BAHRIA UNIVERSITY KARACHI CAMPUS

Project report

UNIVERSITY NETWORKING MODEL

Enrollment #	Name
02-134211-069	Raffay Ahmed Khan
02-134211-077	Furqan Zaka Ud Din
02-134211-087	Absar Azeem

DEPARTMENT OF COMPUTER

SCIENCE BAHRIA UNIVERSITY,

KARACHI, PAKISTANFALL 2022

TABLE OF CONTENTS

CHAPTERS

Table of Contents

UNIVERSITY NETWORKING MODEL

Acknowledgement

I would like to take this opportunity to express my deepest gratitude and appreciation to my course teacher for his dedication and hard work in ensuring that we have a great learning experience. He has been an invaluable source of knowledge, guidance and support throughout this course, and their patience and encouragement have been immensely helpful. I am very grateful for all the time and effort they have invested in making this course a great success. Thank you!

Abstract

The importance of understanding the network requirements and constraints when creating a campus-networking model. The design of the network architecture, including the placement of network devices and the use of different network protocols and technologies. The importance of planning for network security and access control. The need for network management and monitoring tools to ensure the network is functioning properly.

The literature review on campus networking models, including the various research papers that have been published on the topic.

The aim and objectives of a campus networking model, including designing and implementing a scalable, secure, and high-performance network that is compliant with regulatory and compliance requirements, easy to manage and monitor, and able to support cloud-based services and technologies and IoT.

In summary, the campus networking model is a complex and multi-faceted topic that requires a thorough understanding of the network requirements and constraints, proper design and implementation, and consideration of various factors such as scalability, security, performance, compliance, management and monitoring, environmental aspects, and IoT and cloud-based services and technologies.

LIST OF FIGURES

LIST OF SYMBOLS / ABBREVIATIONS

LAN	Local Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
IoT	Internet of Things
Gbps	billions of bits per second
VLAN	virtual local area network
VPN	Virtual private network
IEEE	Institute of Electrical and Electronics Engineers
OSI	Open Systems Interconnection
IP	Internet Protocol address
DHCP	Dynamic Host Configuration Protocol
RIP	Routing Information Protocol
PC	Personal Computer
ISP	internet service provider
CAN	controller area network
PoE	Power over Ethernet

CHAPTER 1

Introduction

University Networking is a group of interconnected Local Area Networks (LAN) within a limited geographical area like Schools, universities, military bases, organizational University s and corporate buildings, etc. A University Network is larger than Local Area Network but smaller than Metropolitan Area Network (MAN) and Wide Area Network (WAN).

A university networking system is a system of interconnected computers and devices that are used to facilitate communication, collaboration, and other activities among students, faculty, and staff. This system enables users to access resources such as course materials, library databases, and administrative services. It also provides the infrastructure for connecting to the internet, allowing users to send and receive emails, chat, and access websites. The goal of a university networking system is to create an efficient and secure environment for students, faculty, and staff to work in. Therefore, network designers typically tend to design the University portion of the enterprise network to be optimized for the fastest functional architecture that runs on high- speed physical infrastructure (1/10/40/100 Gbps). Moreover, enterprises can also have morethan one University block within the same geographic location, depending on the number ofusers within the location, business goals, and business nature.

Local area network (LAN) is a network that is controlled by a single authority. University network is a set of virtual local area networks, which are virtually divided for increasing the performance of network and increases University network management with security. When the term “Internet of Things” was first announced, the primary question might have been what is considered as “Things”.

Smart University Network Design is the proposed method to design University network by integrating IoT device with networking device, to facilitate different activities in university network. This design includes Hierarchical Network Design as a hierarchical design is used to cluster devices into multiple networks layers. The networks are structured in a layered approach, those are Core layer, distribution layer and access layer. Each layer has its own functionalities that are Core layer: connect distribution layer to the internet Distribution layer: Interconnects the smaller local networks, Access layer: Provides connectivity for network hosts, smart things, and end devices.

To design Smart University Network Design I used cisco packet tracer simulator software.

Background

When creating a campus networking model, it is important to have a clear understanding of the network requirements and constraints. This includes the number of buildings and users, the types of devices and applications that will be used on the network, and any regulatory or compliance requirements that must be met.

Next, we will need to design the network architecture, including the placement of network devices such as switches, routers, and firewalls. This will also involve determining the appropriate network protocols and technologies to use, such as IPv4 or IPv6 and VLANs.

It is also important to plan for network security and access control, including the use of firewalls, VPNs, and other security technologies to protect against threats such as hacking and malware.

We will also need to consider network management and monitoring, including the use of tools for monitoring network performance and troubleshooting issues as they arise.

Literature Review

- "Designing and Implementing a Campus Network" by S. V. Raghavan and R. K. S. Rajagopalan (2009) - This paper presents a case study of the design and implementation of a campus network at an Indian engineering college, including the network architecture and security measures.
- "IPv6-based Campus Network Design and Implementation" by Y. L. Chen and W. J. Li (2011) - This paper presents a case study of the design and implementation of an

IPv6-based campus network at a Chinese university, including the migration from IPv4 to IPv6.

- "Software-Defined Campus Networking" by J. S. Kang and J. H. Song (2015) - This paper presents an overview of the use of software-defined networking (SDN) in campus networks, including the benefits and challenges of implementing SDN.
- "Campus Networking in the Cloud Era" by K. R. Chiang and C. C. Tsai (2017) - This paper presents an overview of the use of cloud-based services and technologies in campus networks, including the benefits and challenges of implementing cloud-based networking.

Problem Statement

Problem statements on campus networking models can vary depending on the specific context and requirements of the network. However, here are a few examples of common problem statements that may be encountered when designing and implementing a campus network:

- Scalability: As the number of users and devices on the network increases, the network may become overwhelmed and unable to handle the traffic.
- Security: With the increasing number of threats such as hacking and malware, it is important to ensure that the network is secure and protected against these threats.
- Performance: As more applications and services are used on the network, it is important to ensure that the network is able to provide the necessary performance and quality of service for these applications and services.
- IPv6 migration: As the IPv4 address protocol is depleting it is important to migrate to IPv6 protocol.
- Managing and monitoring: As the network grows, it becomes more difficult to manage and monitor, making it important to have the necessary tools and processes in place to ensure that the network is running smoothly.

- Compliance: With the increase of regulations and compliance requirements, it is important to ensure that the network is compliant with these requirements to avoid penalties or fines.
- Wireless networking: As the number of mobile devices increases, it becomes important to provide wireless connectivity for these devices, while maintaining the same level of security and performance as wired devices.
- Cloud-based networking: As more services and applications are moved to the cloud, it becomes important to ensure that the network is able to support cloud-based services and technologies, while maintaining the same level of security and performance as traditional on-premises services.
- IoT networking: As the number of IoT devices increases, it becomes important to ensure that these devices are integrated with the existing network and that the network is able to handle the increased traffic and security challenges associated with IoT.

These problem statements are not exhaustive but are some of the common challenges that might be faced when designing and implementing a campus network

Aim and Objectives

The aim and objectives of a campus networking model will depend on the specific context and requirements of the network. However, here are a few examples of common aims and objectives that may be set when designing and implementing a campus network:

- To design and implement a scalable, secure, and high-performance campus network that can handle an increasing number of users and devices.
- To ensure that the network is compliant with all relevant regulatory and compliance requirements.
- To design and implement an IPv6-based campus network, to ensure the sustainability of internet addresses.

- To design and implement a network that is easy to manage and monitor, with the necessary tools and processes in place to ensure that the network is running smoothly.
- To design and implement a wireless network that can provide the same level of security and performance as wired devices, for mobile devices.
- To design and implement a network that can support cloud-based services and technologies, while maintaining the same level of security and performance as traditional on-premises services.
- To design and implement a network that can handle the increased traffic and security challenges associated with IoT and integrating IoT devices with the existing network.
- To use Software-Defined Networking and Network Function Virtualization to increase the flexibility and programmability of the network.
- It is important to note that these aims and objectives should be specific, measurable, attainable, relevant, and time-bound (SMART) to ensure they are achievable.

Scope

Today's smart University network is built on a foundation of connectivity designed to increase productivity, efficiency, learning, and safety. Reliable high speed fiber rings, inside plant fiber, power over Ethernet and powered fiber create a solid infrastructure for Wi-Fi, cellular and IoT network coverage inside and out. Converged wired and wireless management solutions simplify support, enhance network performance, and make everything easier to use.

More than a vital IT asset, the University network and all it enables reflects the vision and values of the organization. Whether you're building a smart university, smart medical University or smart corporate University , Common Scope helps you shape and transform the future.

Environmental aspects

Environmental aspects can play an important role in campus networking models and should be considered when designing and implementing a network. Here are a few examples of environmental aspects that may be relevant:

- Energy efficiency: Network devices such as switches and routers can consume a significant amount of energy, so it is important to consider energy-efficient devices and technologies that can help reduce the energy consumption of the network.
- Recycling and disposal of devices: At the end of their lifecycle, network devices need to be disposed of properly, it is important to consider recycling and disposal options that are environmentally friendly and comply with local regulations.
- Cooling: Network devices generate heat, which needs to be dissipated to ensure proper functioning, it is important to consider cooling options that are energy-efficient and minimize the environmental impact.
- Green design: Green design principles may be used to minimize the environmental impact of the network, for example, by placing network devices in a central location and using optical fibers to transmit data over long distances to reduce energy consumption.
- Carbon footprint: The network infrastructure might generate a carbon footprint, it is important to measure and reduce the carbon footprint of the network.
- Security: As the network infrastructure might be vulnerable to cyber-attacks, it is important to consider the security of the network infrastructure to ensure that they are not used as a point of entry for cyber-attacks.
- Material sourcing: It is important to consider the sourcing of materials used in the construction of network infrastructure, to ensure that they are sustainably sourced and do not contribute to environmental degradation.

It is important to note that these environmental aspects should be considered as part of the overall design and implementation of the network and should be integrated with the other aspects such as security, performance, and cost.

CHAPTER 2

Design and methodology

Components

The component for the creation of University Networking Model is computer or laptop may contain the specifications which includes CPU Speed 2GHz recommended or higher Processor, Memory/RAM: 1GB minimum,2GB or higher Display Properties, Greater than 256 color depth, Size of Hard Disk 60 GB minimum and a NIC Card. The main component which will be used for the creation of the project is the software Cisco Packet Tracer version 7.2 running over the operating system windows 10 64 bit.

For further creation of University Networking Model in cisco packet tracer, the Devices and Configuration addresses used in the creation of the project are briefly described below:

Router

A router is a device that communicates between the internet and the devices in your home that connect to the internet. As its name implies, its “routes” traffic between the devices and the internet.

A typical home has a range of internet connected devices personal computers, tablets, smartphones, printers, thermostats, smart TVs, and more. With your router, these devices form a network. A router directs incoming and outgoing internet traffic on that network in the fastest and most efficient way. The information traveling on your home network could be an email, a movie, or a live feed from your baby cam, each of which takes up varying amounts of bandwidth.

