Spring Semester of 2021

School of Information Science and Engineering.

Final Assignment of Routing and Switching

Title: Large Campus Network Design

Name: MD AHAD ALI

Chinese Name: 阿里

Student ID: 20183290242

Major: Computer Science and Technology

Date: 07/13/2021

Contents

Title: Large Campus Network Design

1 Abstract

In this paper I have shown the technology in campus network which I have use several method and technology such as Interior Gateway Protocol to implement a campus network. Campus network is network that some technology an be private to access and can be local also. In the campus network security and fast network is very important that I have been improve this. The campus network system is a very large and complicated system. It is not only for modern teaching, integrated information management and office automation series of applications to provide basic operating platform, but also to provide a variety of application services, so that information can be timely and accurate delivery. So my design is explained that How a large campus network works.

2 Keyword

Router, Switch, OSPF, Static, RIPv2, VLAN, STP

3 Introduction

A campus network is a network system which implement a geographic area with a bunch of technology. The campus area networks often interconnect a variety of buildings like Data Center, Administrator, Library, Dormitory etc. The distinct characteristic of a campus environment is that the company that owns the campus network also has the physical wires deployed on the campus. The campus network topology is also LAN technology connecting all the end systems within the building.

4 Devices and Technologies

I am giving an overview of the devices and configurations which selected for the campus network design.

4.1 Devices

For network design we need to use some network devices which help us transmit and receive data. There are various device used in the implementation of network design in accordance to the requirements.

4.1.1 Router

A router is a network device that connects different computer networks by routing packets from one network to the other. This device is usually connected to two or more different networks. When a data packet comes to a router port, the router reads the address information in the packet to determine out which port the packet will be sent. For example, a router provides you with the internet access by connecting your LAN with the Internet.

4.1.2 Switch

A switch is a device in a computer network that connects other devices together. Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network. A switch has many ports, to which computers are plugged in.

4.1.3 Access Point

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

4.1.4 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. This means that a device could be both a server and a client at the same time.

4.1.5 Smartphone

A smartphone is a handheld electronic device that provides a connection to a cellular network and Wi-Fi. Smartphones allow people to make phone calls, send text messages, and access the Internet.

4.1.6 Tablet-PC

Popular uses for a tablet PC include viewing presentations, video-conferencing, reading e-books, watching movies, sharing photos and more.

4.2 Technologies

Some Technologies I applied into device to solve real-world problem.

4.2.1 RIPv2

RIP version 2 was developed in 1993. It supports classless Inter-Domain Routing (CIDR) and has ability to carry subnet information, its metric is also hop count and max hop count 15 is same as rip version 1. It support authentication and does subnetting and multicasting. Auto summary can be done on every router. In RIPv2 Subnet masks are included in the routing update.

4.2.2 OSPF

OSPF (Open Shortest Path First) is a link state routing protocol. Because it is an open standard, it is implemented by a variety of network vendors. It is a classless routing protocol. OSPF will run on most routers that doesn’t necessarily have to be Cisco routers. It supports VLSM, CIDR, manual route summarization, equal cost load balancing.

4.2.3 Static

Static routing protocols are used when an administrator manually assigns the path from source to the destination network. It offers more security to the network. The advantages are No overhead on router CPU, No unused bandwidth between links and Only the administrator is able to add routes.

4.2.4 VLAN

VLANs (Virtual LANs) are logical grouping of devices in the same broadcast domain. VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. Each VLAN acts as a subgroup of the switch ports in an Ethernet LAN. It allows you to create groups of logically connected devices that act like they are on their own network. VLAN makes managing physical devices less complex. It lets you easily segment your network. It helps you to enhance network security.

4.2.5 Router-on-a-Stick Inter-VLAN Routing

A router-on-a-stick is a method of inter-VLAN routing in which the router is connected to the switch using a single physical interface, hence the name router-on-a-stick. Most modern inter-VLAN routing implementations are designed using this method. Unlike the traditional inter-VLAN routing method, router-on-stick does not require multiple physical interfaces on both the router and the switch.

4.2.6 VTP

VLAN Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere.

4.2.7 STP

STP- Spanning Tree Protocol is a link management protocol designed to support redundant links that stops switching loops in the STP network. It is a Layer 2 protocol that runs on bridges and switches, which should be enabled on the switch interfaces.

4.2.8 DTP

The Dynamic Trunking Protocol is a proprietary networking protocol developed by Cisco Systems for the purpose of negotiating trunking on a link between two VLAN-aware switches, and for negotiating the type of trunking encapsulation to be used. It works on Layer 2 of the OSI model.

4.2.9 SSH (Secure Shell)

SSH is a network protocol used to remotely access and manage a device. The key difference between Telnet and SSH is that SSH uses encryption, which means that all data transmitted over a network is secure from eavesdropping. SSH uses the public key encryption for such purposes.

4.2.10 Frame Relay

Frame relay is a cost-effective way to connect Local Area Networks (LANs) or transport data between endpoints in Wide Area Network (WANs).

4.2.11 DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol that provides quick, automatic, and central management for the distribution of IP addresses within a network. It's also used to configure the subnet mask, default gateway, and DNS server information on the device.

4.2.11 ACLs

Access Control Lists, or ACLs, are a tool that is used to define traffic on Cisco routers. ACLs are a set of rules used most commonly to filter network traffic. They are used on network devices with packet filtering compatibilities (e.g. routers or firewalls). ACLs are applied on the interface basis to packets leaving or entering an interface.

4.2.12 Port security

Switch port Security is a network security feature that associates specific MAC addresses of devices (such as PCs) with specific interfaces on a switch. This will enable you to restrict access to a given switch interface so that only the authorized devices can use it. If an unauthorized device is connected to the same port, you can define the action that the switch will take, such as discarding the traffic, sending an alert, or shutting down the port.

4.2.13 Others

There are also many more technologies used for improve a better network design. Such as Syslog, NTP (The Network Time Protocol is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.), HTTP, Email etc.

5 Design and configurations

5.1 Design overview

The network topology design was based on Yunnan university Chenggong campus. I implemented maximum area and provided a best design topology. So First I designed Internet service provider (ISP) structure which provide network that can be accessing, using, or participating in the Internet. Then I used Data Center that will provide and supply internet data. I also used university Administration that they will store, provide and supply schools Hospital data and they will also control university email service. I designed most secure network of information schools and Gewa buildings topology. I demonstrate School’s hospital that they can receive or send broadcast data from administrator building. I designed Minguyan building international office which they can access datacenter of tuition fee data and student info data. I also designed advanced dormitory network. There have 3 dormitories. Then I designed library network topology That student can access network through ISP.

