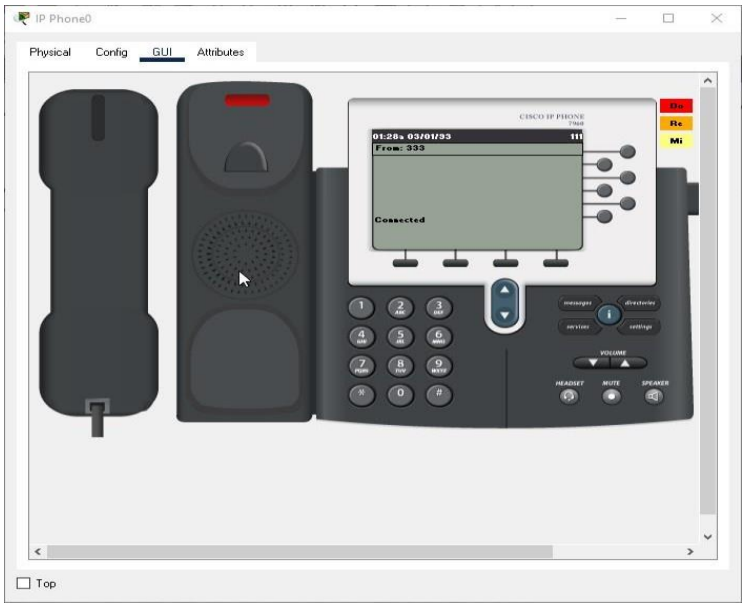

PC6
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.2
Pinging 172.16.10.2 with 32 bytes of data:
Request timed out.
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Ping statistics for 172.16.10.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.16.10.2
Pinging 172.16.10.2 with 32 bytes of data:
Reply from 172.16.10.2: bytes=32 time=11ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time=16ms TTL=127
Ping statistics for 172.16.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 16ms, Average = 6ms
C:\>
Top