Wireless routers are usually found in homes. They are the hardware devices that Internet service providers use to connect you to their cable or DSL Internet network. A wireless router, also called a Wi-Fi router, combines the networking functions of a wireless access point and a router.

A router connects local networks to other local networks or to the Internet. A wireless access point connects devices to the network wirelessly, using radio frequencies in the 900 MHz and

2.4, 3.6, 5, and 60 GHz frequency bands. The latest wireless routers are based on the IEEE 802.11ac Wave 2 standard, often shortened to Wave 2

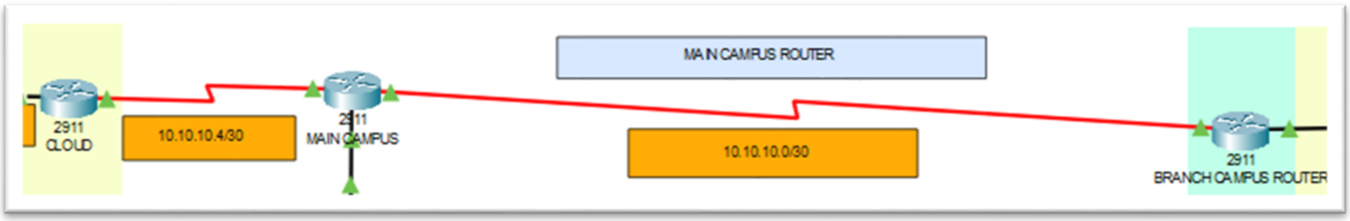


Figure 0-1

Personal computer

In University Networking the personal computer plays a vital role in demonstrating the packet transferred or transmitted through the router switches and clouds interconnected with each other. In the creation of the University Networking Model the types of personal computers used are PCs.

These personal computers are very helpful in the encryption and decryption of the packets that are being transferred with the help of routers connected through switches and Ethernet cables and clouds as, and the packets are being travelling from one University's Campus to another that are at a maximum distance of 11 to 17 km and after that they are being transmitted throughout the whole University having 3 Buildings each.

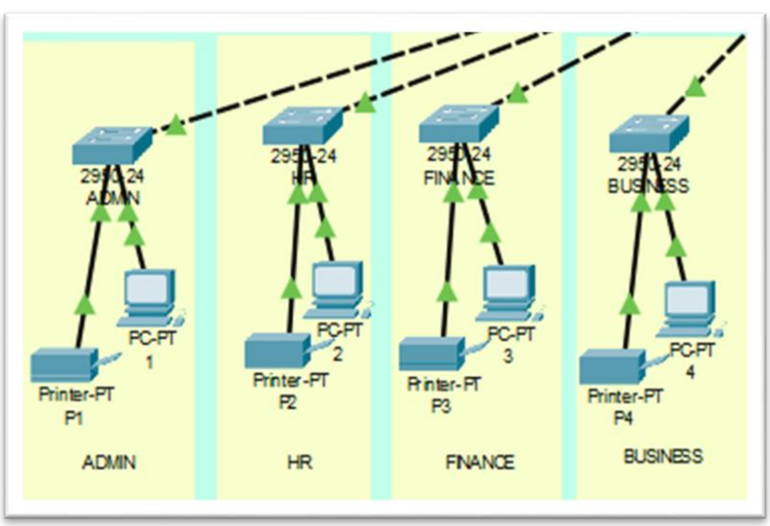


Figure 0-2

Switch

Switches facilitate the sharing of resources by connecting all the devices, including computers, printers, and servers, in a small business network. Thanks to the switch, these connected devices can share information and talk to each other, regardless of where they are in a building or on a university. Building a small business network is not possible without switches to tie devices together.

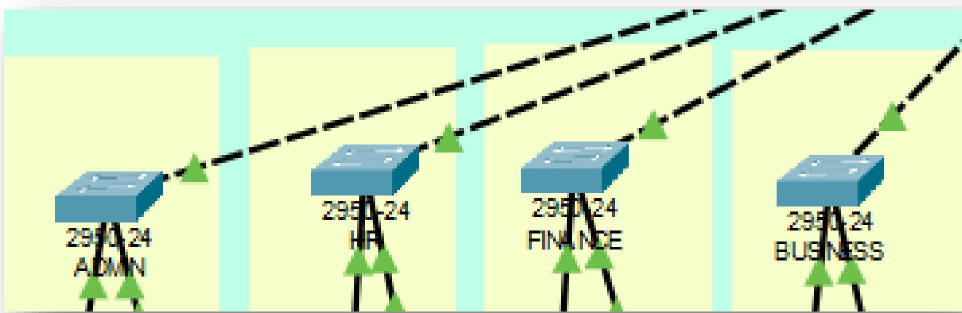


Figure 0-3

IP Multilayer Switches

A multilayer switch is a network device that has the ability to operate at higher layers of the OSI reference model, unlike the Data Link Layer (DLL) traditionally used by switches. A multilayer switch can perform the functions of a switch as well as that of a router at incredibly fast speeds. A switch traditionally inspects frames, while a multilayer switch inspects deeper into the protocol description unit (at packet or even at segment level). Multilayer switches use ASIC hardware circuits to perform routing functions. This differs from typical routers, which reside on a microprocessor and use applications running on it to perform their routing operations.

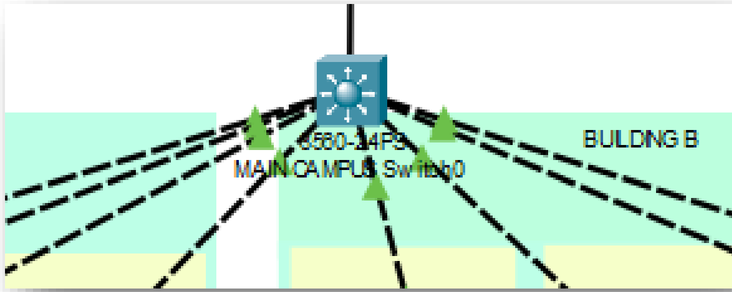


Figure 0-4

IP Address

IP address stands for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information. An IP address allows computers to send and receive data over the internet. Most IP addresses are purely numerical, but as internet usage grows, letters have been added to some addresses.

There are four types of IP addresses: public, private, static, and dynamic. While the public and private are indicative of the location of the network—private being used inside a network while the public is used outside of a network—static and dynamic indicate permanency.

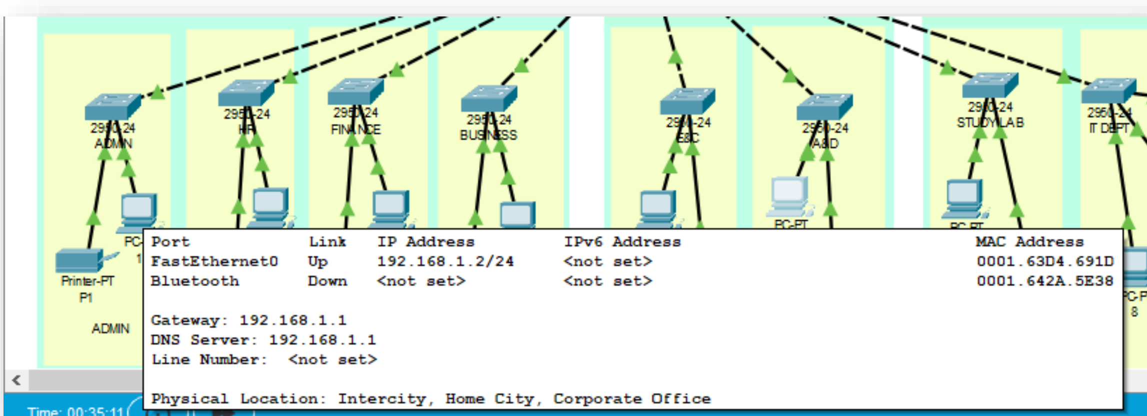


Figure 0-5

Subnet Masks

A subnet mask is like an IP address, but for only internal usage within a network. Routers use subnet masks to route data packets to the right place. Subnet masks are not indicated within data packets traversing the Internet — those packets only indicate the destination IP address, which a router will match with a subnet.

Server

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines, they are considered servers. There are many types of servers, including web servers, mail servers, and virtual servers.

An individual system can provide resources and use them from another system at the same time. This means that a device could be both a server and a client at the same time. Initially, such servers were connected to clients known as terminals that did not do any actual computing. These terminals, referred to as dumb terminals, existed simply to accept input via a keyboard or card reader and to return the results of any computations to a display screen or printer. The actual computing was done on the server.

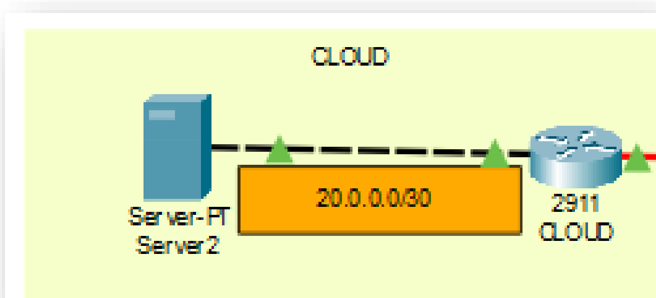
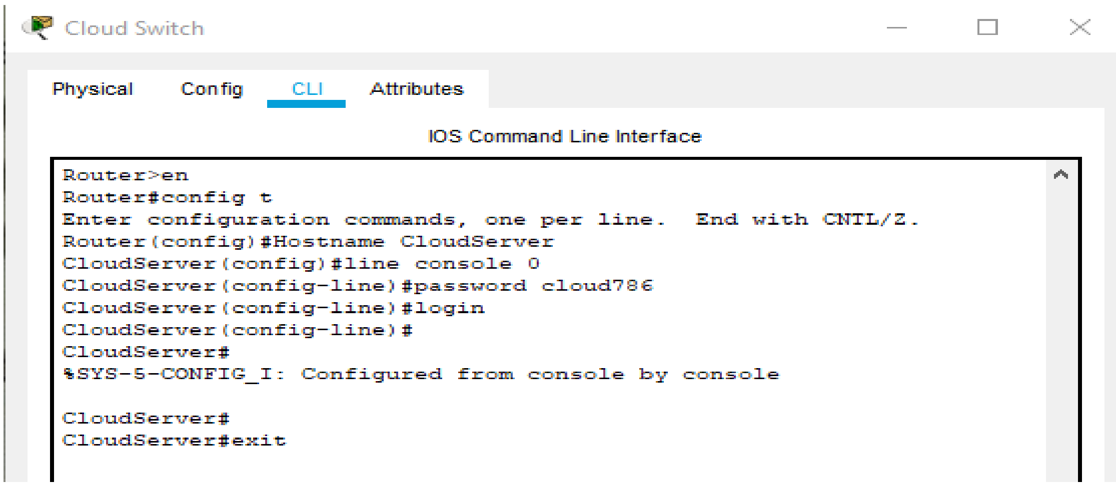
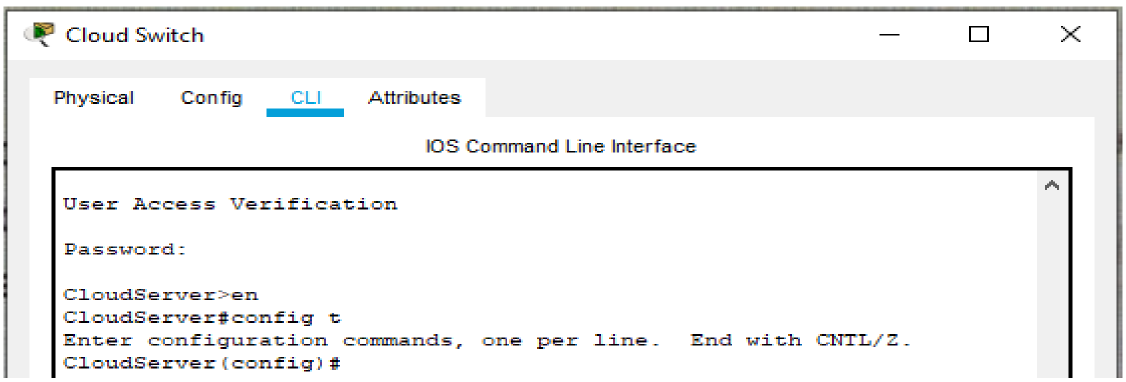