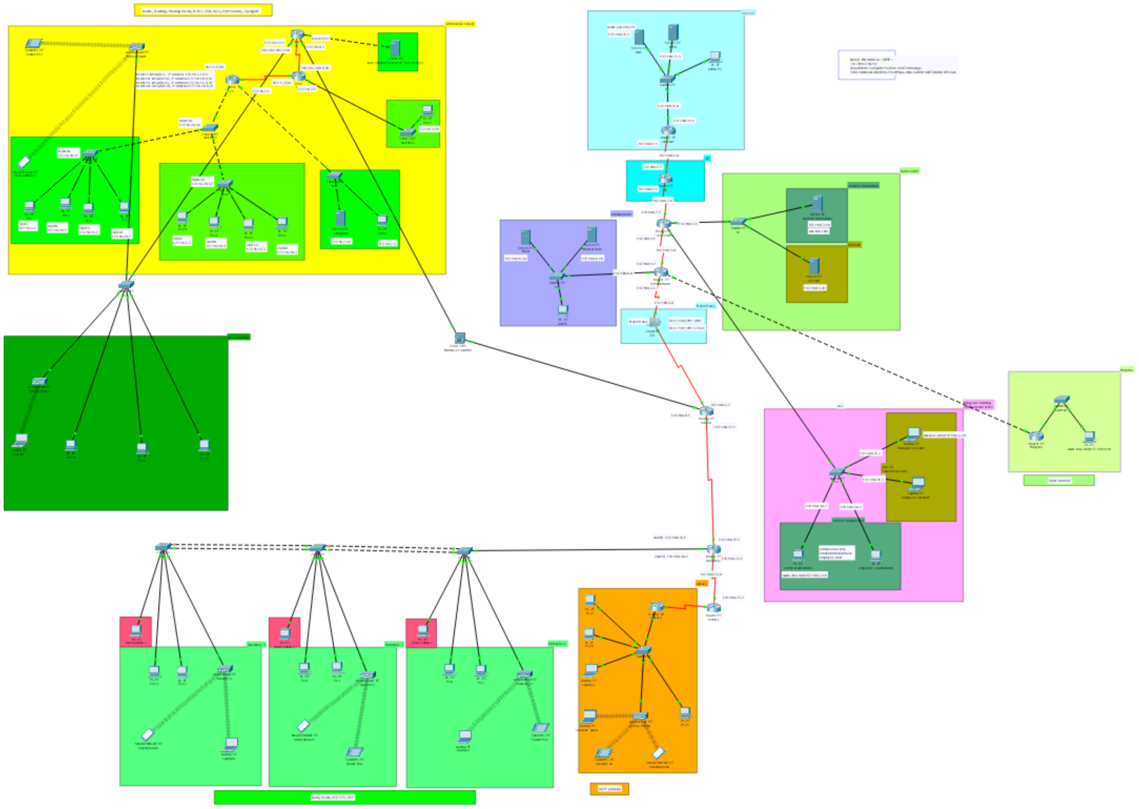


Figure 1: Campus Network.

5.2 Hardware and software requirement

Computer, *Cisco Packet Tracer 7.1, Windows 10.

** In Cisco packet tracer software has some bugs, So some connection like pinging or browsing may not be succeed in first attempt but second attempt will succeed.*

5.3 Configuration

5.3.1 Router IP Address and Subnet mask.

Device	Name	Port	IPv4 Address	Subnet mask	Default getway
Router	Internet	F0/0	192.168.21.1	255.255.255.0	
		Se2/0	192.168.1.1	255.255.255.0	
Router	ISP	Se2/0	192.168.1.2	255.255.255.0	
		Se3/0	192.168.2.1	255.255.255.0	
Router	Data Center	F0/0	192.168.3.1	255.255.255.0	
		Se2/0	192.168.2.2	255.255.255.0	
		Se3/0	192.168.4.1	255.255.255.0	
		F1/0	VLAN10- 192.168.30.1 VLAN20- 192.168.31.1	255.255.255.0	

Router	Administrator	F0/0	192.168.6.1	255.255.255.0	
		F1/0	192.168.11.1	255.255.255.0	
		Se2/0	192.168.4.2	255.255.255.0	
		Se3/0	192.168.5.1	255.255.255.0	
Router	School	F0/0	192.168.8.1	255.255.255.0	
		Se2/0	192.168.5.2	255.255.255.0	
		Se3/0	192.168.22.1	255.255.255.0	
Router	Dormitory	Se2/0	192.168.22.2	255.255.255.0	
		Se3/0	192.168.23.1	255.255.255.0	
		F0/0	VLAN10-192.168.35.1	255.255.255.0	
			VLAN20-192.168.36.1	255.255.255.0	
Router	Others	Se2/0	192.168.23.2	255.255.255.0	
		Se3/0	192.168.9.1	255.255.255.0	
Router	Hospital	F0/0	192.168.11.2	255.255.255.0	
		F1/0	192.168.12.1	255.255.255.0	
Router	Library	F0/0	192.168.10.1	255.255.255.0	
		Se2/0	192.168.9.2	255.255.255.0	
Router	r1	G0/0	VLAN5-172.16.5.1 VLAN10-172.16.10.1 VLAN 15-172.16.15.1 VLAN50-172.16.20.1	255.255.255.0	
		G0/1	172.16.2.1	255.255.255.0	
		Se0/0/0	10.1.1.1	255.255.255.252	
Router	r2	G0/0	172.16.3.1	255.255.255.0	
		Se0/0/0	10.1.1.2	255.255.255.252	
		Se0/0/1	209.165.200.1	255.255.255.252	
Router	r3	F0/0	8.8.8.1	255.255.255.0	
		F0/1	192.168.8.2	255.255.255.0	
		Se0/0/1	209.165.200.2	255.255.255.252	
		F1/0	192.168.75.1	255.255.255.0	
Server	DNS		192.168.21.2	255.255.255.0	192.168.21.1
Server	WEB		192.168.21.3	255.255.255.0	192.168.21.1
Server	Student information		192.168.3.10	255.255.255.0	192.168.3.1
Server	Account		192.168.3.20	255.255.255.0	192.168.3.1
Server	local-student-database-8.8.8.10/24		8.8.8.10	255.255.255.0	8.8.8.1
Server	syslog/ntp		172.16.2.10	255.255.255.0	172.16.2.1

Server	Hospital-Data		192.168.6.10	255.255.255.0	192.168.6.1
Server	Email		192.168.6.30		192.168.6.1
PC	PC1		172.16.5.2		172.16.5.1
PC	PC3		172.16.10.2		172.16.10.1
PC	PC4		172.16.15.2		172.16.15.1
PC	PC5		172.16.20.2		172.16.20.1
PC	PC10		172.16.5.3		172.16.5.1
PC	PC11		172.16.10.3		172.16.10.1
PC	PC13		172.16.15.3		172.16.15.1
PC	PC15		172.16.20.3		172.16.20.1
PC	PC16		172.16.2.25		172.16.2.1
PC	PC17		172.16.3.10		172.16.3.1
Laptop	Manager-account		192.168.31.2		192.168.31.1
Laptop	Employee-account		192.168.31.3		192.168.31.1
PC	Admin-studentinfo		192.168.30.2		192.168.30.1
PC	Employee-studentinfo		192.168.30.3		192.168.30.1
PC	www.hda.com/ 192.168.6.10		192.168.12.2		192.168.12.1
PC	dorm-admin-1		192.168.35.4		192.168.35.1
PC	dorm-admin-2		192.168.35.3		192.168.35.1
PC	dorm-admin-3		192.168.35.2		192.168.35.1