IP Phone3
Physical
Config
GUI
Attributes
The phone is ringing
Top

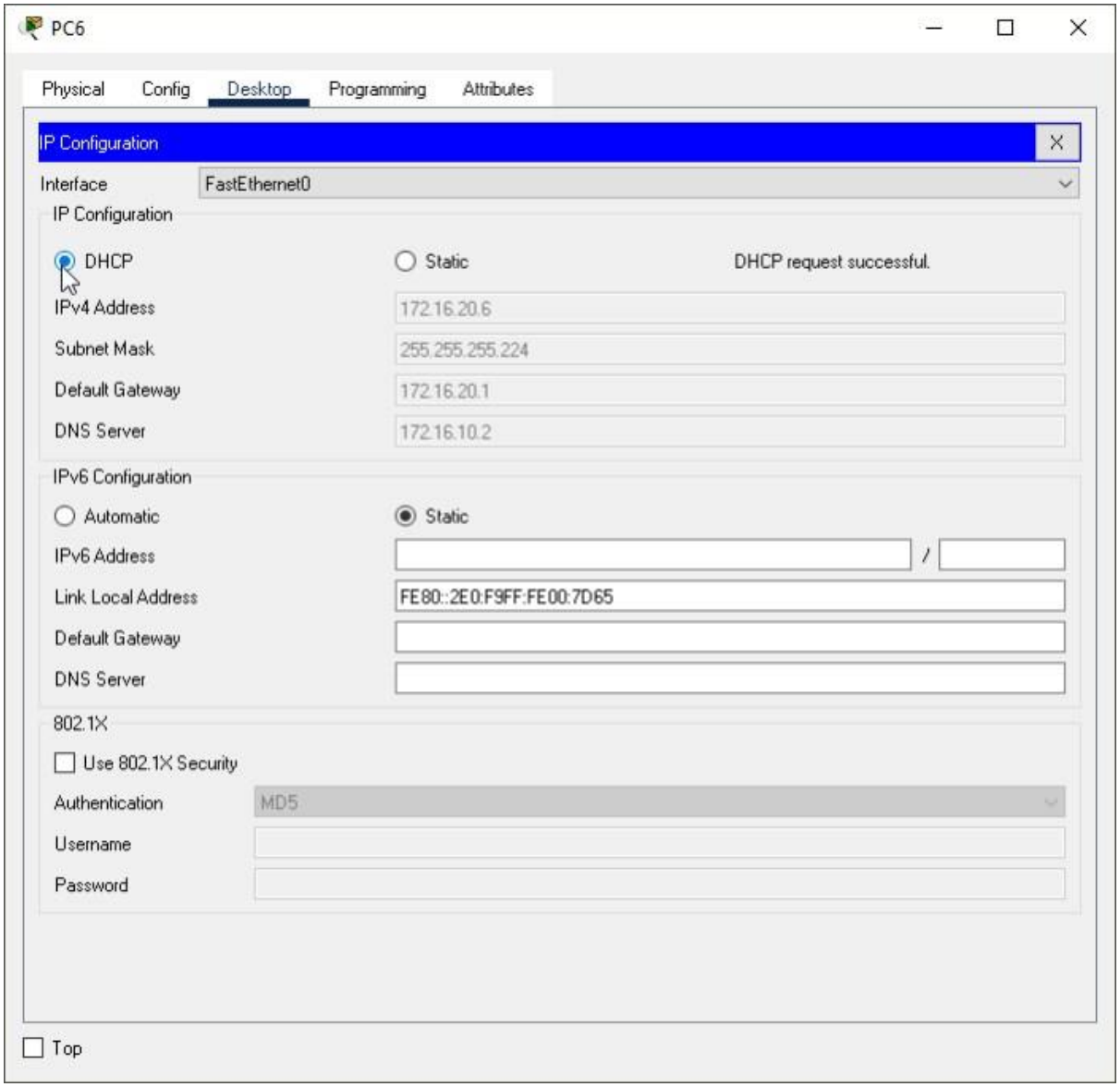

IP Phone0
Physical
Config
GUI
Attributes
To: 222
Ring Out
Top

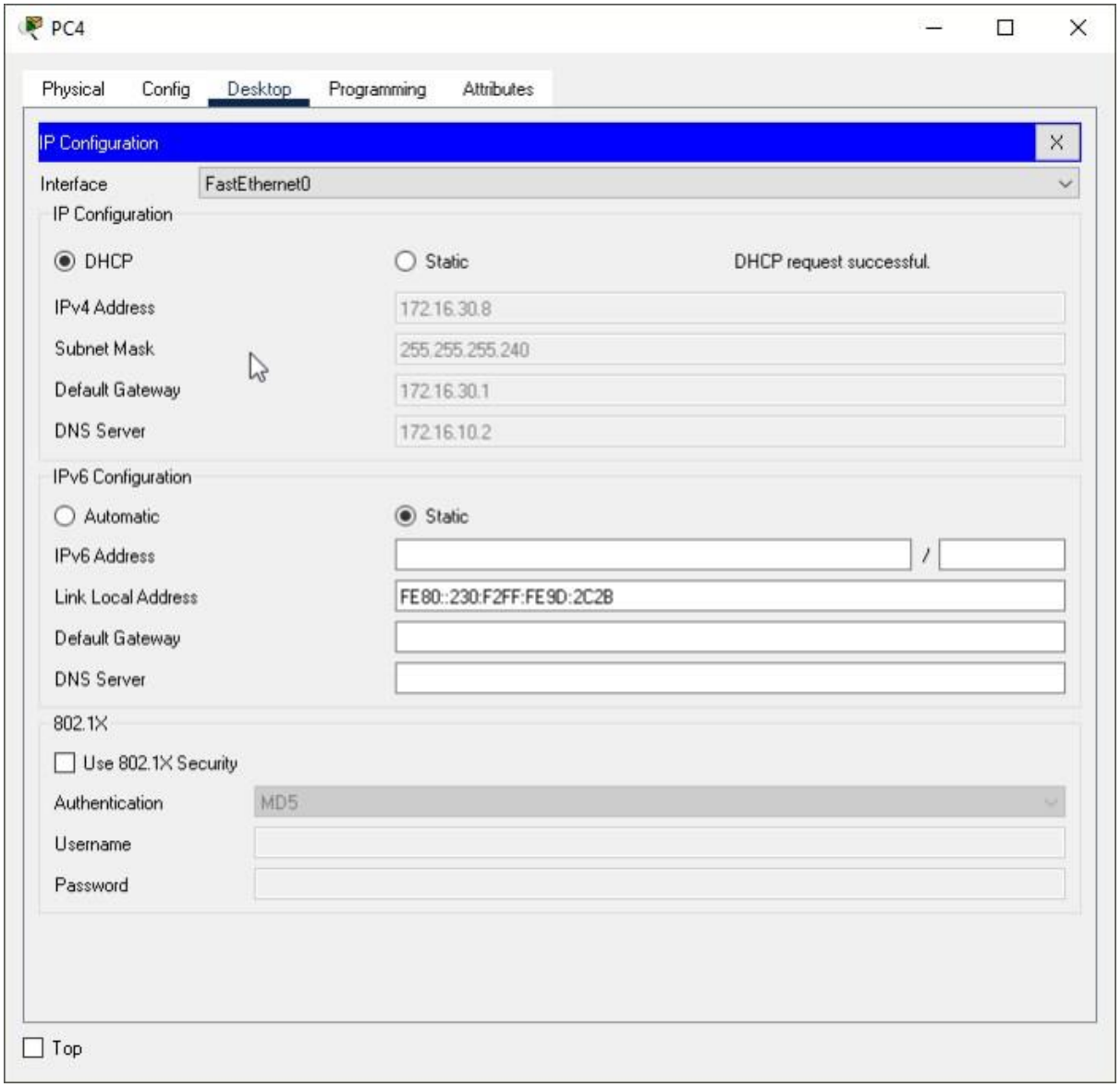

IP Phone2
Physical
Config
GUI
Attributes
From: 111
Connected
Top

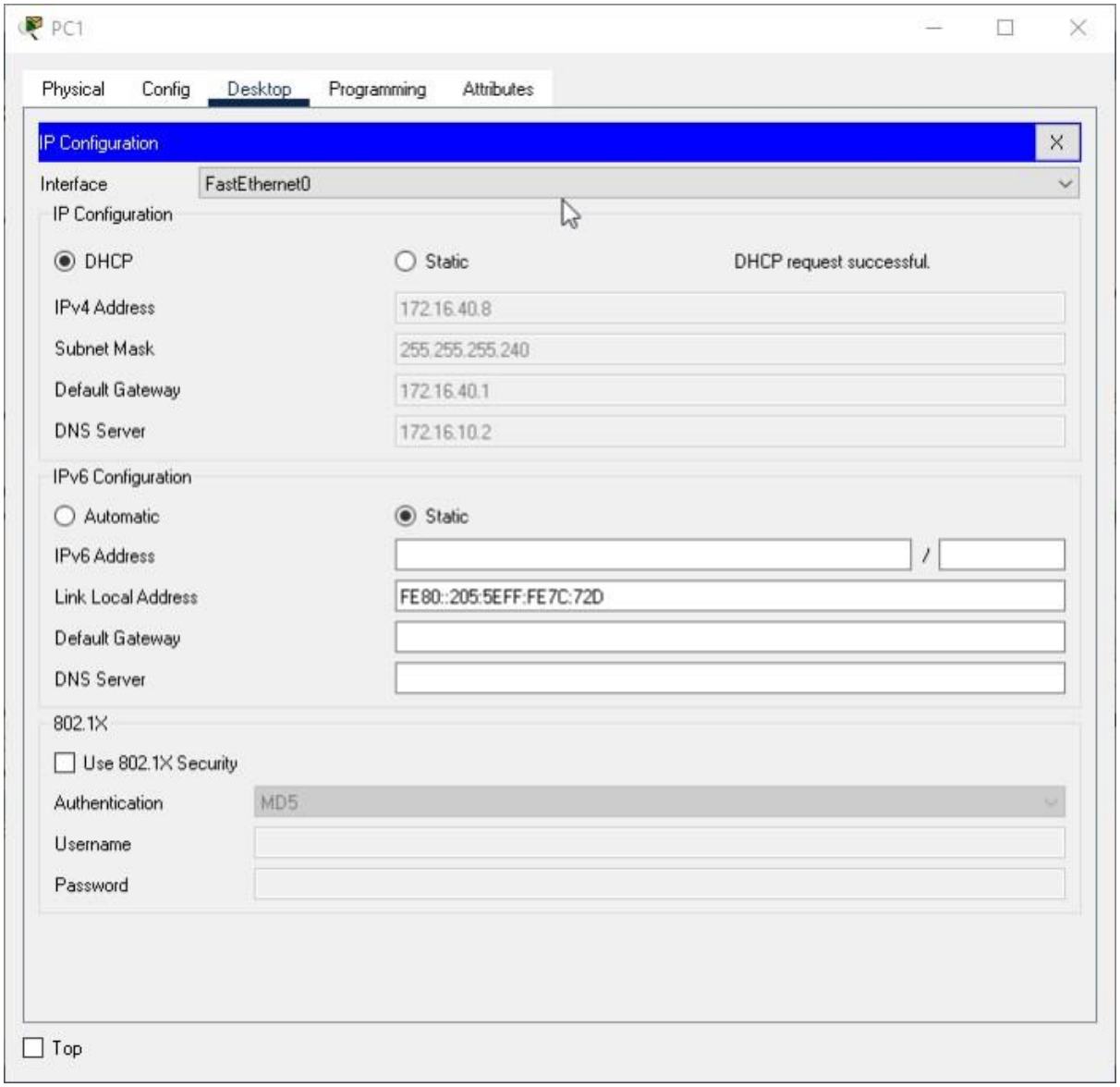

IP Phone3
Physical
Config
GUI
Attributes
To: 111
Ring Out
Top


IP Phone0
Physical
Config
GUI
Attributes
From: 333
Connected
Top

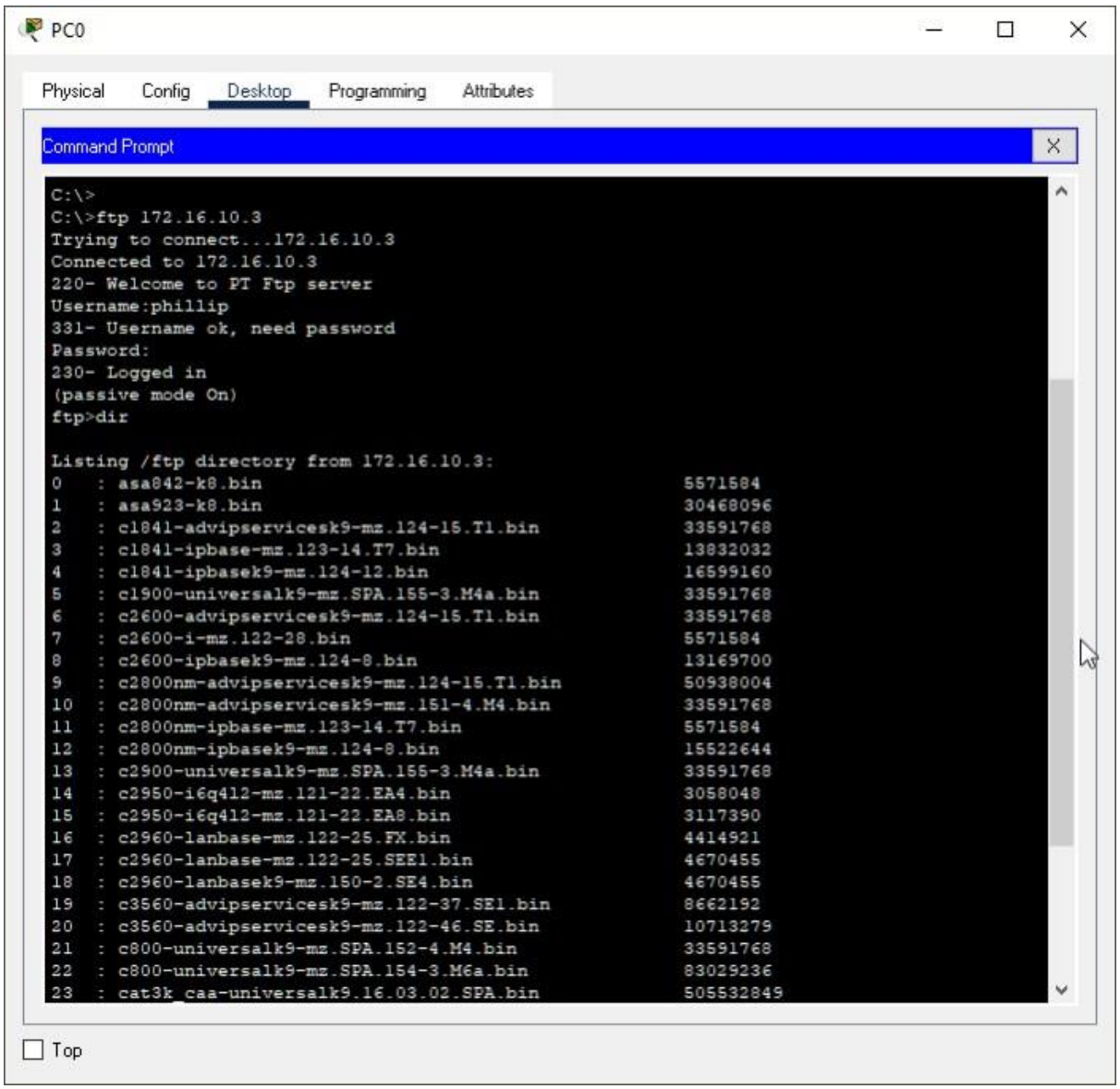
//DHCP assigned PCs on VLAN 20, VLAN 30 and VLAN 40


PC6