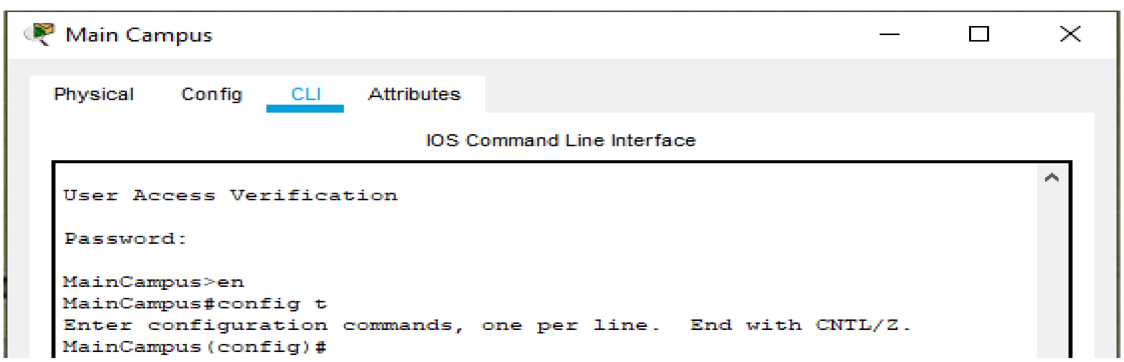
Figure 0-6

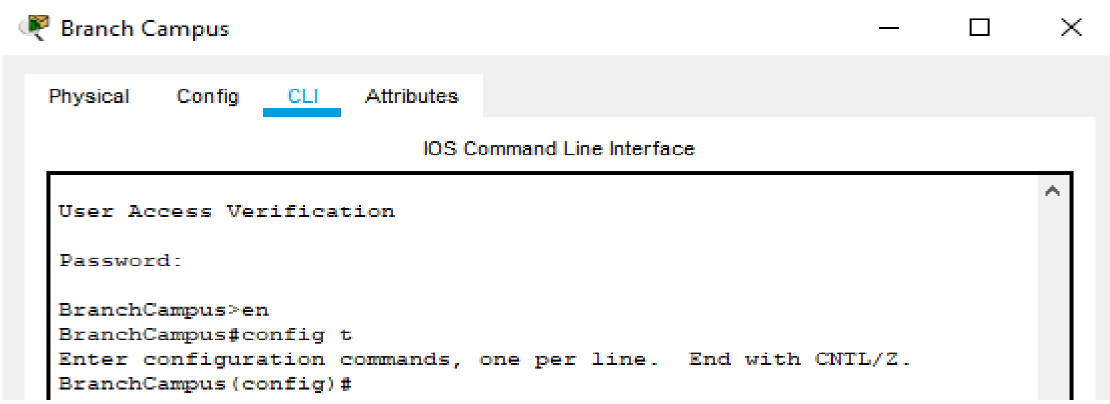
Security system

A security system is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet. A security system can be hardware, software, or both.









Clouds

Cloud networking, or cloud-based networking, gives users access to networking resources through a centralized third-party provider operating inter-connected servers. This involves connecting to a Wide Area Network (WAN) or other internet-based technology and helps to distribute content quickly and securely.

By using a cloud network an organization can deliver content more rapidly, reliably, and securely, without having to bear the costs and difficulties of building and operating its own network. A variety of organizations may find value in using a cloud network, including web content providers, ecommerce businesses, cloud service providers, enterprises using public or private cloud services, or network operators looking to extend their network reach.

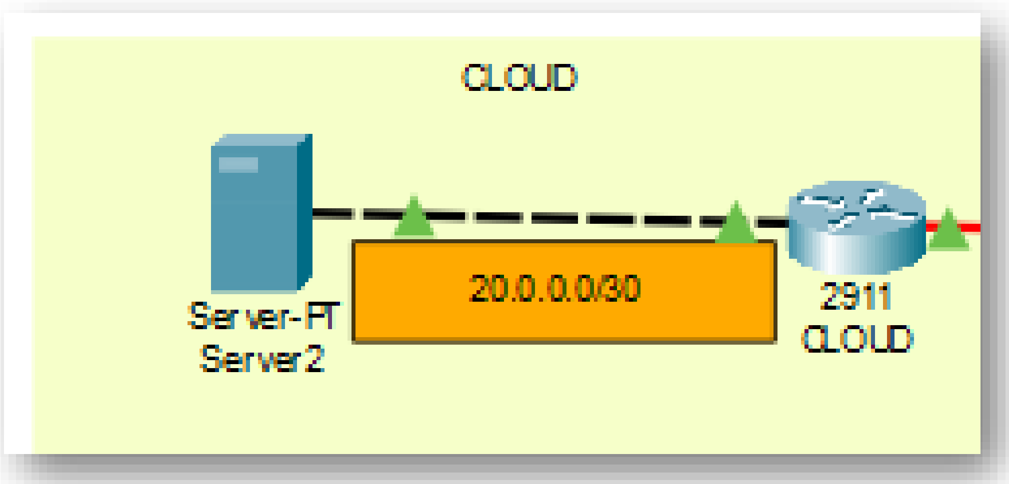
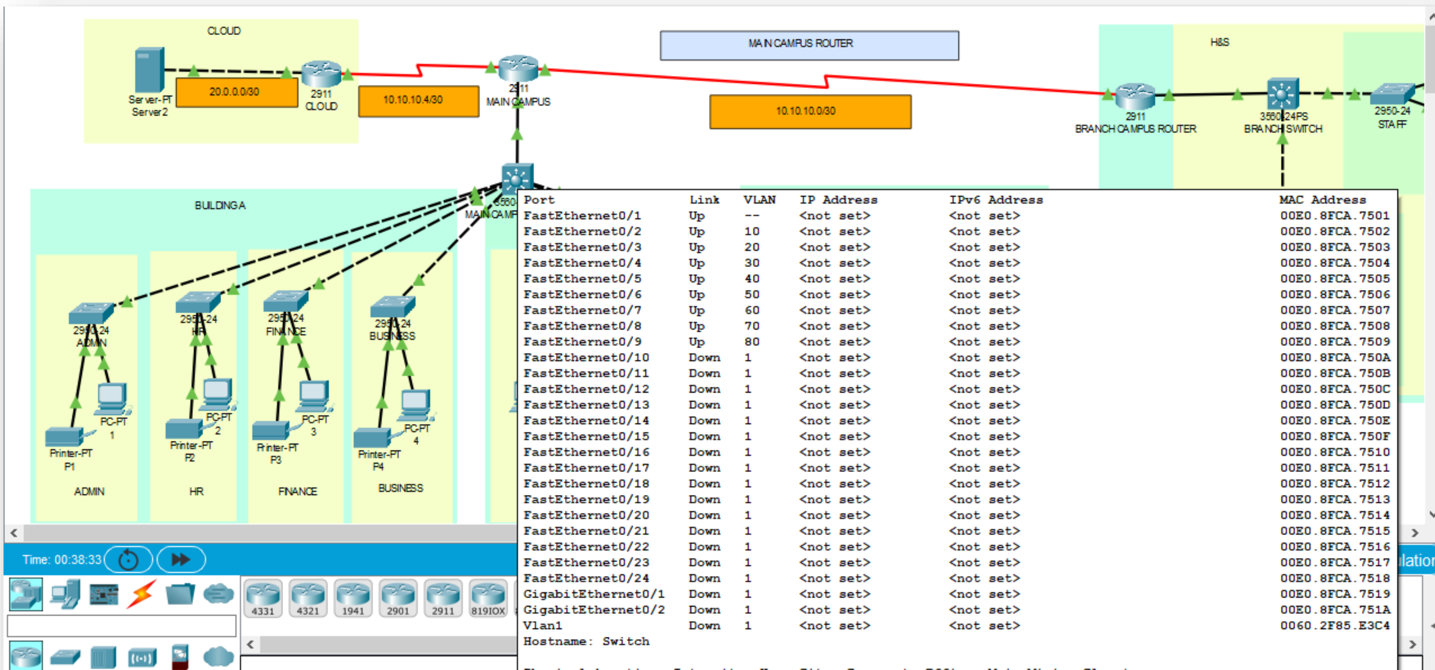
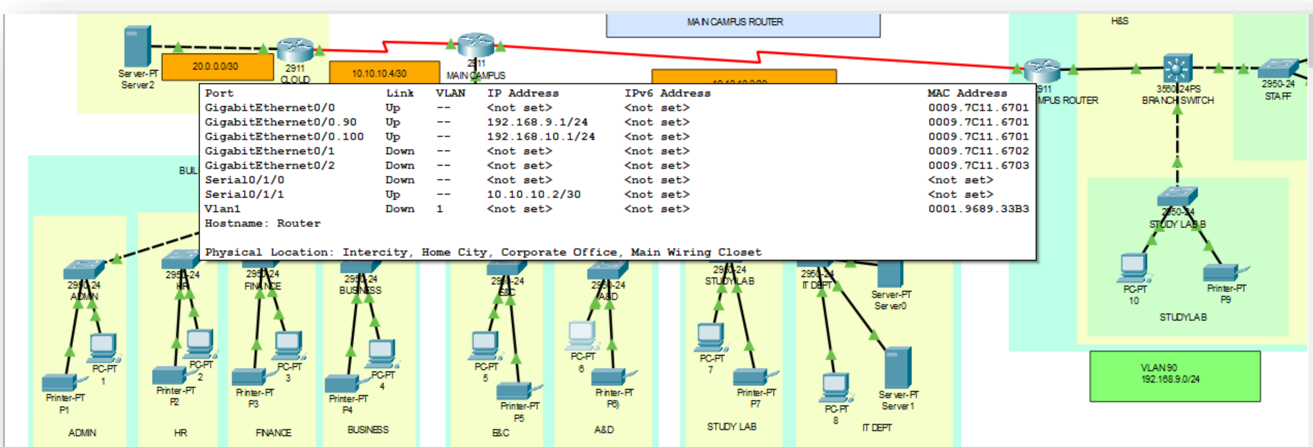