5.3.2: Internet and ISP management

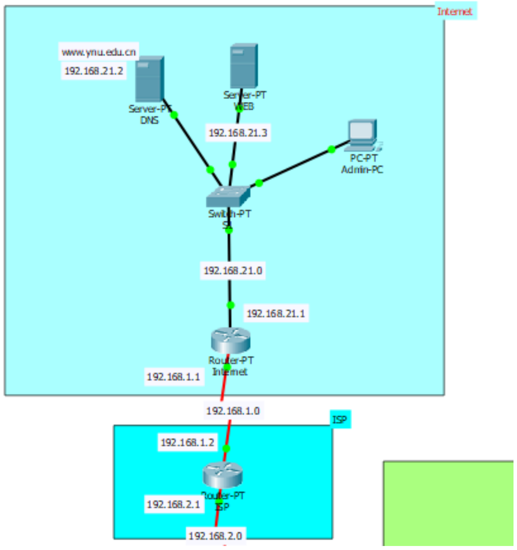
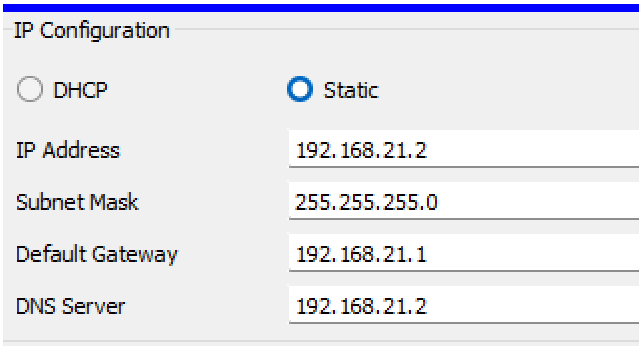


Figure 2: Internet and ISP management.

Here in this figure 2, we can see the internet and internet service provider. My purpose was designed global web configuration and different between the campus network and the global network. Internet service provider (ISP), company that provides Internet connections and services to individuals and organizations. In addition to providing access to the Internet and web access. I added DNS server in internet topology.



IP Configuration

○ DHCP ● Static

IP Address 192.168.21.2

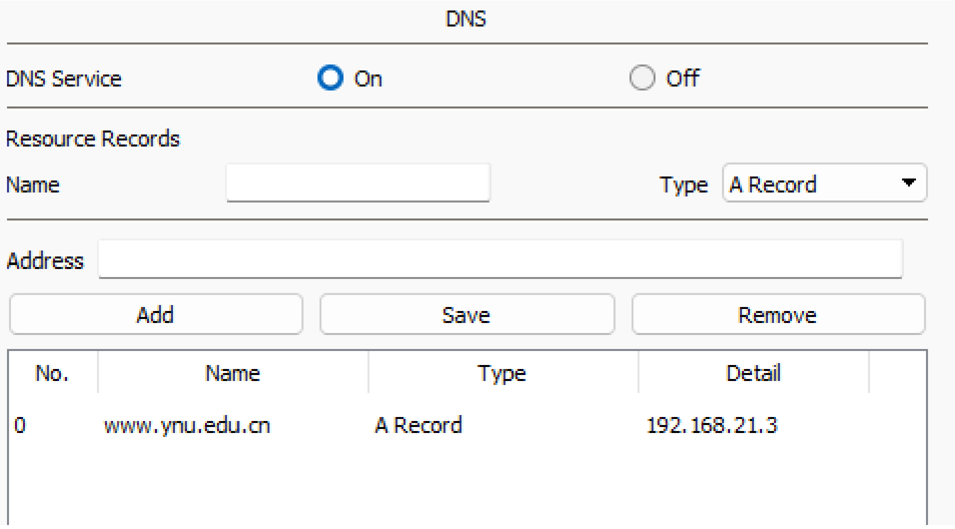
Subnet Mask 255.255.255.0

Default Gateway 192.168.21.1

DNS Server 192.168.21.2

Figure 3: IP config.

Then I defined website domain.



DNS

DNS Service ● On ○ Off

Resource Records

Name

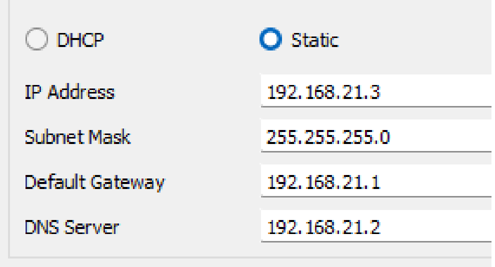
Type A Record

Address

No.	Name	Type	Detail
0	www.ynu.edu.cn	A Record	192.168.21.3

Figure 4: DNS

As domain name configuration I added a web server.



○ DHCP ● Static

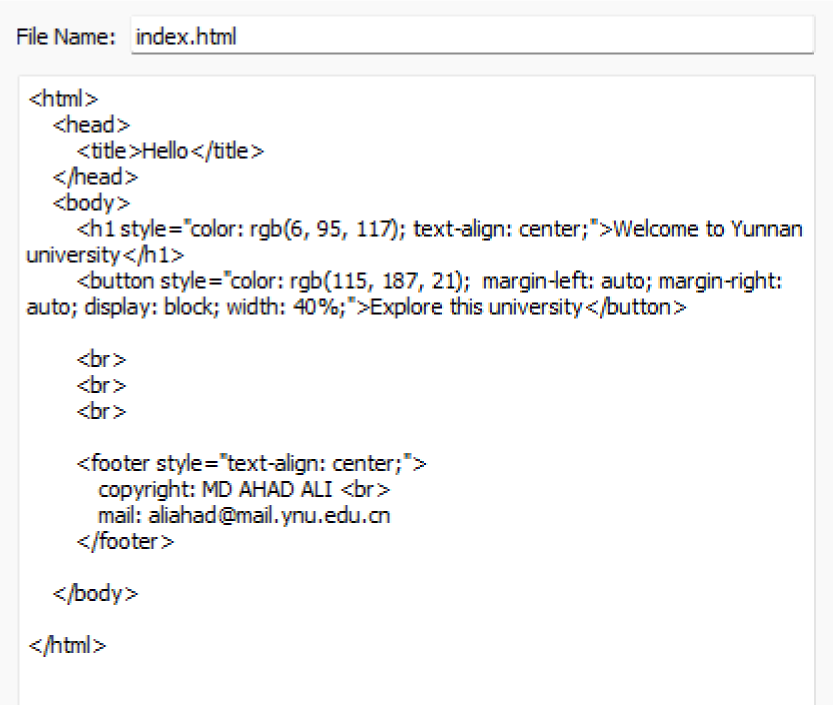
IP Address 192.168.21.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.21.1

DNS Server 192.168.21.2

Figure 5: IP config.



```
<html>
  <head>
    <title>Hello</title>
  </head>
  <body>
    <h1 style="color: rgb(6, 95, 117); text-align: center;">Welcome to Yunnan
university</h1>
    <button style="color: rgb(115, 187, 21);  margin-left: auto; margin-right:
auto; display: block; width: 40%;">Explore this university</button>

    <br>
    <br>
    <br>

    <footer style="text-align: center;">
      copyright: MD AHAD ALI <br>
      mail: aliahad@mail.ynu.edu.cn
    </footer>

  </body>

</html>
```

Figure 6: HTML, CSS

Based on DNS every maximum router who need web access from topology I Configure DHCP server.