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
172.16.20.6
Subnet Mask
255.255.255.224
Default Gateway
172.16.20.1
DNS Server
172.16.10.2
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2E0:F9FF:FE00:7D65
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

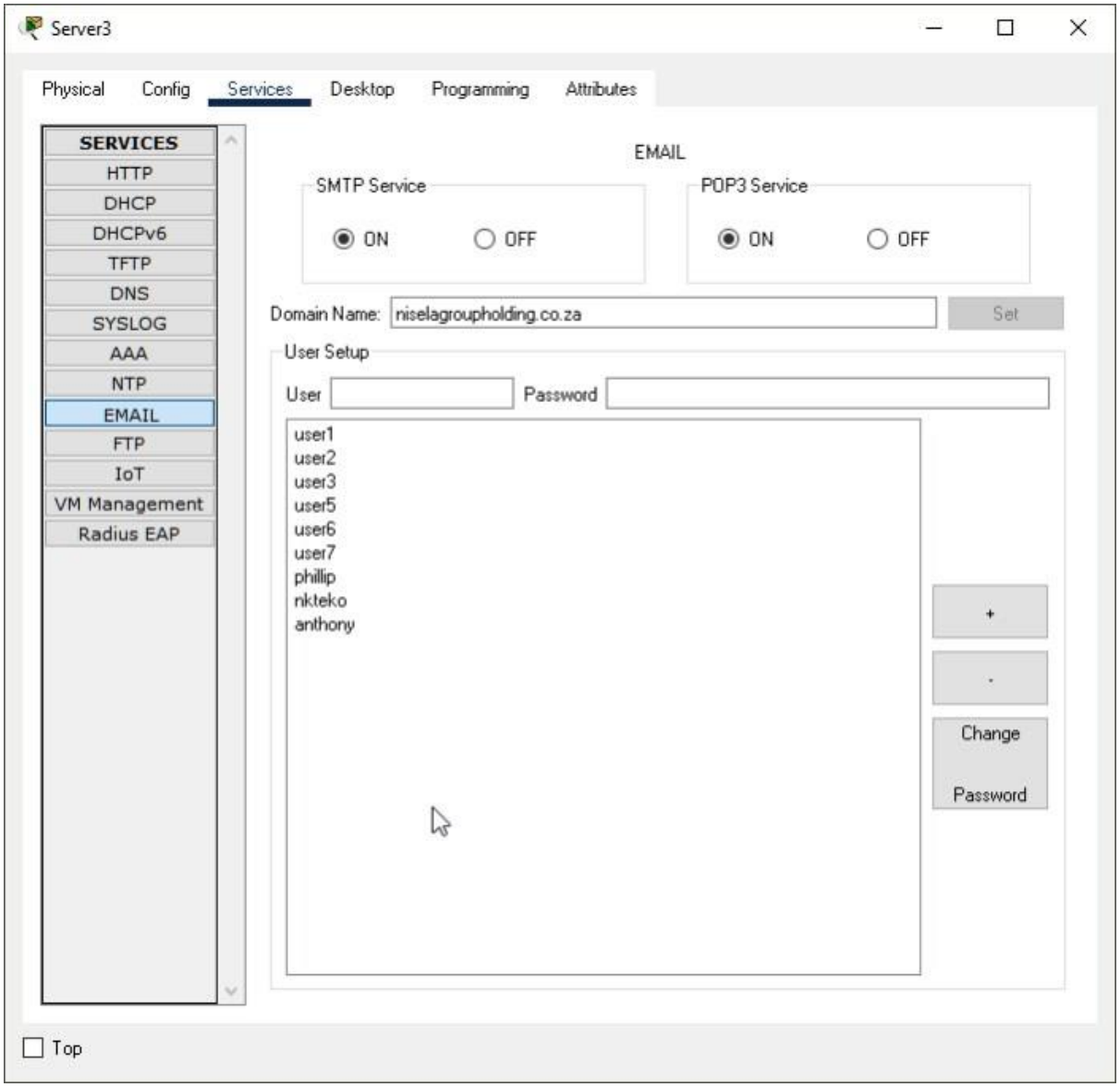

PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
172.16.30.8
Subnet Mask
255.255.255.240
Default Gateway
172.16.30.1
DNS Server
172.16.10.2
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::230:F2FF:FE9D:2C2B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top