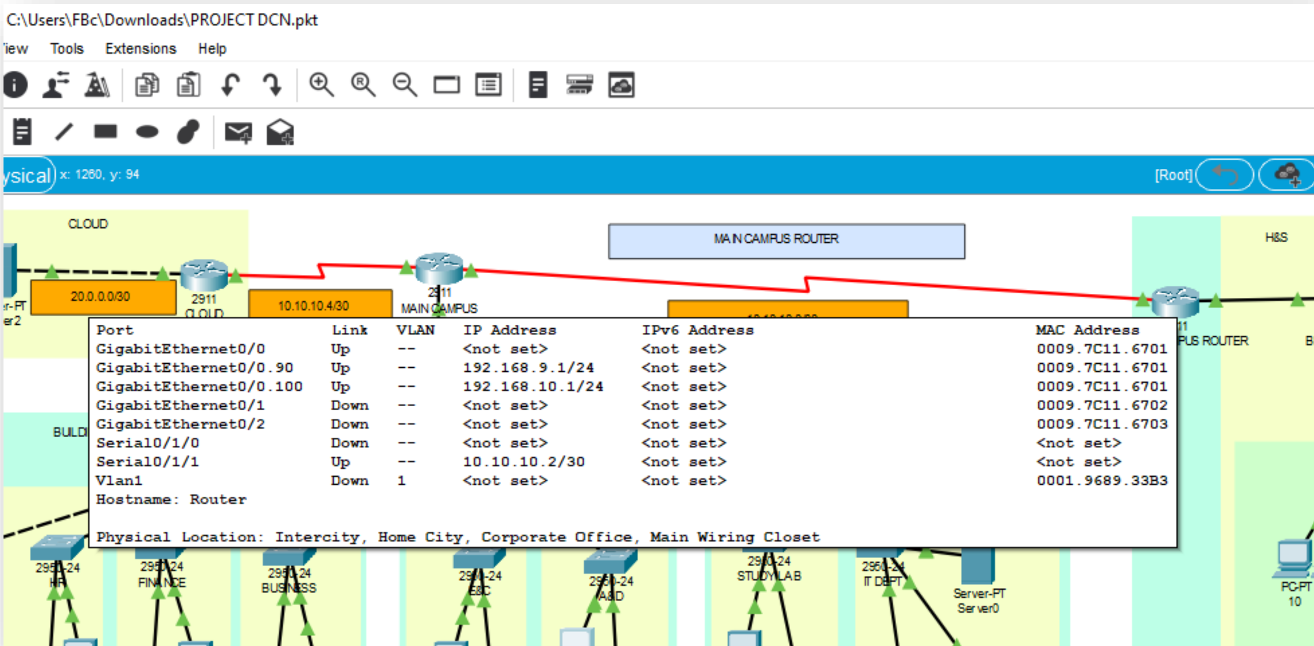
Figure 0-7

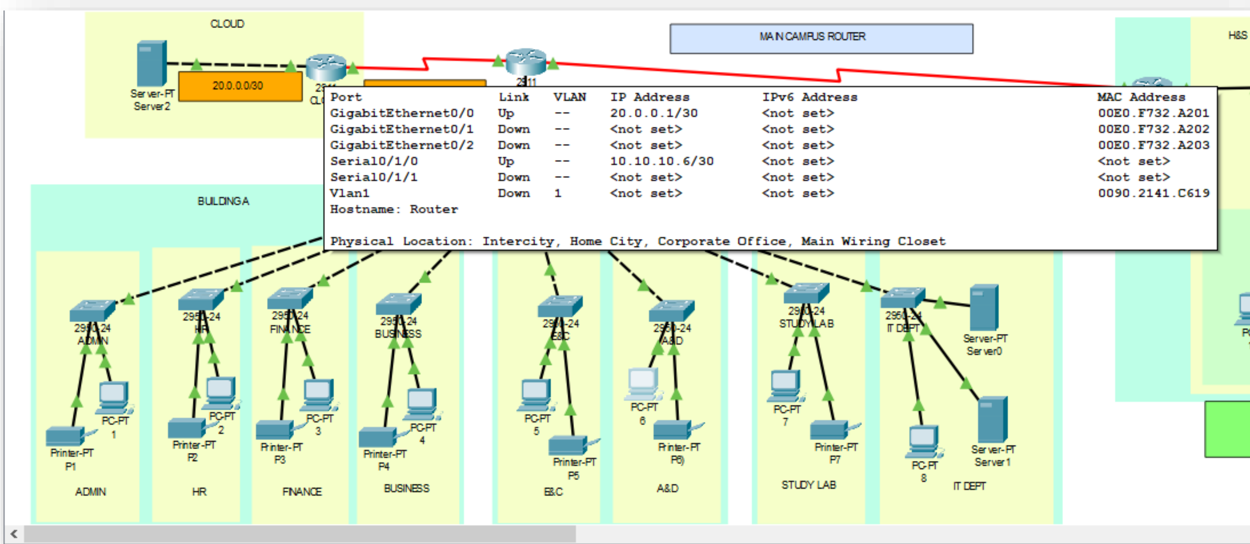
Vlan

By default a Cisco switch creates a VLAN called the Default VLAN 1. All the machines connected to the switch are in the default VLAN 1. It is required to split this by creating one more VLAN called VLAN 2.If you were designing a school it would be nice to use a VLAN for teacher and a VLAN for students. No communication would be possible without the use of router.





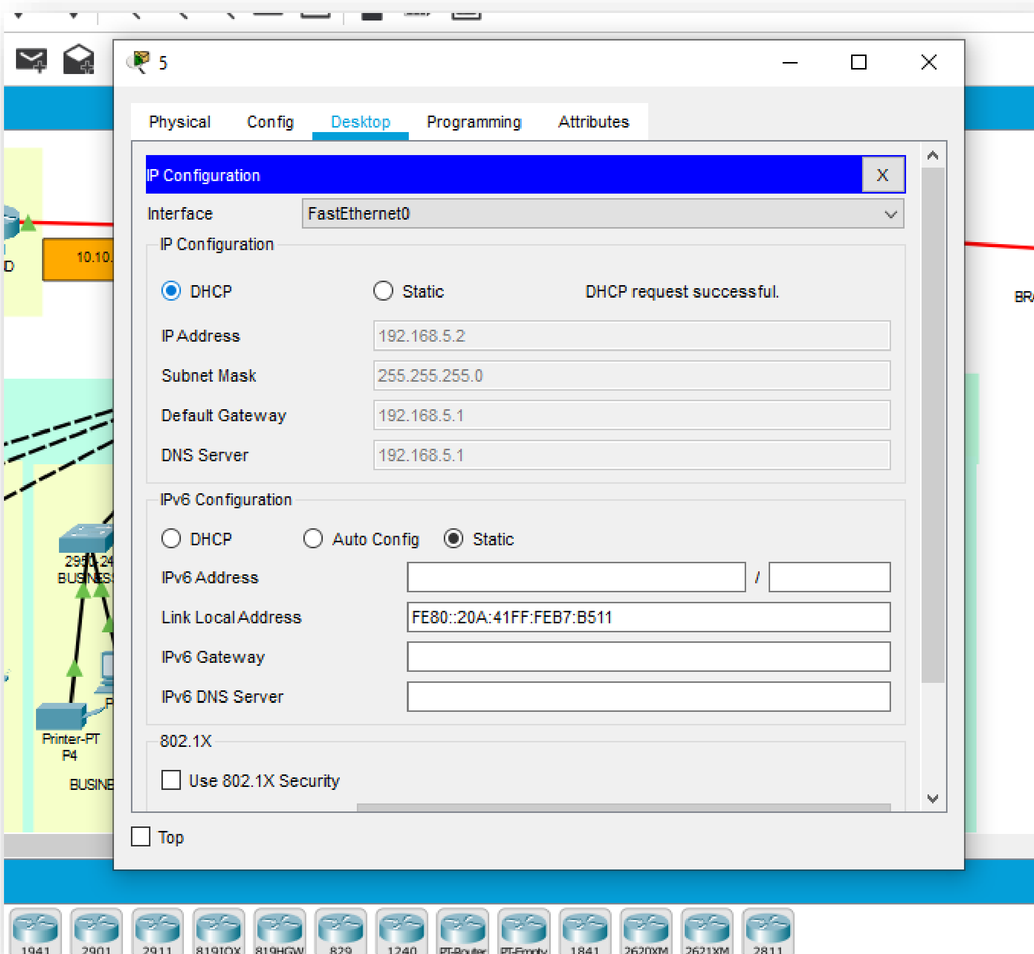

C:\Users\FBc\Downloads\PROJECT DCN.pkt
iew Tools Extensions Help
ysical x: 1260, y: 94
[Root]
CLOUD
MAIN CAMPUS ROUTER
H&S
20.0.0.0/30
2911
CLOUD
10.10.10.4/30
2911
MAIN CAMPUS
Port Link VLAN IP Address IPv6 Address MAC Address
GigabitEthernet0/0 Up -- <not set> <not set> 0009.7C11.6701
GigabitEthernet0/0.90 Up -- 192.168.9.1/24 <not set> 0009.7C11.6701
GigabitEthernet0/0.100 Up -- 192.168.10.1/24 <not set> 0009.7C11.6701
GigabitEthernet0/1 Down -- <not set> <not set> 0009.7C11.6702
GigabitEthernet0/2 Down -- <not set> <not set> 0009.7C11.6703
Serial0/1/0 Down -- <not set> <not set> <not set>
Serial0/1/1 Up -- 10.10.10.2/30 <not set> <not set>
Vlan1 Down 1 <not set> <not set> 0001.9689.33B3
Hostname: Router
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
Server-PT
Server0
PC-PT
10