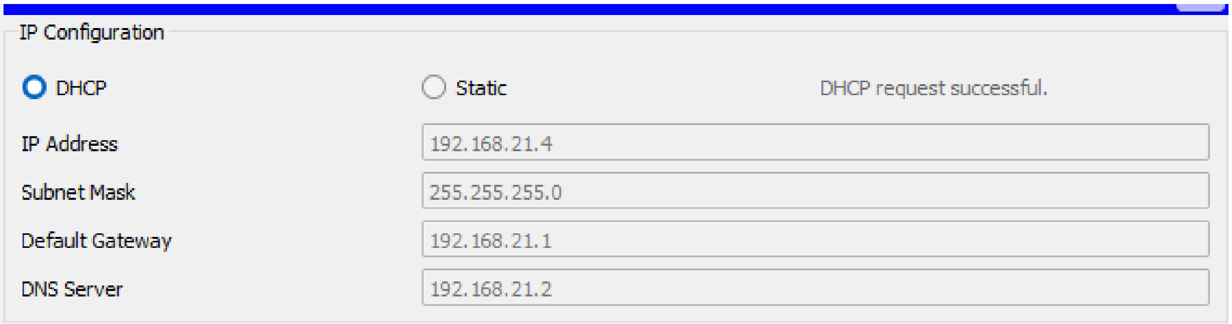
Example of

```
Router(config)#

Router(config)#ip dhcp pool dataC

Router(dhcp-config)#network 192.168.21.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.21.1

Router(dhcp-config)#dns-server 192.168.21.2
```

Now we can see in internet router about DHCP configuration.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.21.1.

%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.21.2.

%DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged 192.168.21.3.
```

Now we can configure every pc IP address, Subnet mask, Default gateway and DNS server automatically through DHCP.



IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address: 192.168.21.4

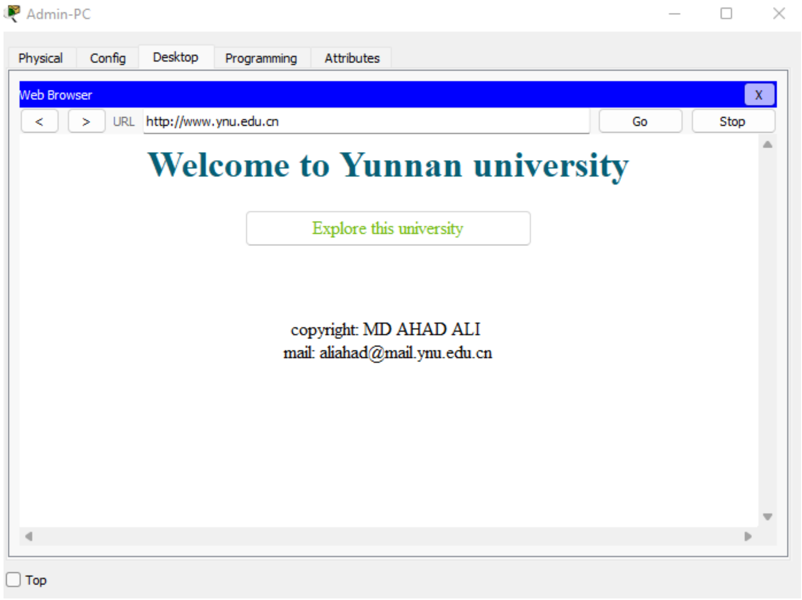
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.21.1

DNS Server: 192.168.21.2

Figure 7: IP config.

Now we can go to Admin-PC and check from the browser.



URL: http://www.ynu.edu.cn

Welcome to Yunnan university

Explore this university

copyright: MD AHAD ALI
mail: aliahad@mail.ynu.edu.cn

Figure 8: Brows the internet.

5.3.3: Data center management and Minguyan building international office.

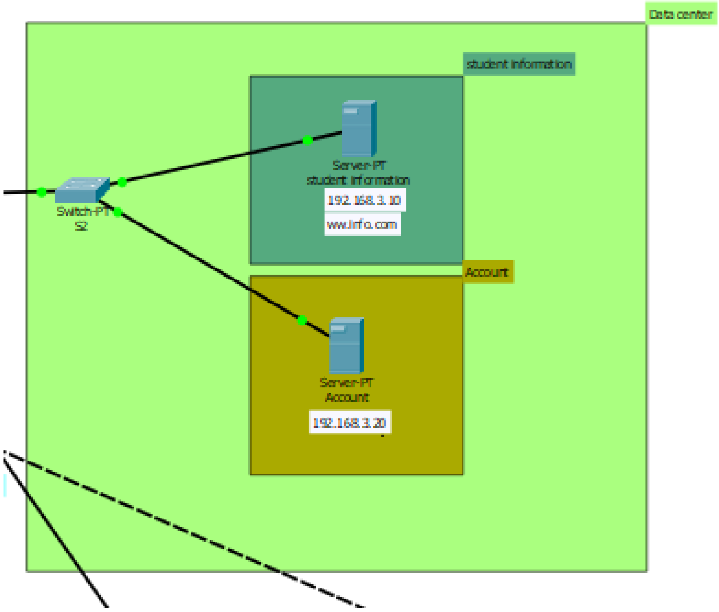
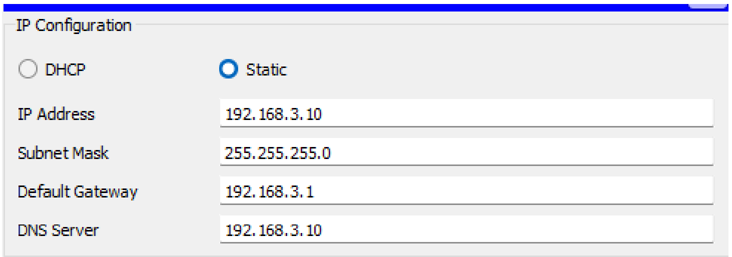


Figure 9: Student INFO and Account INFO in DataCenter.

Here I added two data servers. One is student-information which I defined DNS and HTTP.

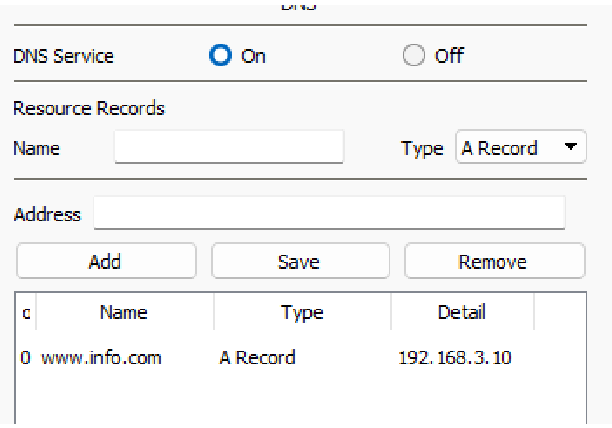


IP Configuration

○ DHCP ● Static

IP Address	192.168.3.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
DNS Server	192.168.3.10

Figure 10: IP config.



DNS

DNS Service ● On ○ Off

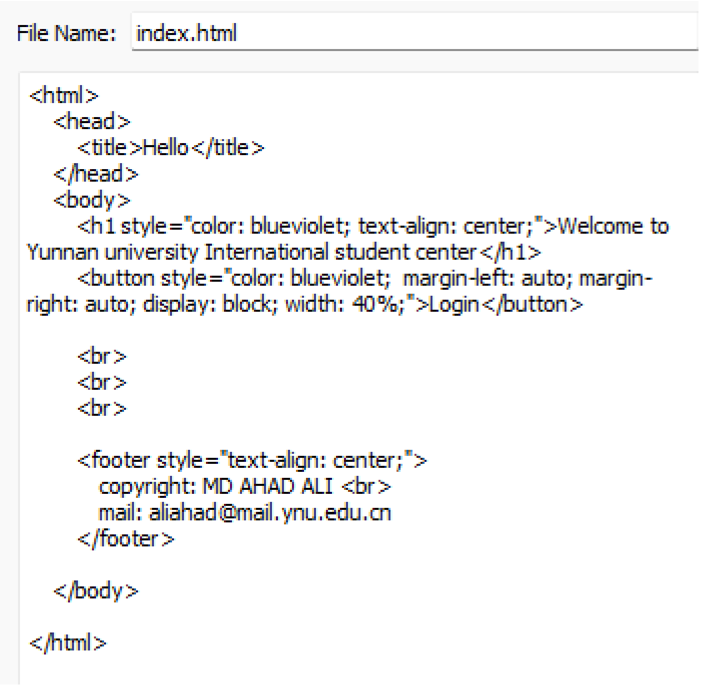
Resource Records

Name Type A Record

Address

c	Name	Type	Detail
0	www.info.com	A Record	192.168.3.10

Figure 11: DNS



File Name: index.html