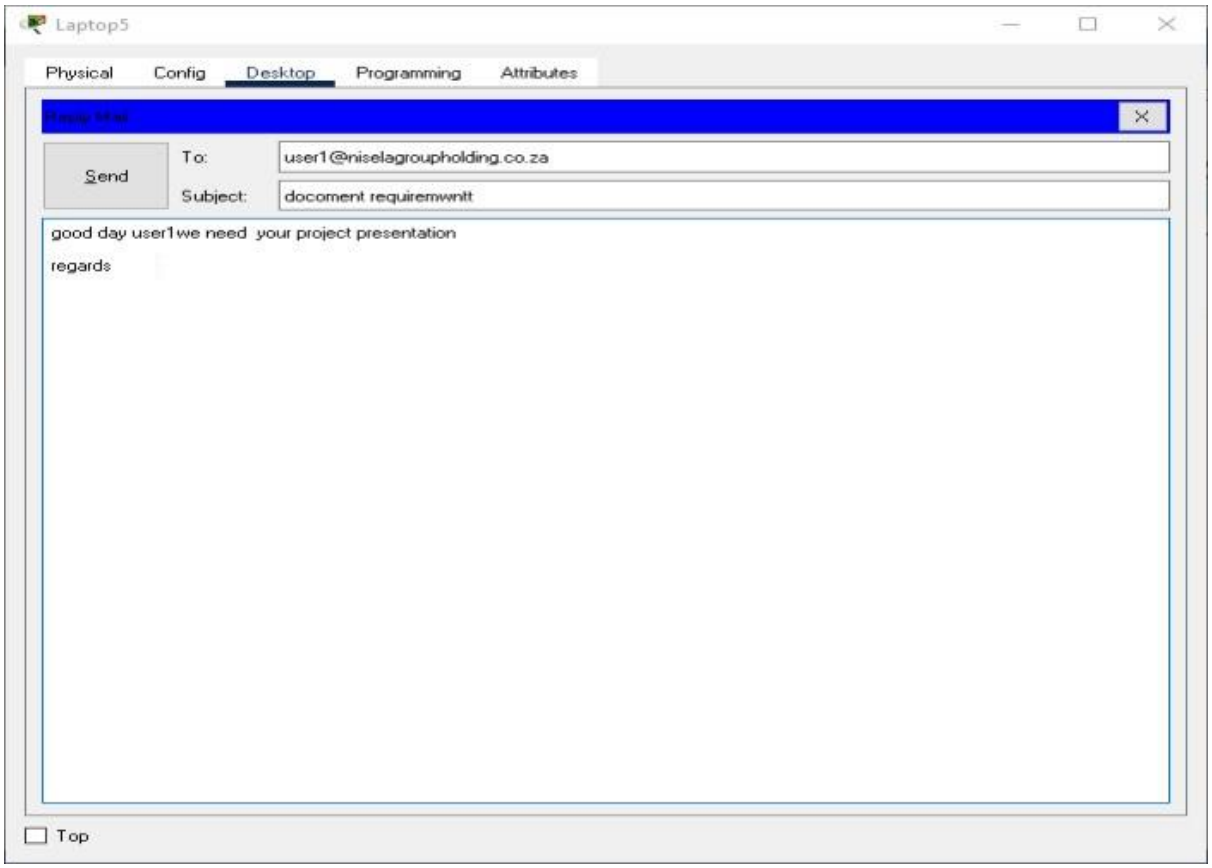
//Login to ftp server in the datacentre from Management department