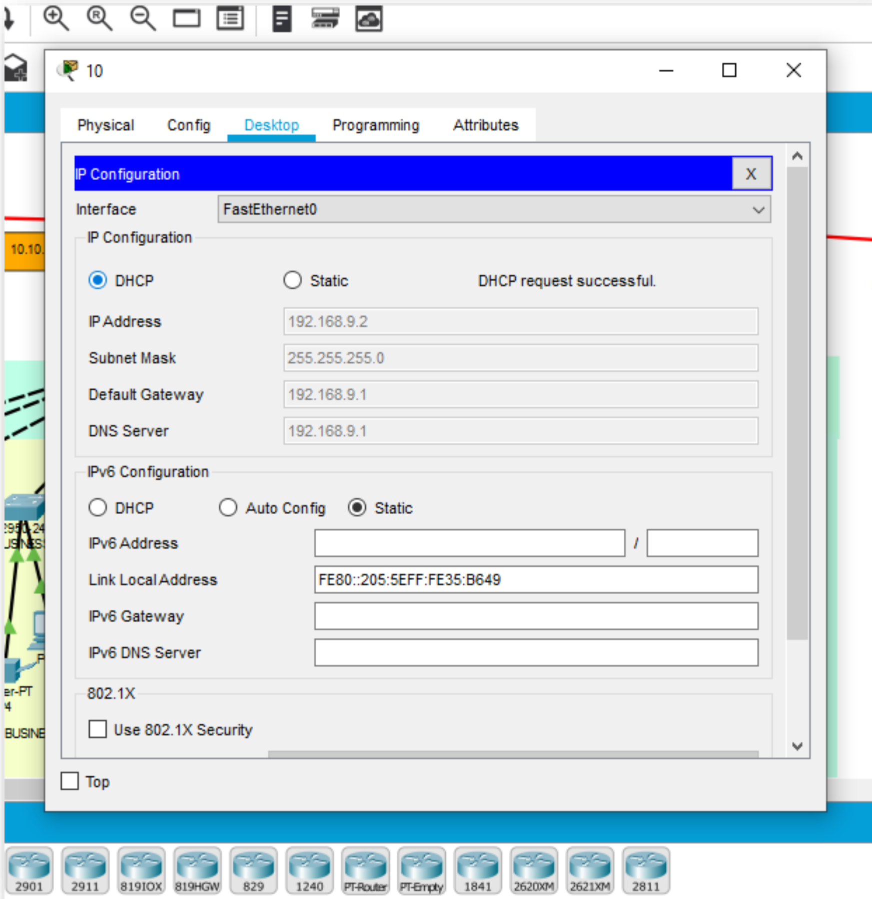

CLOUD
MAIN CAMPUS ROUTER
H&S
Server-PT
Server2
20.0.0.0/30
BULDINGA
Port Link VLAN IP Address IPv6 Address MAC Address
GigabitEthernet0/0 Up -- 20.0.0.1/30 <not set> 00E0.F732.A201
GigabitEthernet0/1 Down -- <not set> <not set> 00E0.F732.A202
GigabitEthernet0/2 Down -- <not set> <not set> 00E0.F732.A203
Serial0/1/0 Up -- 10.10.10.6/30 <not set> <not set>
Serial0/1/1 Down -- <not set> <not set> <not set>
Vlan1 Down 1 <not set> <not set> 0090.2141.C619
Hostname: Router
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
Server-PT
Server0
Server-PT
Server1
ADMIN
HR
FINANCE
BUSINESS
E&C
A&D
STUDY LAB
IT DEPT

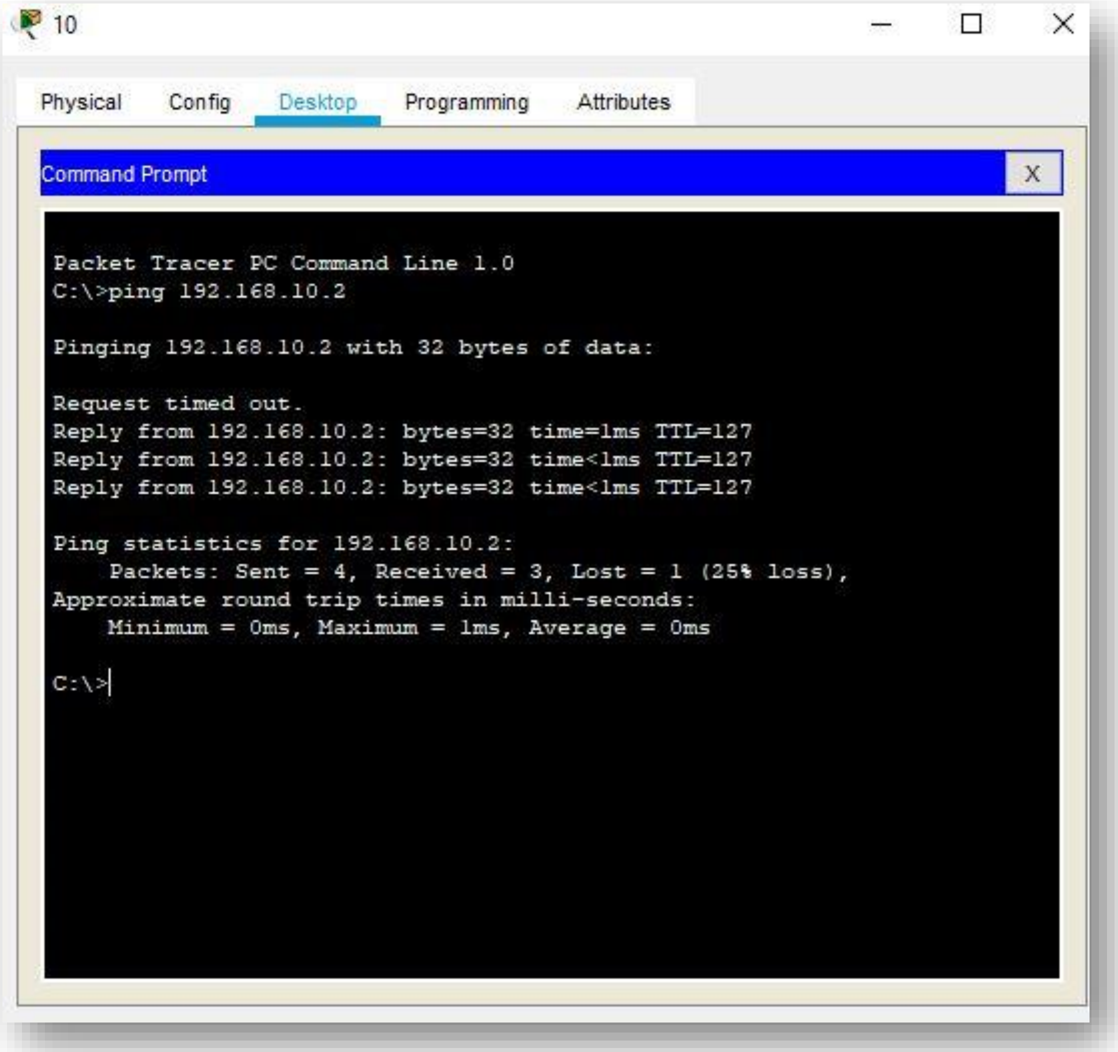
DHCP

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard designed to reduce the complexity of administering address configurations by using a server computer to centrally manage IP addresses and other related configuration details used on your network. Windows 2003 Server provides the DHCP service, which enables the server computer to perform as a DHCP server and configure DHCP-enabled client computers on your network as described in the current DHCP draft standard, RFC 2131.

Before DHCP, we were unable to contact PCs which were in different VLANs




10
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.9.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.9.1
DNS Server
192.168.9.1
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::205:5EFF:FE35:B649
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Top
2901
2911
819IOX
819HGW
829
1240
PT-Router
PT-Empty
1841
2620XM
2621XM
2811


10
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.10.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>

RIP

Routing Information Protocol (RIP) is a true distance-vector routing protocol. RIP sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15 by default, meaning that 16 is deemed unreachable. RIP works well in small networks, but it’s inefficient on large networks with slow WAN links or on networks with a large number of routers installed. It cannot distinguish between high bandwidth link and a lower bandwidth link because delay or bandwidth is not taken under consideration as a metric.

BEFORE RIP

We were unable to connect from 1 campus to another

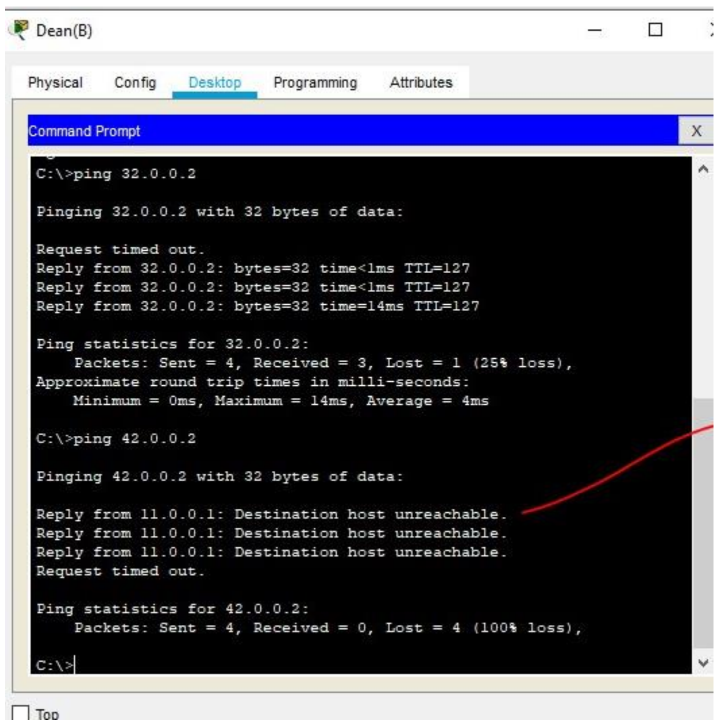
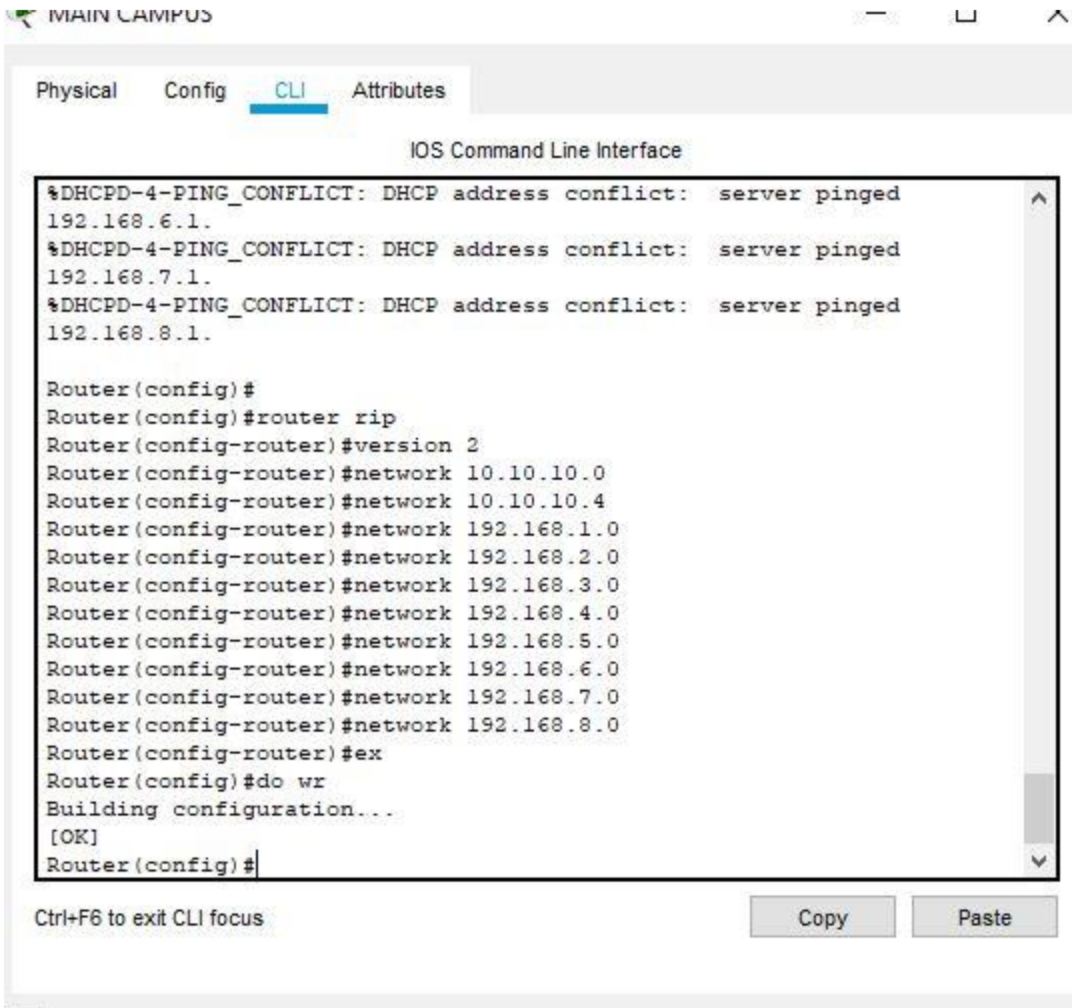