```
<html>
   <head>
      <title>Hello</title>
   </head>
   <body>
      <h1 style="color: blueviolet; text-align: center;">Welcome to
Yunnan university International student center</h1>
      <button style="color: blueviolet;  margin-left: auto; margin-
right: auto; display: block; width: 40%;">Login</button>

      <br>
      <br>
      <br>

      <footer style="text-align: center;">
         copyright: MD AHAD ALI <br>
         mail: aliahad@mail.ynu.edu.cn
      </footer>

   </body>

</html>
```

Figure 12: HTML and CSS

And another server is for Account and I defined DNS (www.ac.com) and HTTP.

Now for this server access I designed another topology called Minguyan Building International office.

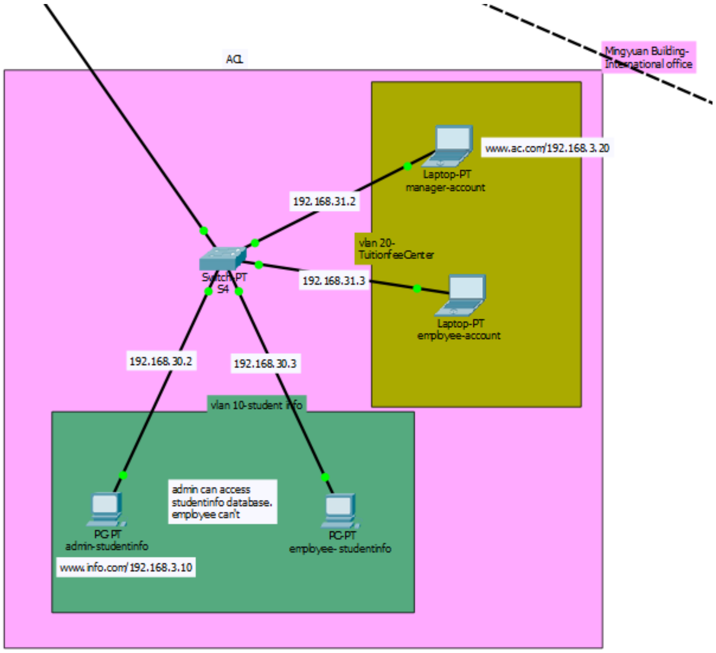


Figure 13: Minguyan Building Managgement.

I designed That only admin and manager can use their own server. So I used ACLs technology here.

```
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 100
  Proxy ARP is enabled
  Security level is default
 --More--
```

```
FastEthernet1/0.20 is up, line protocol is up (connected)
  Internet address is 192.168.31.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 101
  Proxy ARP is enabled
```

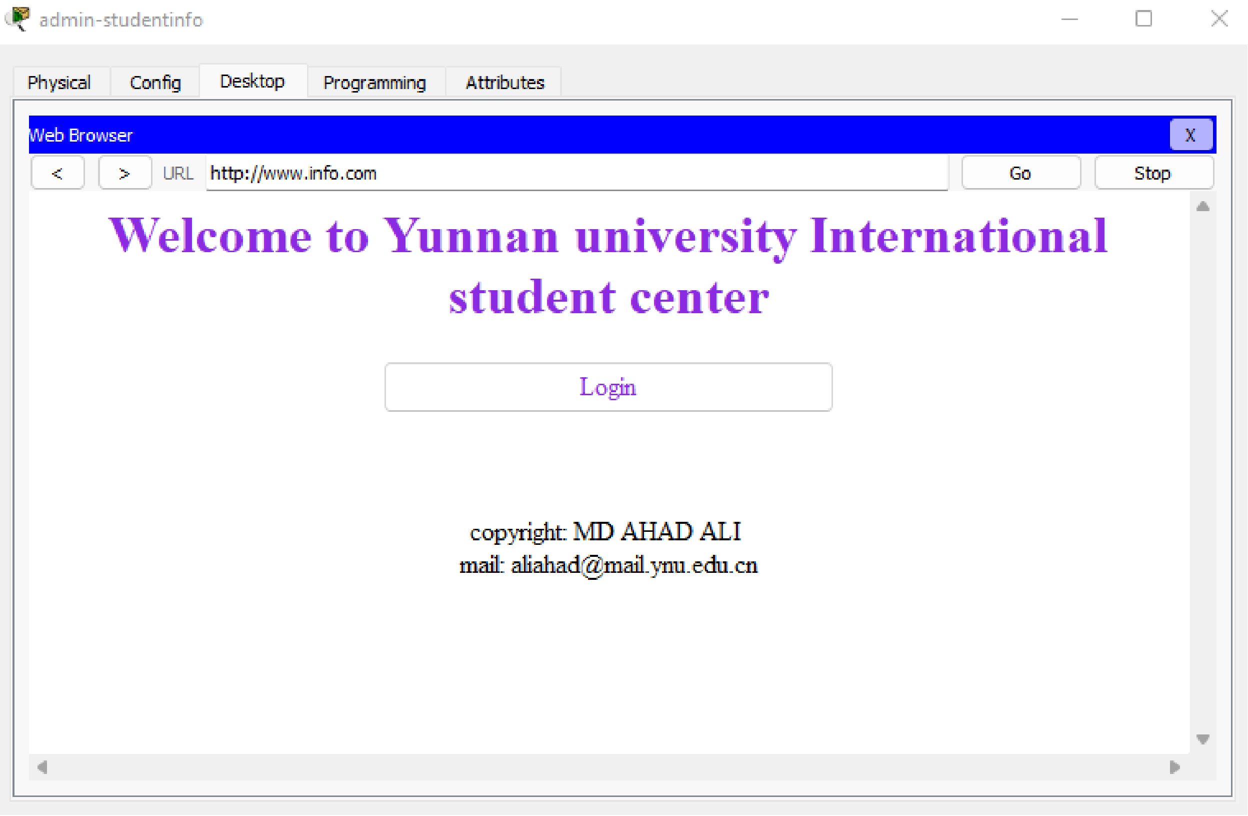
Here we can see I used VLAN in minguyan building topology.