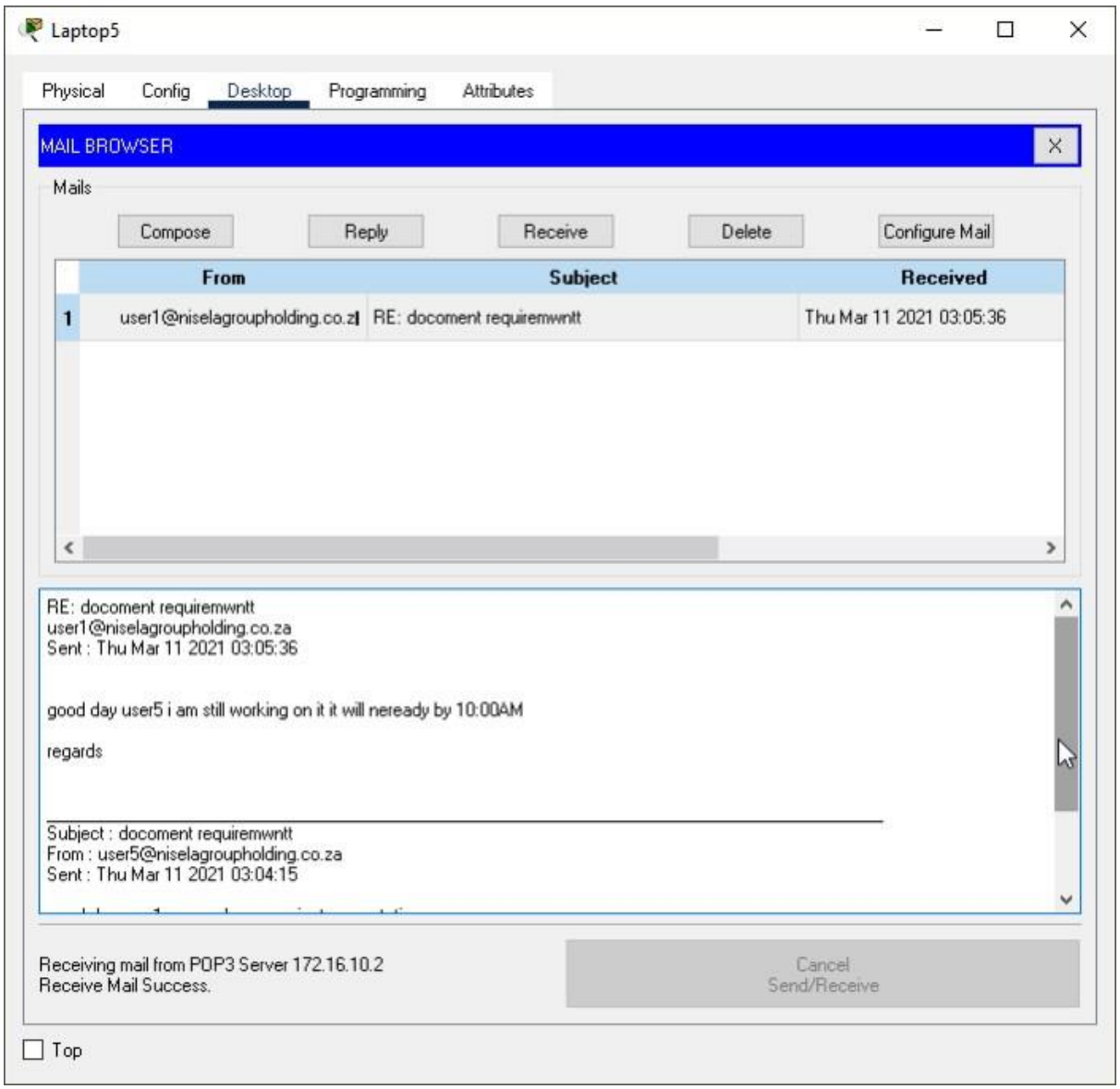


//Sending email from one brunch to another brunch

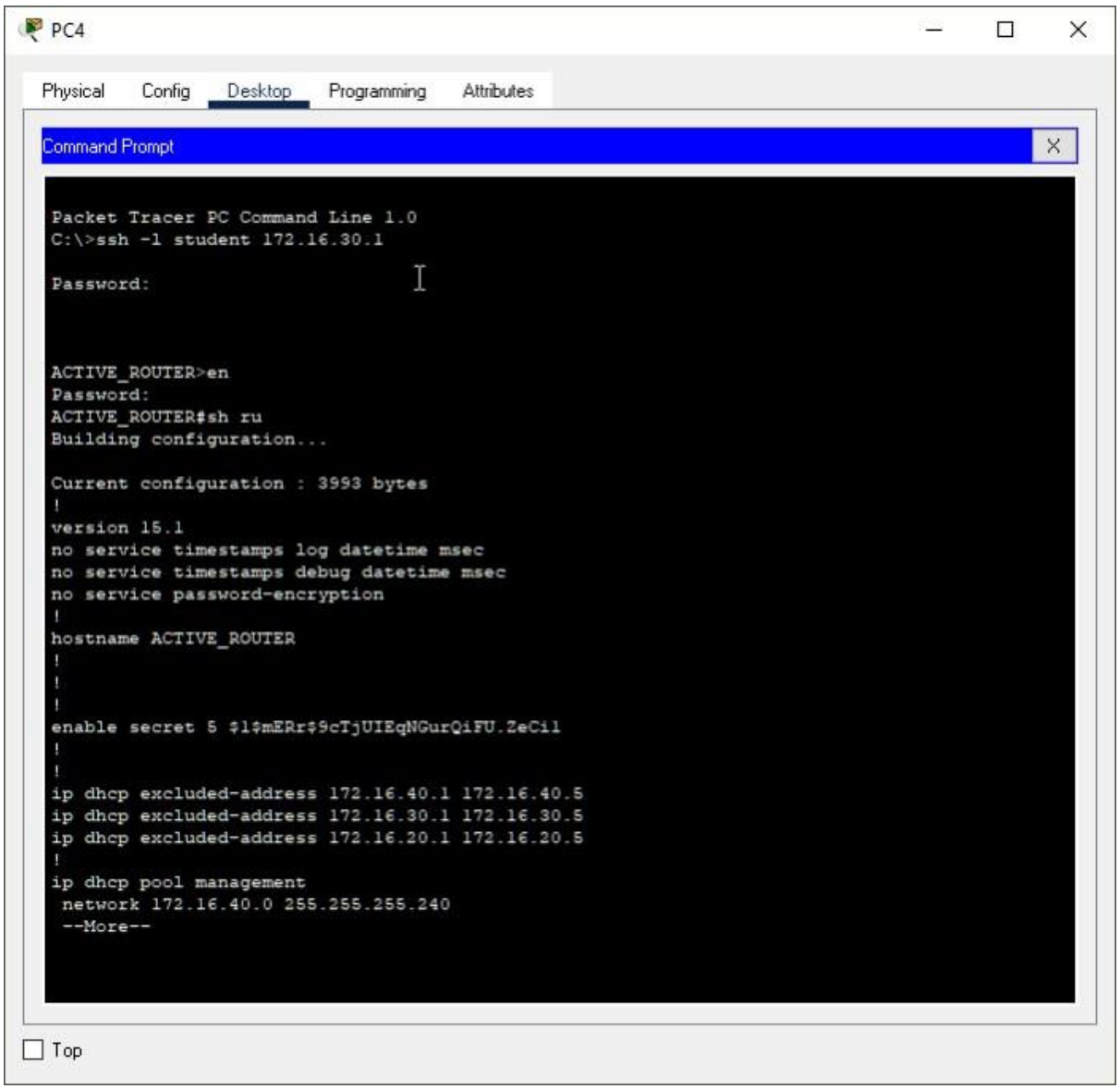


//Sending Email

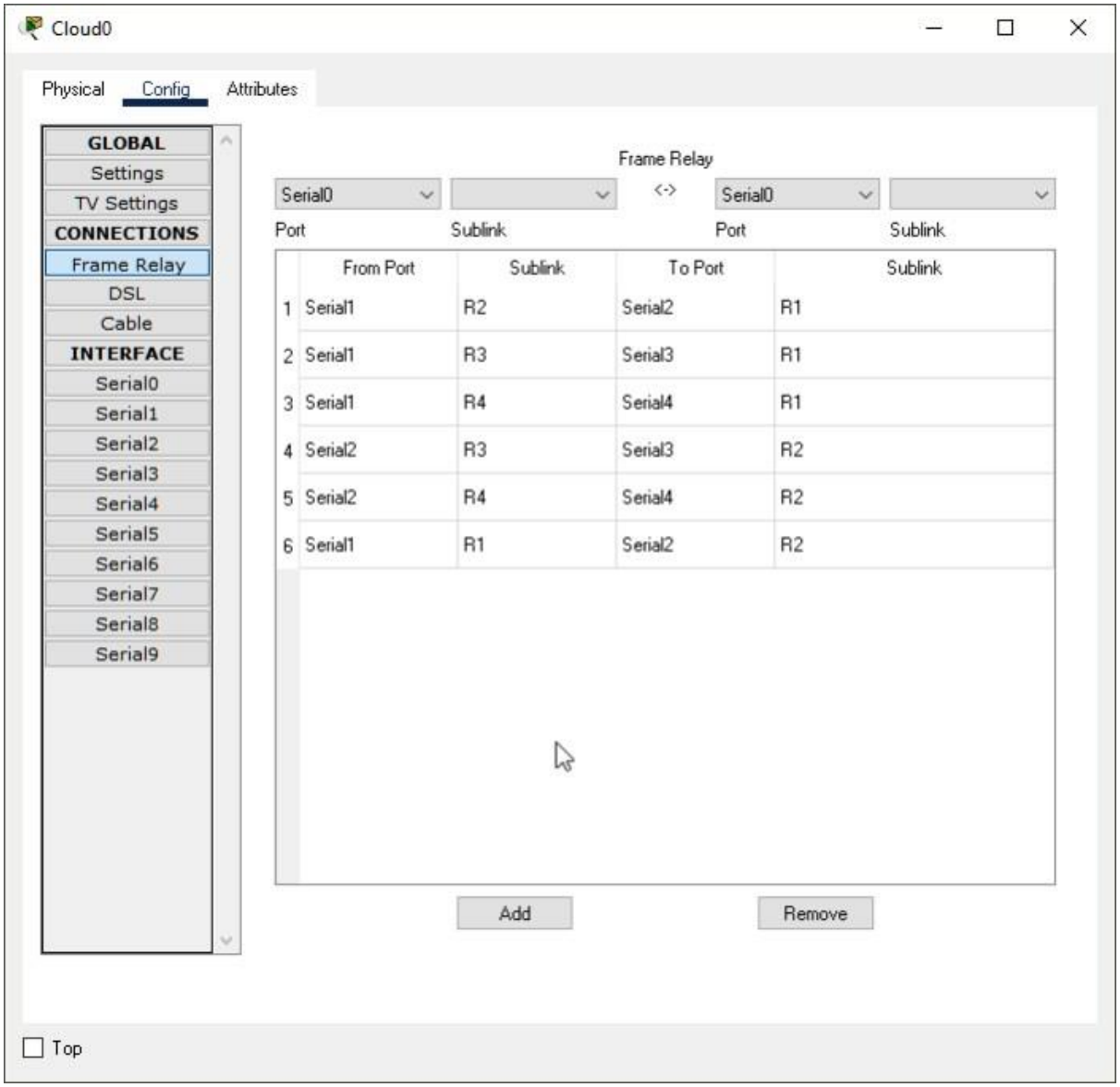

Laptop5
Physical
Config
Desktop
Programming
Attributes
Send
To:
user1@niselagroupholding.co.za
Subject:
docoment requiremwnlt
good day user1we need your project presentation
regards
Top