Figure 0-8


MAIN CAMPUS
Physical
Config
CLI
Attributes
IOS Command Line Interface
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.6.1.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.7.1.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.8.1.
Router(config)#
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.10.10.0
Router(config-router)#network 10.10.10.4
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.4.0
Router(config-router)#network 192.168.5.0
Router(config-router)#network 192.168.6.0
Router(config-router)#network 192.168.7.0
Router(config-router)#network 192.168.8.0
Router(config-router)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste

After RIP

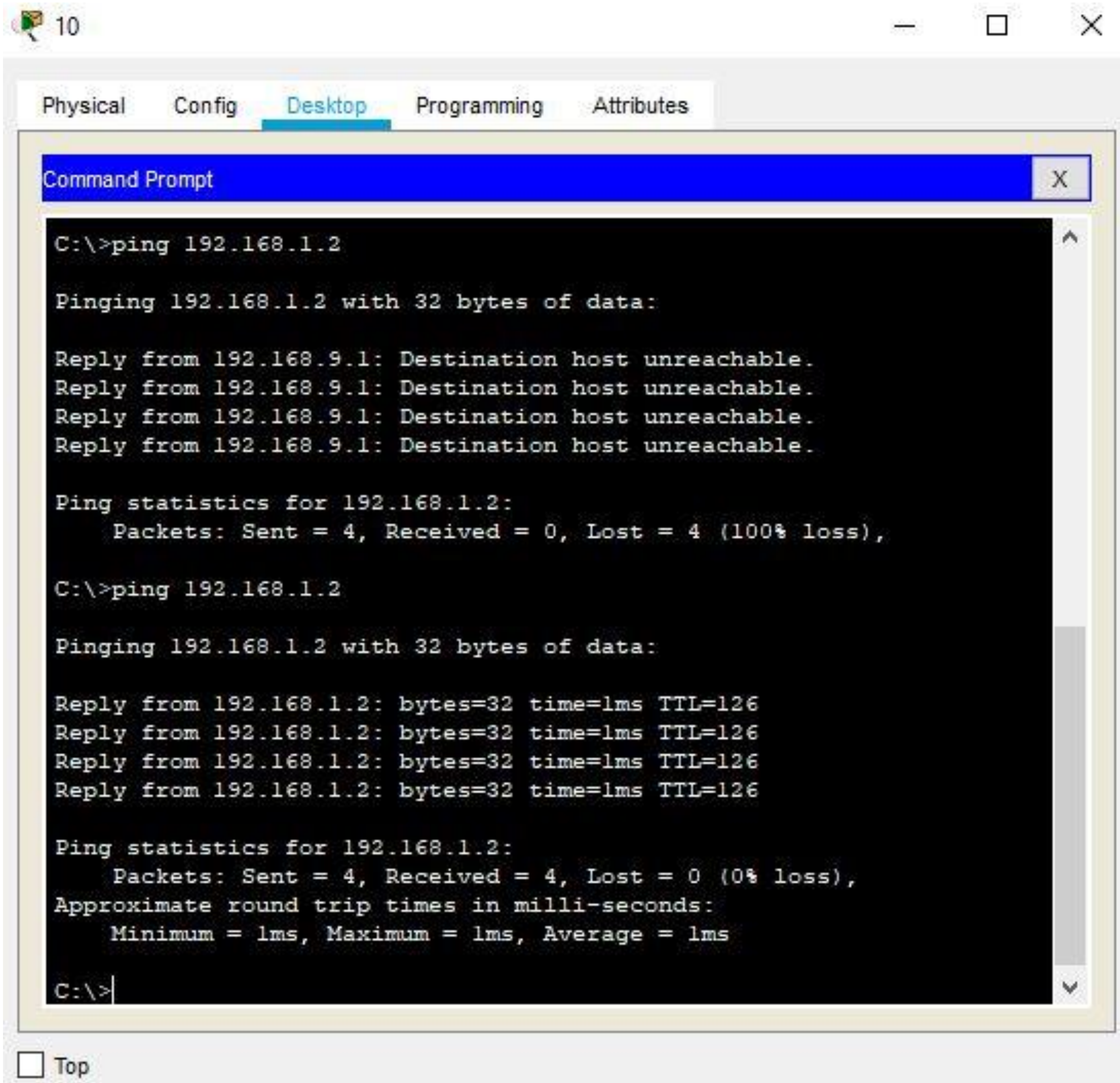


Figure 0-9

Design of the University Model Created in Cisco Packet Tracer

The University networking model that we have projected in cisco packet tracer have 2 Campus of the same organization situated in different areas having approximately the distance of 11km to 17km. these University s are situated in Karachi Pakistan, the first University is situated in Karachi Cantonment and the other is situated in Karsaz Faisal Cantonment.

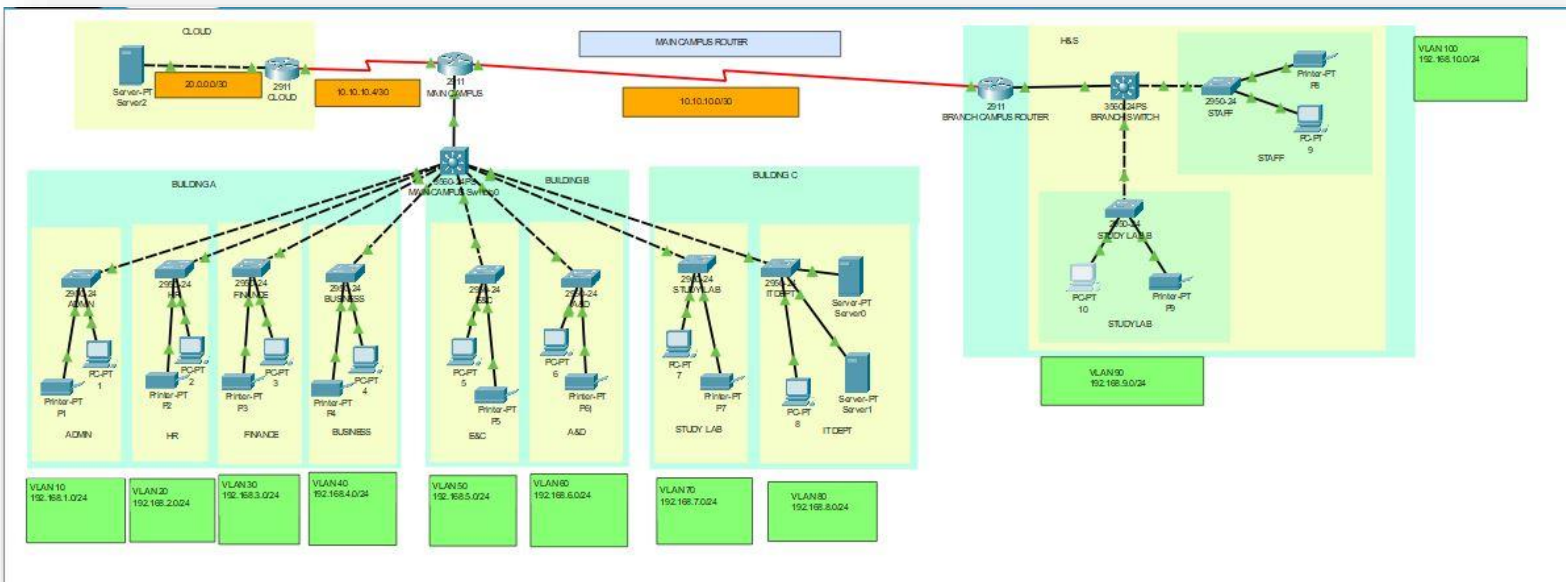


Figure 0-10

CHAPTER 3

Design Implementation

Main Campus

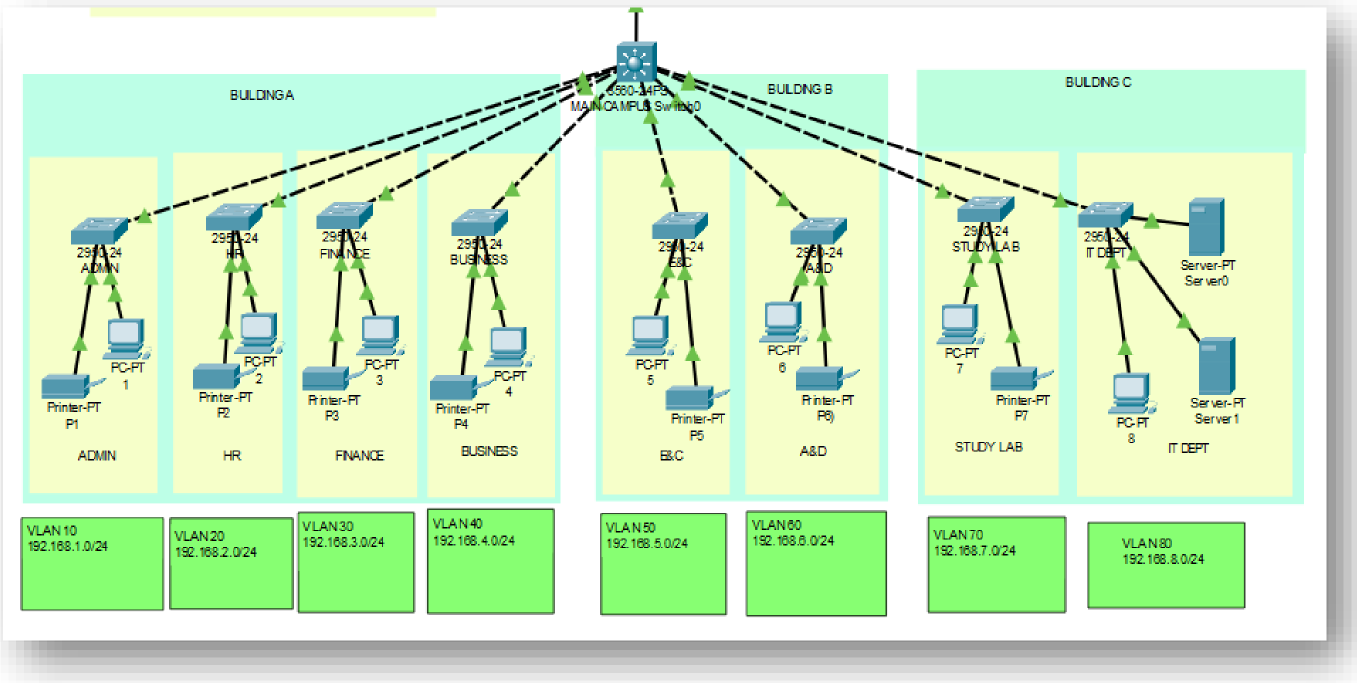


Figure 0-1

Main Campus consists of three Buildings.