```
Switch>en

Switch#sh vlan


VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

1    default                          active    Fa4/1, Fa5/1

10   YNURESULT                        active    Fa1/1, Fa2/1

20   YNUADMIT                         active    Fa3/1, Fa6/1

1002 fddi-default                     act/unsup

1003 token-ring-default               act/unsup

1004 fddinet-default                  act/unsup

1005 trnet-default                    act/unsup
```

So now we can see access-list from ‘show access-list’ command.

```
YNUdata#sh access-list
Extended IP access list 100
    10 permit ip host 192.168.30.2 host 192.168.3.10 (10 match(es))
    20 deny ip host 192.168.30.3 host 192.168.3.10
Extended IP access list 101
    10 permit ip host 192.168.30.3 host 192.168.3.20
    20 deny ip host 192.168.30.2 host 192.168.3.20
    30 permit ip host 192.168.31.2 host 192.168.3.20
    40 deny ip host 192.168.31.3 host 192.168.3.20


YNUdata#
```

Now we can see Admin- student info can access.



URL http://www.info.com

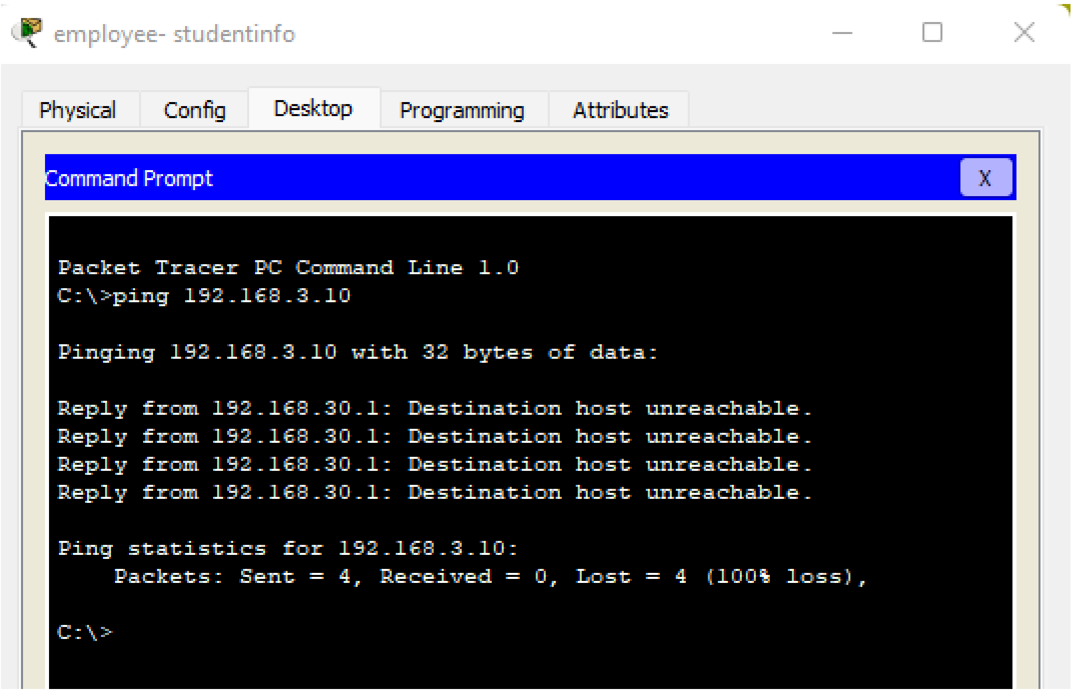
Welcome to Yunnan university International student center

Login

copyright: MD AHAD ALI
mail: aliahad@mail.ynu.edu.cn

Figure 14: Brows the Internet

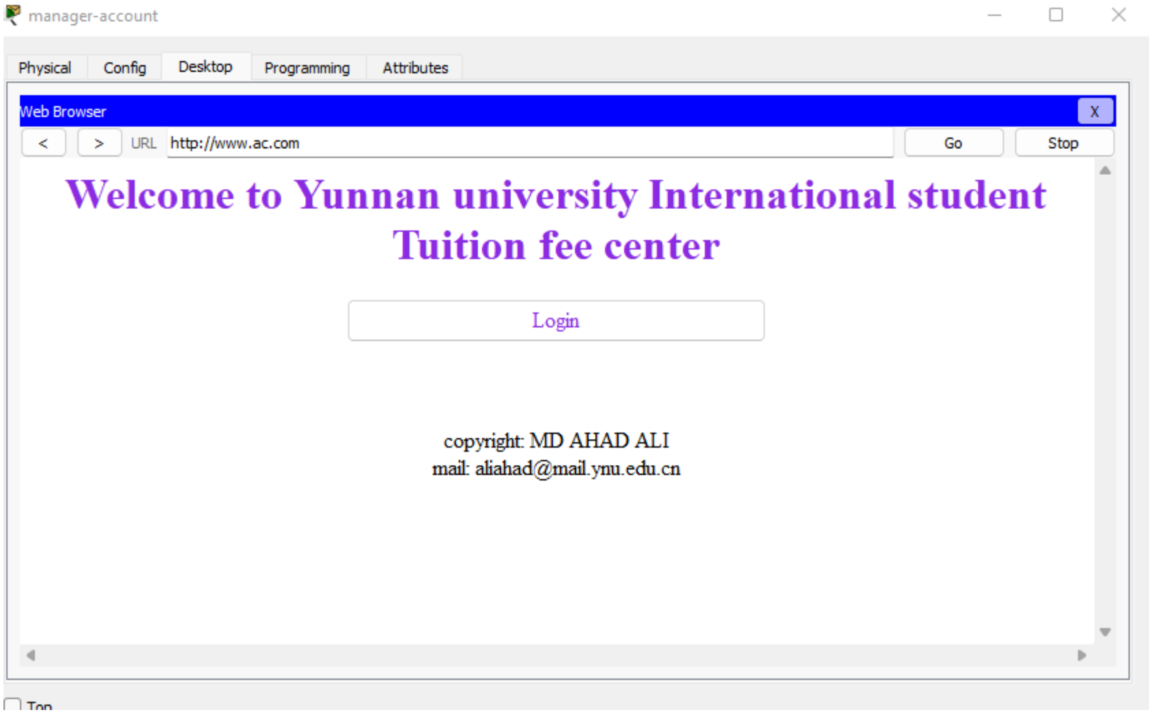
But employee can’t access.



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.3.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 15: Pinging

In Tuition fee center area I did same. The rule is only manager can access but employee can’t access data.



URL http://www.ac.com

Welcome to Yunnan university International student Tuition fee center

Login

copyright: MD AHAD ALI
mail: aliahad@mail.ynu.edu.cn

Figure 16: Browse the Internet

5.3.4 Information school and Gewa management.

In this topology I configured address router interfaces and hosts, and configure VLANs, Trunking and routing between VLANs, I was also configured and customize RIPv2, and control access to router VTY lines with a standard named ACL.

On the r3 router:

```
# enable

# conf t

# hostname r3

# int G0/0

# ip address 8.8.8.1 255.255.255.0

# no shut

# int S0/0/1

# ip address 209.165.200.2 255.255.255.252

# no shut
```

Then I configured Static routes on the r3 router.

```
# conf t

# ip route 172.16.0.0 255.255.0.0 S0/0/1

# ip route 10.1.1.0 255.255.255.252 S0/0/1
```

On the r2:

```
# enable

# conf t

# hostname r2

# int G0/0

# ip address 172.16.3.1 255.255.255.0

# no shut

# int s0/0/0

# ip address 10.1.1.2 255.255.255.252

# no shut

# int s0/0/1

# ip address 209.165.200.1 255.255.255.252

# no shut
```

Then I configured a default route, the exit interface on the r3 router.

```
# conf t

# ip route 0.0.0.0 0.0.0.0 S0/0/1
```

On the r1 router:

Here first I disabled DNS lookup to prevent the router from trying to resolve incorrectly pasted commands in the cli by sending out a DNS query.

```
# enable

# conf t

# no ip-domain lookup

# hostname r1
```

Then I con figured password encryption. I also assigned the encrypted type of privileged EXEC password. Then I configured the console line so that router status messages will not interrupt command line input. Next I configured the console to require a password for access.

```
# service password-encryption

# enable secret ynu

# line console 0

# logging synchronous

# password ynu

# login
```

I configured the VTY ports to only accept connections over SSH, and I used the following values.

-Domain Name: ynu.com

-Local Username: Admin

-User Password: ccna

-Modulus: 1024

-Version: 2

```
# conf t

# ip domain-name ynu.com

# username Admin password ccna

# crypto key generate rsa

# enter

# 1024

# ip ssh version 2

# line vty 0 15

# transport input ssh

# login local
```

Next, I activated and configure G0/1 and S0/0/0 interfaces on Router1 with the IP addresses as shown on the topology, as for G0/0 interface will be configured later in this practice labs.

```
# conf t

# int G0/1

# ip address 172.16.2.1 255.255.255.0

# no shut

# int s0/0/0

# ip address 10.1.1.1 255.255.255.252

# no shut
```

I configured SW-1, SW-2 and SW-3 with VLANs and Trunking. I added the VLANs to the switches I configured the links between SW-1, SW-2 and SW-3 as trunks, and configured the link between SW-1 and Router1 as a Trunk, and all trunking interfaces should be statically configured as trunks.

I assigned the appropriate ports to the VLANs.

On SW-1:

```
# enable
# conf t
# hostname SW-1
# vlan 5
# vlan 10
# vlan 15
# vlan 50
# exit
# int range f0/23-24,G0/1
# switchport mode trunk
```

On SW-2:

```
# enable
# conf t
# hostname SW-2
# vlan 5
# vlan 10
# van 15
# vlan 50
# exit
# int f0/23
# switchport mode trunk
# int f0/5
# switchport mode access
# switchport access vlan 5
# int f0/10
# switchport mode access
# switchport access vlan 10
# int f0/15
# switchport mode access
# switchport access vlan 15
# int f0/20
# switchport mode access
# switchport access vlan 50
```

On SW-3:

```
# enable
# conf t
# hostname SW-3
# vlan 5
# vlan 10
# vlan 15
# vlan 50
# exit
# int f0/24
# switchport mode trunk
# int f0/5
# switchport mode access
# switchport access vlan 5
# int f0/10
# switchport mode access
# switchport access vlan 10
# int f0/15
# switchport mode access
# switchport access vlan 15
# int f0/20
# switchport mode access
```

Next I configured routing between VLANs on r1.

On r1:

```
# conf t

# int g0/0.5

# encapsulation dot1q 5

# ip address 172.16.5.1 255.255.255.0

# int g0/0.10

# encapsulation dot1q 10

# ip address 172.16.10.1 255.255.255.0

# int g0/0.15

# encapsulation dot1q 15

# ip address 172.16.15.1 255.255.255.0

# int g0/0.20

# encapsulation dot1q 50

# ip address 172.16.20.1 255.255.255.0

# int g0/0.99
```

I activated the physical interface G0/0.

```
# int G0/0

# no shut
```

I configured a named “Deny15”, to prevent any host with an address on VLAN 15 subnetwork from access the VLAN10 subnetwork, and all other hosts from other subnetworks should be permitted, and this Access list should have two statements. I applied the ACL close to the destination, which is in our example VLAN 10.

On r1:

```
# conf t

# ip access-list standard Deny15

# deny 172.16.15.0 0.0.0.255

# permit any

# exit

# int g0/0.10

# ip access-group Deny15 out
```

I configured the Switch Virtual Management Interface on SW-1, SW-2 and SW-3, all switches should be reachable from hosts on other networks .

On SW-1:

```
# conf t

# int vlan 50

# ip address 172.16.20.50 255.255.255.0

# exit

# ip default-gateway 172.16.20.1
```

On SW-2:

```
# conf t

# int vlan 50

# ip address 172.16.20.51 255.255.255.0

# exit

# ip default-gateway 172.16.20.1
```

On SW-3:

```
# conf t

# int vlan 50

# ip address 172.16.20.52 255.255.255.0

# exit

# ip default-gateway 172.16.20.1
```

I will configure switch port security. I will improve network security by configuring SW-2 and SW-3.

On SW-2:

I disabled all unused switch ports. I activated port security on all ports that have hosts connected. I allowed only a maximum of two MAC addresses to access the active switch port. I configured the switch ports to automatically learn the two allowed MAC address and record the addresses in the running configuration. I configured the switch ports to that, if maximum number of addresses for each port is exceeded, packets with unknown source addresses are dropping until a sufficient number of secure MAC addresses are removed.

```
# conf t

# int range F0/1-4, F0/6-9, F0/11-14, F0/16-19, F0/21-22, F0/24, G0/1-2

# shutdown

# int range F0/5, F0/10, F0/15, F0/20

# switchport port-security

# switchport port-security maximum 2

# switchport port-security mac-address sticky

# switchport port-security violation restrict
```

On SW-3:

I disabled all unused switch ports. I will activated port security on all ports that have hosts connected. I allowed only a maximum of two MAC addresses to access the active switch port. I configured the switch ports to automatically learn the two allowed MAC address and record the addresses in the running configuration. I configured the switch ports to that, if maximum number of addresses for each port is exceeded, packets with unknown source addresses are dropping until a sufficient number of secure MAC addresses are removed.