Laptop5
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
user1@niselagroupholding.co.z
RE: docoment requiremwntt
Thu Mar 11 2021 03:05:36
RE: docoment requiremwntt
user1@niselagroupholding.co.za
Sent : Thu Mar 11 2021 03:05:36
good day user5 i am still working on it it will neready by 10:00AM
regards
Subject : docoment requiremwntt
From : user5@niselagroupholding.co.za
Sent : Thu Mar 11 2021 03:04:15
Receiving mail from POP3 Server 172.16.10.2
Receive Mail Success.
Cancel
Send/Receive
Top

//SSH

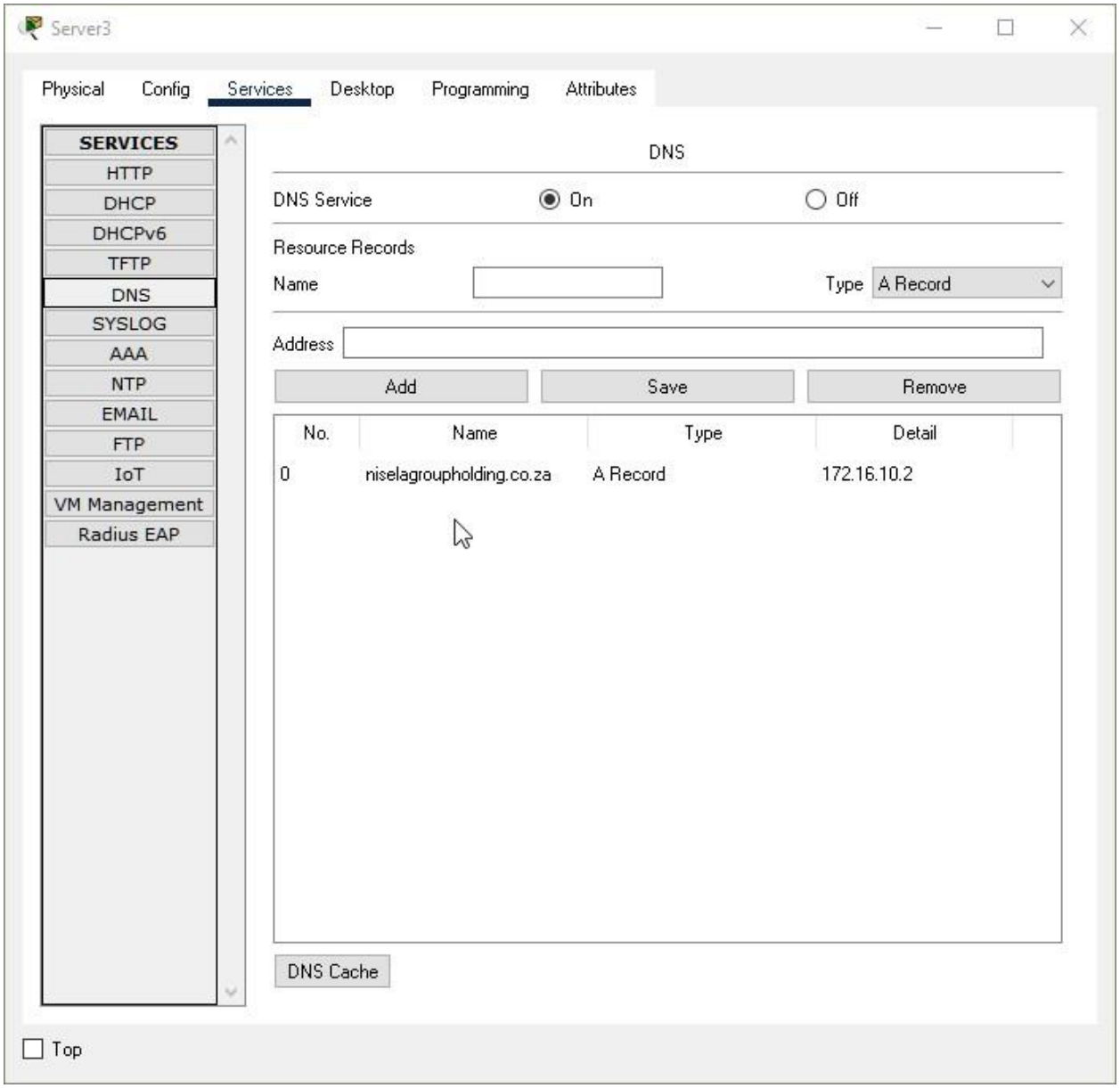

PC4
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ssh -l student 172.16.30.1
Password:
ACTIVE_ROUTER>en
Password:
ACTIVE_ROUTER#sh ru
Building configuration...
Current configuration : 3993 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ACTIVE_ROUTER
!
!
!
enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 172.16.40.1 172.16.40.5
ip dhcp excluded-address 172.16.30.1 172.16.30.5
ip dhcp excluded-address 172.16.20.1 172.16.20.5
!
ip dhcp pool management
network 172.16.40.0 255.255.255.240
--More--
Top