In the 1st Building it have 4 Department; admin Dept, HR Dept, Finance Dept, Business Dept which are IP configured and are connected through switches and multilayerswitch devices. We can have a look on the model of 1st Building created in cisco packet tracer.

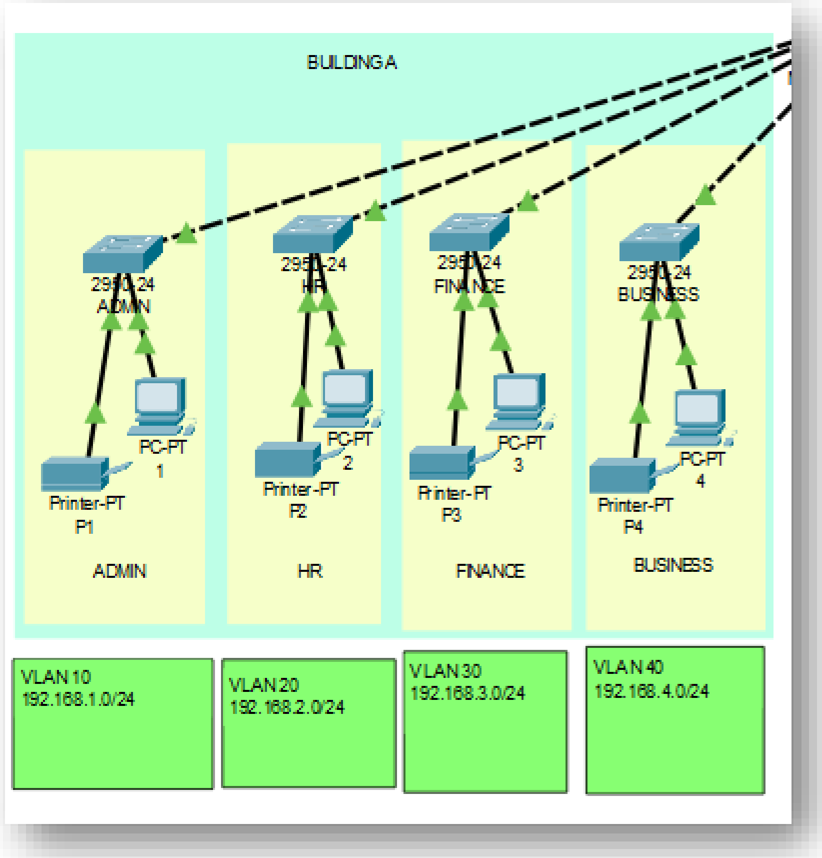

BUILDING A
2950-24
ADMIN
2950-24
HR
2950-24
FINANCE
2950-24
BUSINESS
PC-PT
1
PC-PT
2
PC-PT
3
PC-PT
4
Printer-PT
P1
Printer-PT
P2
Printer-PT
P3
Printer-PT
P4
ADMIN
HR
FINANCE
BUSINESS
VLAN 10
192.168.1.0/24
VLAN 20
192.168.2.0/24
VLAN 30
192.168.3.0/24
VLAN 40
192.168.4.0/24

Figure 0-2

In the 2nd Building it have 2 Department; E&C and A&D which are IP configured and are connected through switches and multilayer switch devices. We can havea look on the model of 2nd Building created in cisco packet tracer.

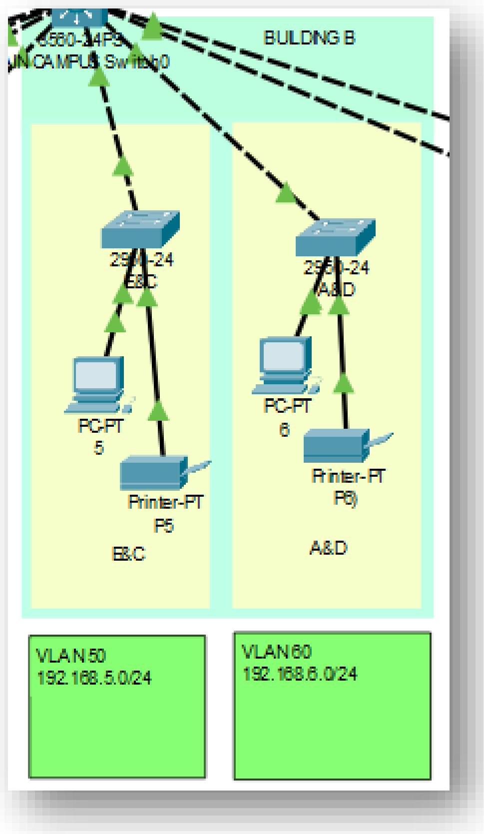


Figure 0-3

In the 3rd Building it have 2 Department; studylab Dept, IT Dept which are IP configured and are connected through switches and multilayer switch devices. We can havea look on the model of 3rd Building created in cisco packet tracer.

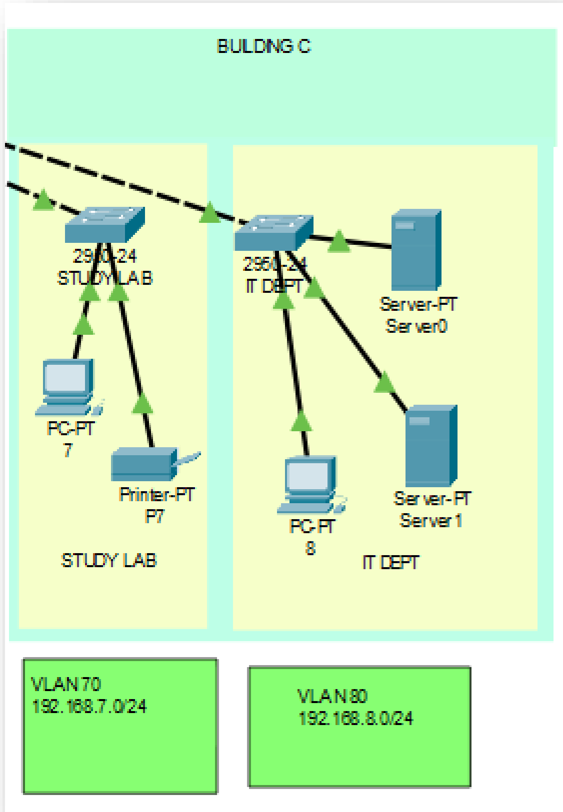


Figure 0-4

The Main Campus Also have a cloud server, where it can save student records, Fee Records, Faculty Records which is IP configured and are connected through Routers. We can have a look on the model of Cloud Server created in cisco packet tracer.

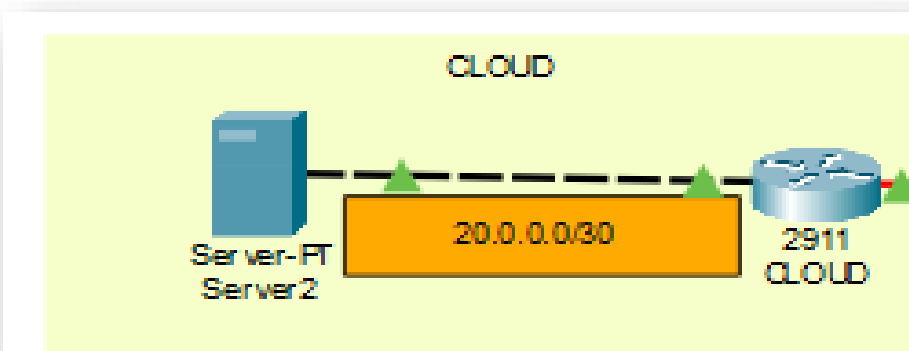


Figure 0-5

Now the main and the most important thing which connects these two University's Campuses to communicate and transmit packets with each other, is came in to being with the help of routers, wireless routers, clouds, servers, firewalls, tablets, multilayer and core switches which connects these two University's Campuses with each other to transmit their packets which are in form of confidential messages and important documents. We can have a look at the structure that how they are connected with each other after being configured on IP and subnet masks.

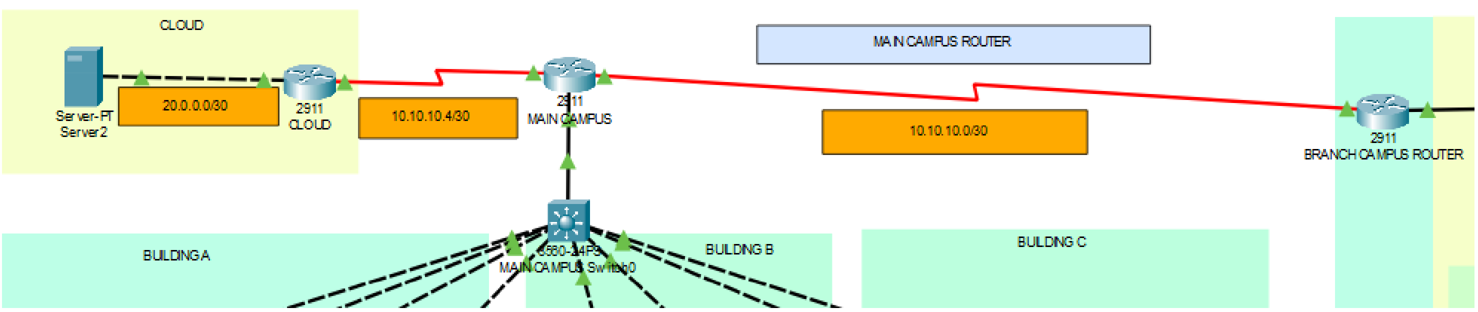


Figure 0-6

Branch Campus

Branch Campus consists of 2 Departments; DPT Dept, Bio-Tech Dept which are IP configured and are connected through switches and multilayer switch devices. We can have a look on the model of Branch Campus created in cisco packet tracer.