//Frame Relay

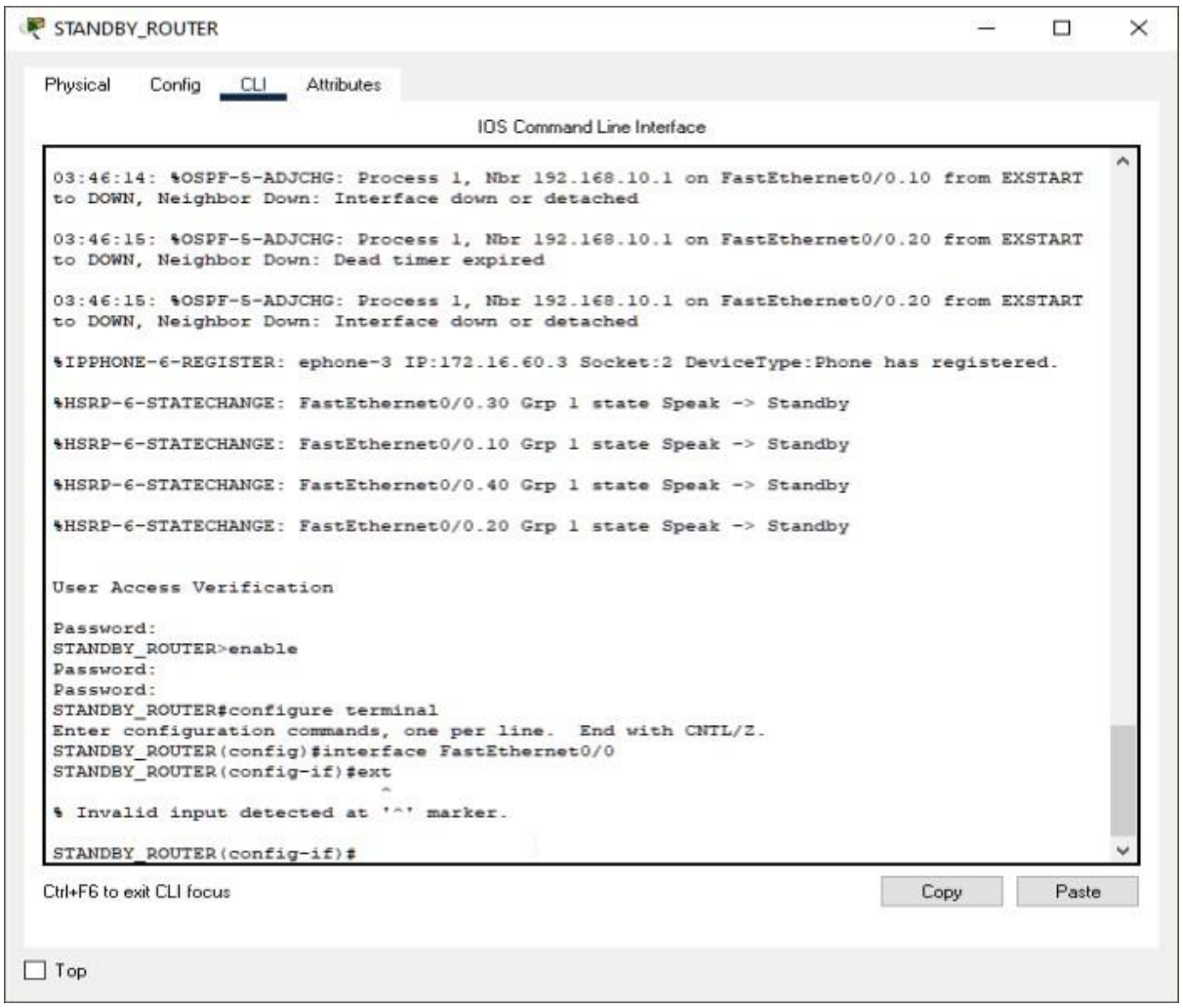


//DNS

//DNS Server


Server3
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DNS
DNS Service
On
Off
Resource Records
Name
Type
A Record
Address
Add
Save
Remove
No.
Name
Type
Detail
0
niselagroupholding.co.za
A Record
172.16.10.2
DNS Cache
Top

//Web site



Overall Summary

I believe this project is of value and will allow me to broaden my knowledge in networking considering the complex network infrastructure design I have put in place measures which requires extensive configuring such as IPS which will allow remote monitoring administration and real-time traffic analysis.

Hybrid topology is used to design the network which this address the issues of a single point of failure. Implementation of VLANs and Wi-Fi address the issue of network congestion and increase the overall network productivity and availability.

I understand what it means to design a reliable security infrastructure for medium enterprise companies hence I have incorporated high security technologies such as port

security, DHCP snooping, filtering traffic based on ACLs, IPSec, VLANs and IPS used to monitor both internal and external attacks.

Replication of resources such as core routers and switches and introducing link aggregation has addressed the redundancy issue by providing standbys in case of any failure, this provide reliability. Security implementation with designated security protocols such as SSH, ACL and others protects the network from unauthorized users and attackers. The overall network is secure, cost effective and reliable.

With this proposed solution, I believe every medium enterprise may consider it as a best solution to incorporate in their live network environment.

References

- Halsall, F. (2001) *Multimedia Communications*, Addison Wesley.
- ITU-T X.509 (2000) *Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks* , International Telecommunication Union.

- King, T. and Newson, D. (1999) *Data Network Engineering*, Kluwer.
- Peterson, L. L. and Davie, B. S. (1996) *Computer Networks: A Systems Approach*, Morgan Kaufmann.

- RFC 2401 (1998) *Security Architecture for the Internet Protocol*, Kent, S., Atkinson, R.
- Schneier, B. (1996) *Applied Cryptography*, 2nd edn, Wiley.
- Stallings, W (1999) *Cryptography and Network Security*, Prentice Hall.
  Stallings, W (2001) *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, 3rd edn, Addison Wesley.

- Anderson, R. (2001) *Security Engineering: A Guide to Building Dependable Distributed Systems* , Wiley.
- BS 7799-2 (2002) *Information Security Management Systems – Specification with Guidance for Use* , British Standards Institution.
- Ellis, J. and Speed, T. (2001) *The Internet Security Guidebook*, Academic Press.
- ISO/IEC 17799 (2000) *Information Technology – Code of Practice for Information Security Management* , International Organization for Standardization.
- Tanenbaum, A. S. (1996) *Computer Networks*, 3rd edn, Prentice Hall.

- Network-security-essentials-4th-edition-william-stallings

- http://www.cisco.com/univercd/home/home.htm

- http://www.cisco.com/security
- http://www.cisco.com/pcgi-bin/front.x/csec/csecHome.pl

- www.YouTube.com

- Harold, Scott Warren, Martin C. Libicki, and Astrid Cevallos. "Getting to Yes with China in Cyberspace." RAND Corporation. 2016.

- Hathaway, Melissa E. "Strategic Advantage: Why America Should Care About Cybersecurity." Belfer Center for Science and International Affairs. October 2009.

- Hathaway, Melissa E. “Cyber Readiness 1.0.” Hathaway Global LLC. (2013).

- Hathaway, Melissa E. "Cyber Readiness Index 2.0" Belfer Center for Science and International Affairs. November 30, 2015.

- Hathaway, Oona A. “The Drawbacks and Dangers of Active Defense.” Presented at the 6th International Conference on Cyber Conflict, Tallinn, Estonia, 2014.

- Heinze T, Bauer G (2007) Characterizing creative scientists in nano-S&T: Productivity, multidisciplinarity, and network brokerage in a longitudinal perspective. Scientometrics 70: 811–830.
View ArticleGoogle Scholar

- .Yan EJ, Ding Y (2009) Applying Centrality Measures to Impact Analysis: A Coauthorship Network Analysis. Journal of the American Society for Information Science and Technology 60: 2107–2118.
View ArticleGoogle Scholar

- .Newman MEJ (2009) The first-mover advantage in scientific publication. Epl 86..

- Mazloumian A, Eom YH, Helbing D, Lozano S, Fortunato S (2011) How Citation

Boosts Promote Scientific Paradigm Shifts and Nobel Prizes. Plos One 6.
- View ArticleGoogle Scholar

- Csardi G, Nepusz T (2006) The igraph software package for complex network research. InterJournal, Complex Systems 1695.

- Uddin S, Hossain L, Abbasi A, Rasmussen K (2012) Trend and efficiency analysis of co-authorship network. Scientometrics 90: 687–699.
- View ArticleGoogle Scholar

View ArticleGoogle Scholar
- Frigotto ML, Riccaboni M (2011) A few special cases: scientific creativity and network dynamics in the field of rare diseases. Scientometrics 89: 397–420.
View ArticleGoogle Scholar

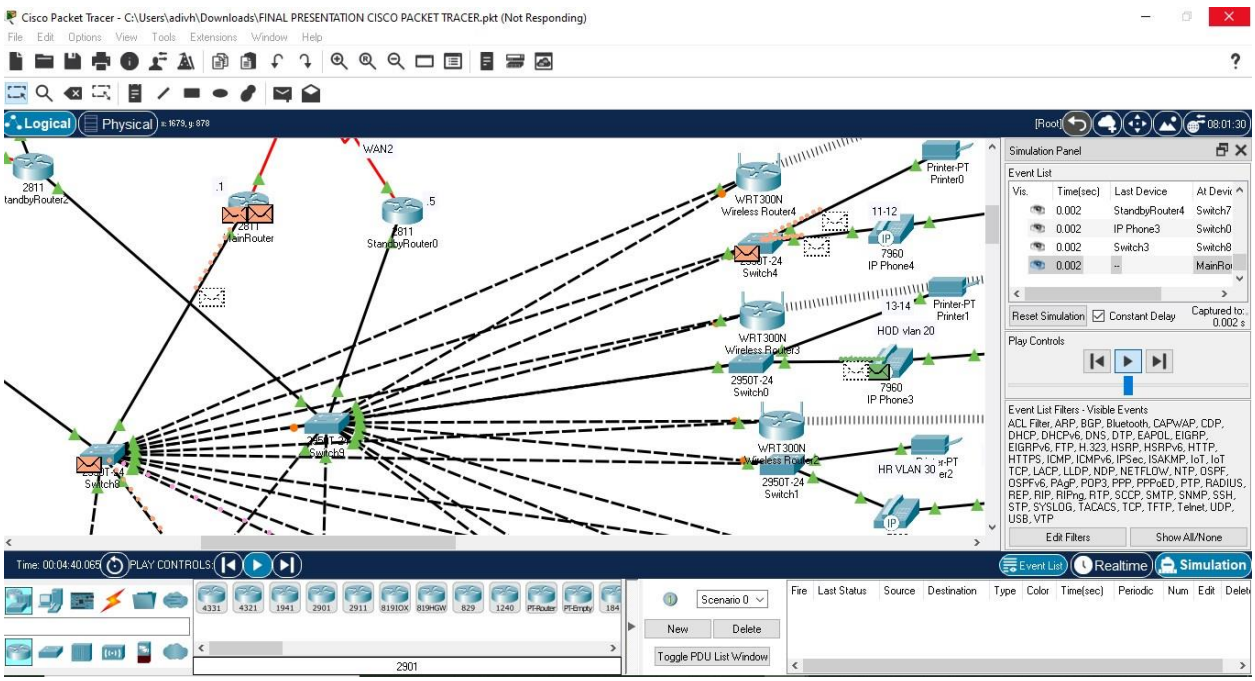
- Simonton DK (1995) Foresight in insight? A Darwinian answer. In: Sternberg RJ, Davidson JE, editors. The nature of insight. Cambridge, MA: MIT Press. pp. 465–494.

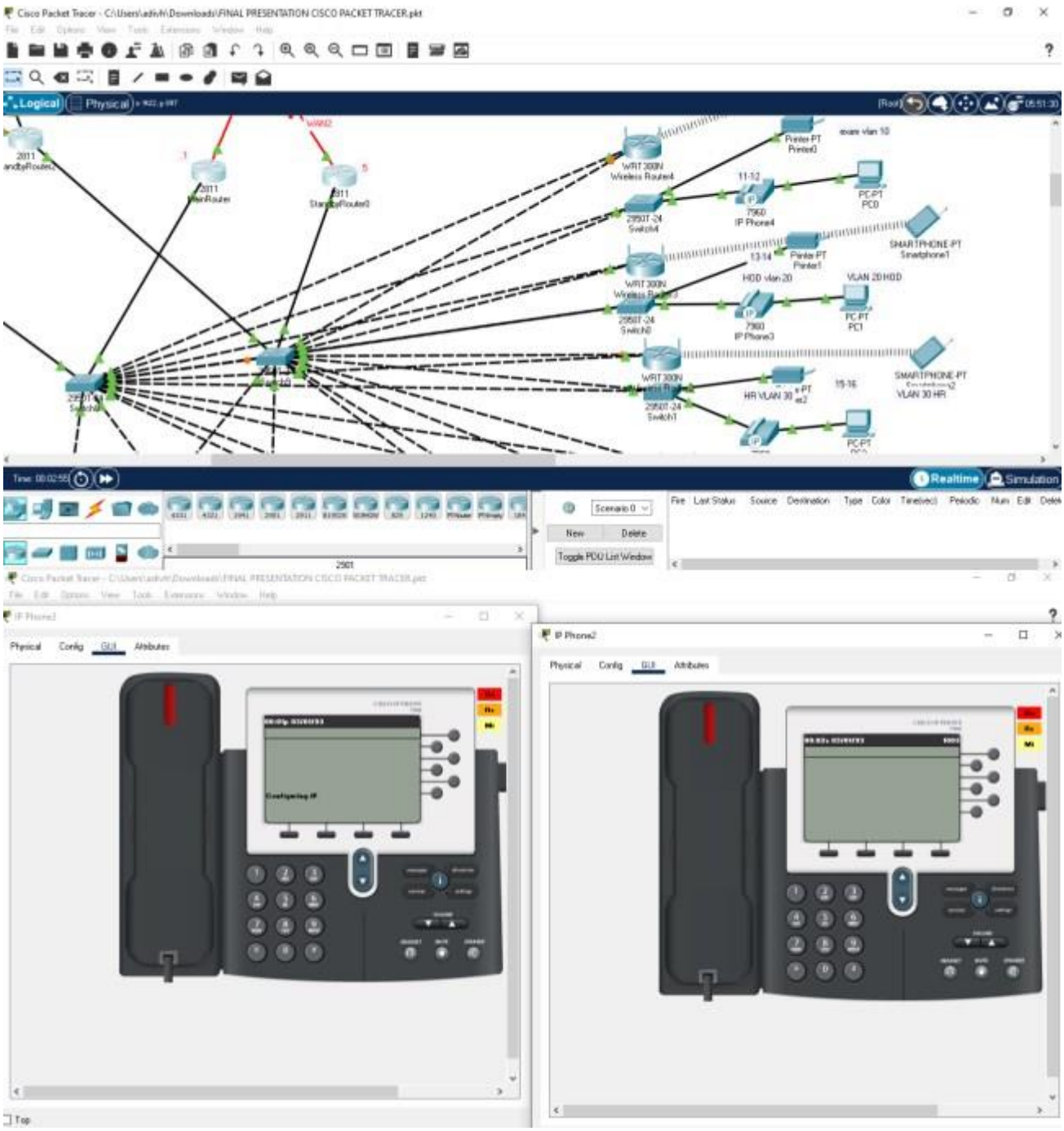
- Yin L-c, Kretschmer H, Hanneman RA, Liu Z-y (2006) Connection and stratification in research collaboration: An analysis of the COLLNET network. Information Processing & Management 42: 1599–1613.
View ArticleGoogle Scholar

- Kessler MM (1963) Bibliographic coupling between scientific papers. American documentation 14: 10–25.
View ArticleGoogle Scholar

- Sun XL, Kaur J, Milojevic S, Flammini A, Menczer F (2013) Social Dynamics of Science. Scientific Reports 3..

Appendices


Cisco Packet Tracer - C:\Users\adivh\Downloads\FINAL PRESENTATION CISCO PACKET TRACER.pkt (Not Responding)
File Edit Options View Tools Extensions Window Help
Logical
Physical
WAN2
MainRouter
StandbyRouter0
WRT300N
Wireless Router4
Printer-PT
Printer0
IP Phone4
Switch4
Printer-PT
Printer1
HOD vlan 20
Switch0
IP Phone3
Switch1
HR VLAN 30
Simulation Panel
Event List
Vis. Time(sec) Last Device At Devic
0.002 StandbyRouter4 Switch7
0.002 IP Phone3 Switch0
0.002 Switch3 Switch8
0.002 -- MainRou
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT_IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:04:40.065
PLAY CONTROLS:
Event List
Realtime
Simulation
2901
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit


Cisco Packet Tracer - C:\Users\adivh\Downloads\FINAL PRESENTATION CISCO PACKET TRACER.pkt
Logical
Physical
Realtime
Simulation
IP Phone2
Physical
Config
GUI
Attributes