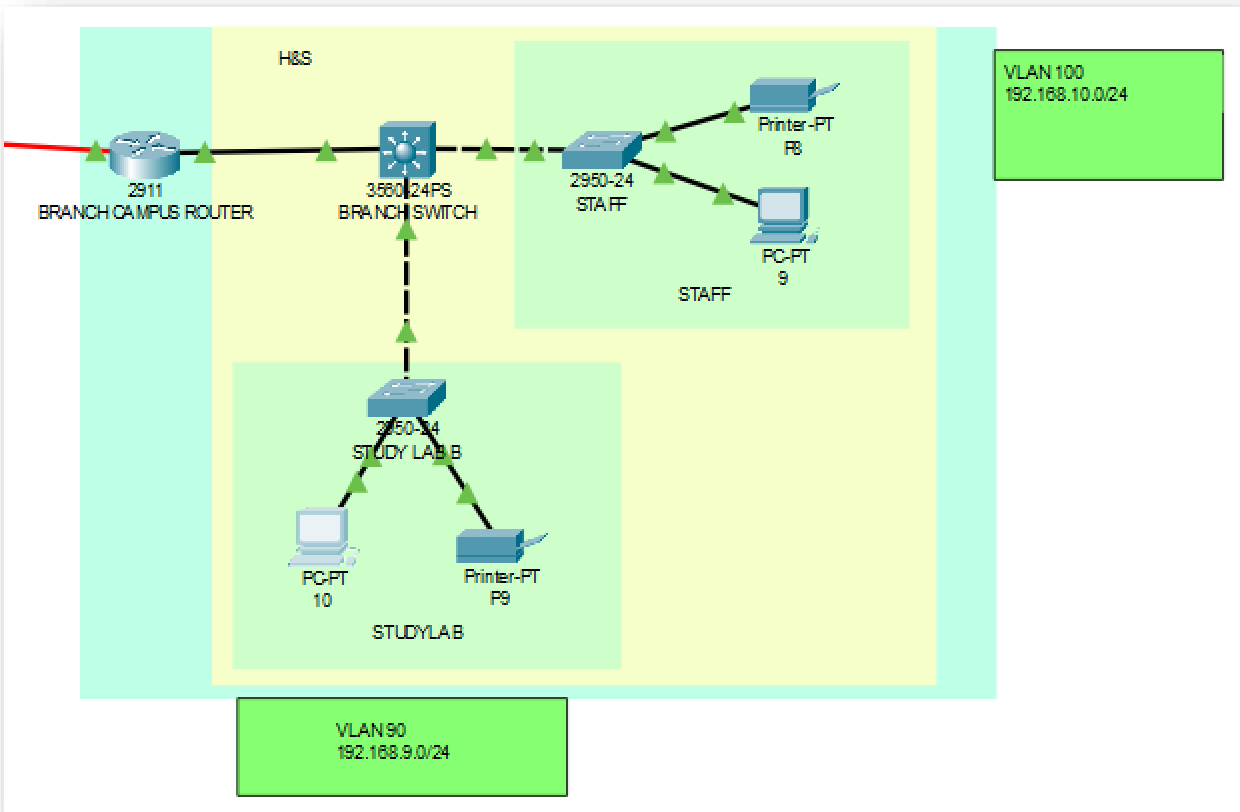


Figure 0-7

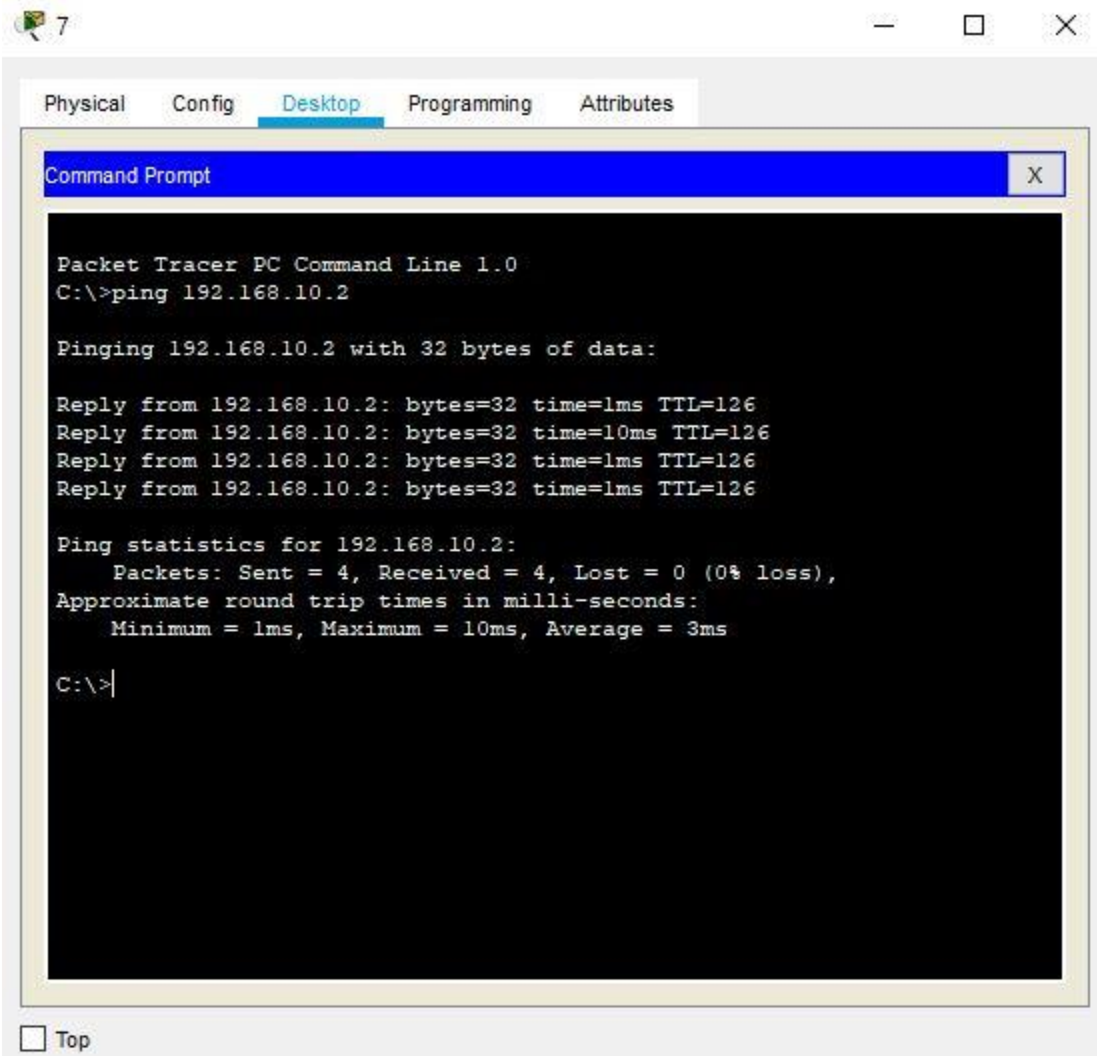
CHAPTER 4

Results and Discussion

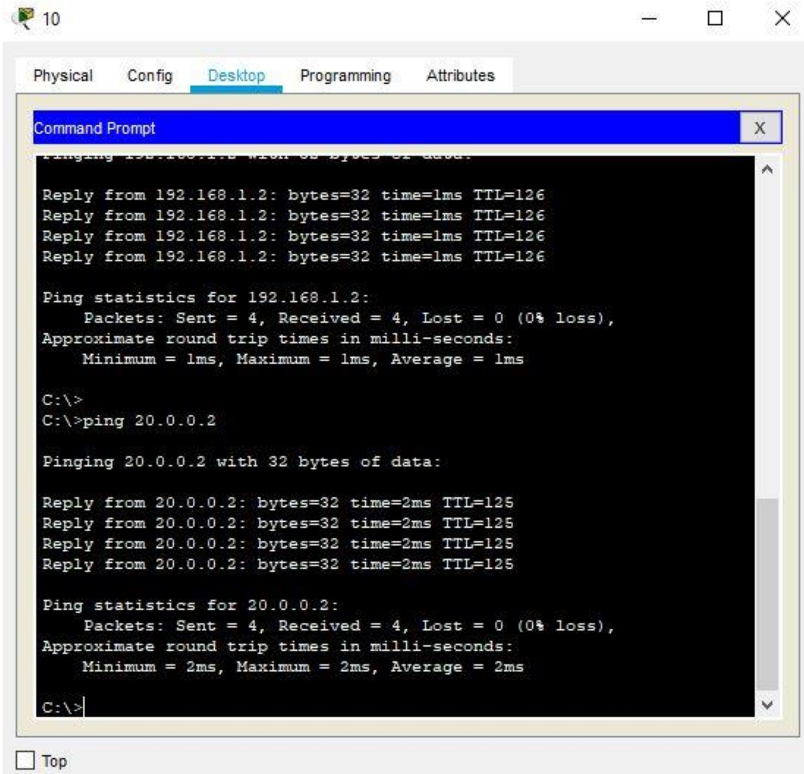
Result

PC:

PC ping from 1 campus to another



From 1 Building to Another:



Discussion

Advantages

- Communication throughout the University s takes place over Wide Area Network (WAN) so data transfer rate between systems is little bit faster than Internet.
- With a little effort and maintenance, the network works well by providing fast data transfer rates with multi-departmental network access. It can be enabled wirelessly, where wiring and cabling costs can be managed. So to work within a University using University Area Network is cost effective in view of performance.
- In University networking, to use some hardware devices of networking such as hub, routers, switches, cable, bridge etc.
- Multiple departments of University are connected to each other in LAN networks. So the message is fired one time, and it transferred to all nodes easily.
- Wireless connections are used to link various offices and buildings with single organization.

- It is capable to transfer huge files with higher speed over entire computer network via internet.
- CAN Network is combination of multiple LAN networks, and it takes form a single entity. In CAN network, firewall or proxy server are used for security purposes from unauthorized access.
- Single ISP (Internet Service Provider) is being used by different client machines.

Conclusion

University networks have unique design criteria that provide greater flexibility to support a wide range of client devices and applications. Wired access, wireless, and PoE devices coexist at the network edge. Mission-critical client applications require high bandwidth, high availability, and security. A tiered University network architecture with fan-out to client devices at the access layer, consolidation of access layer traffic through the aggregation layer, and centralized routing through the network core provides a scalable model for growing the University network over time and accommodating higher traffic volumes and multiple protocols, as required. The full suite of Ruckus intelligent University network IP infrastructure solutions and comprehensive network management tools enable customers to build and expand robust, cost-effective, and business optimized University networks that meet both current and future corporate requirements.