```
# conf t

# int range F0/1-4, F0/6-9, F0/11-14, F0/16-19, F0/21-23, G0/1-2

# shutdown

# int range F0/5, F0/10, F0/15, F0/20

# switchport port-security

# switchport port-security maximum 2

# switchport port-security mac-address sticky

# switchport port-security violation restrict
```

I configured Dynamic Routing RIPv2 routing on r1 and r2 so that all networks are reachable.

On r1:

I prevented RIP to automatically summarizing networks. I configured all LAN physical interfaces so that RIP updates are not sent out to the LANs.

```
# conf t

# router rip

# version 2

# network 10.1.1.0

# network 17.16.5.0

# network 172.16.10.0

# network 172.16.15.0

# network 172.16.20.0

# network 172.16.2.0

# no auto-summary

# passive-interface g0/0.5

# passive-interface g0/0.10

# passive-interface g0/0.15

# passive-interface g0/0.20

# passive-interface g0/1
```

On r2:

I did not advertise the network connected to the internet r3 router. I configured RIP to automatically sent the default route that is already configured on r2 to r1.

```
# conf t
# router rip
# version 2
# network 10.1.1.0
# network 172.16.3.0
# default-information originate
# no auto-summary
# passive-interface g0/0
# passive-interface s0/0/1
```

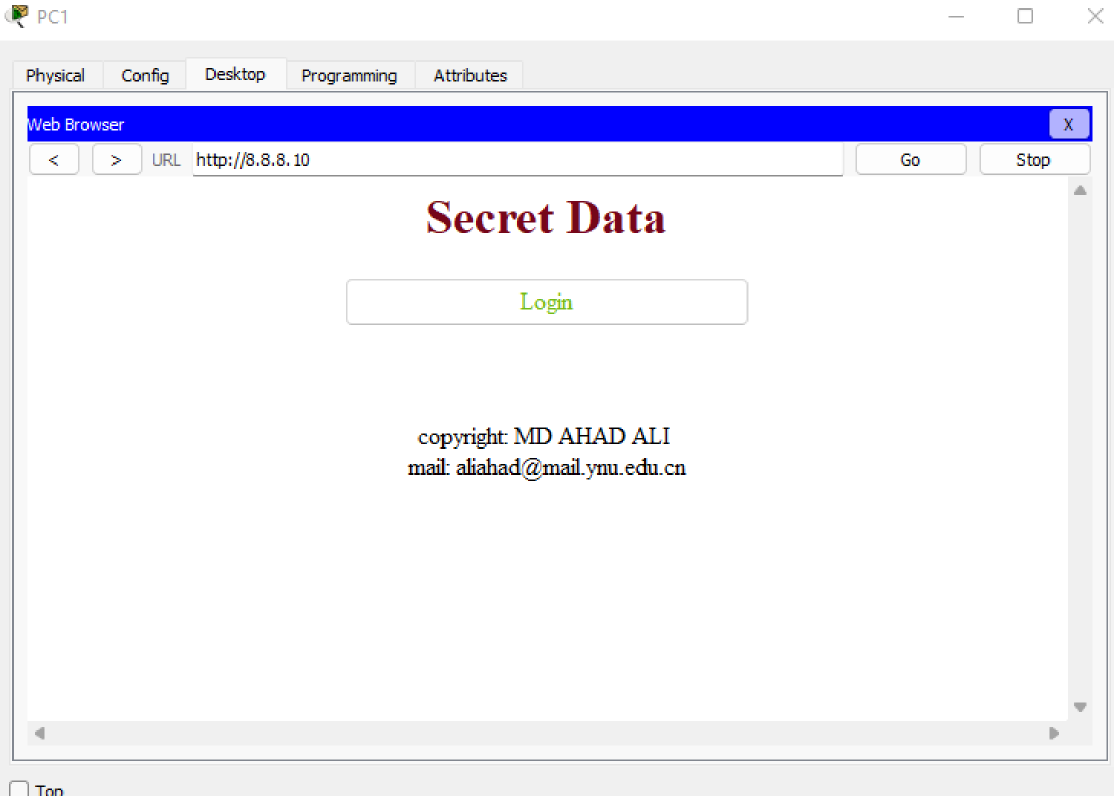
I configured Network Monitoring. I configured NTP and Syslog server logging on Router1. I activated the logging and debug timestamp services.

On r1:

I configured r1 as an NTP client, the NTP server is Syslog/NTP Svr with the address of 172.16.2.10/24. I configured Syslog to send debug level messages to the Syslog/NTP Svr logging server.

```
# conf t
# service timestamp log datetime msec
# service timestamp debug datetime msec
# ntp server 172.16.2.10
# logging 172.16.2.10
# logging trap debugging
# ntp update-calendar
```

Now the PC’s can visit server as well.

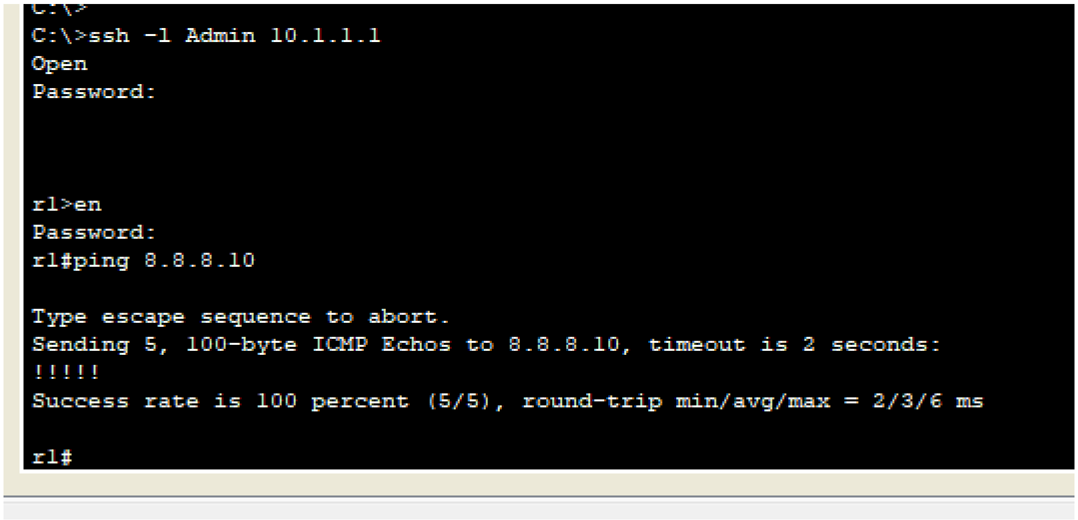


Secret Data

copyright: MD AHAD ALI
mail: aliahad@mail.ynu.edu.cn

Figure 17: Brows the Internet.

Now we can use SSH also.



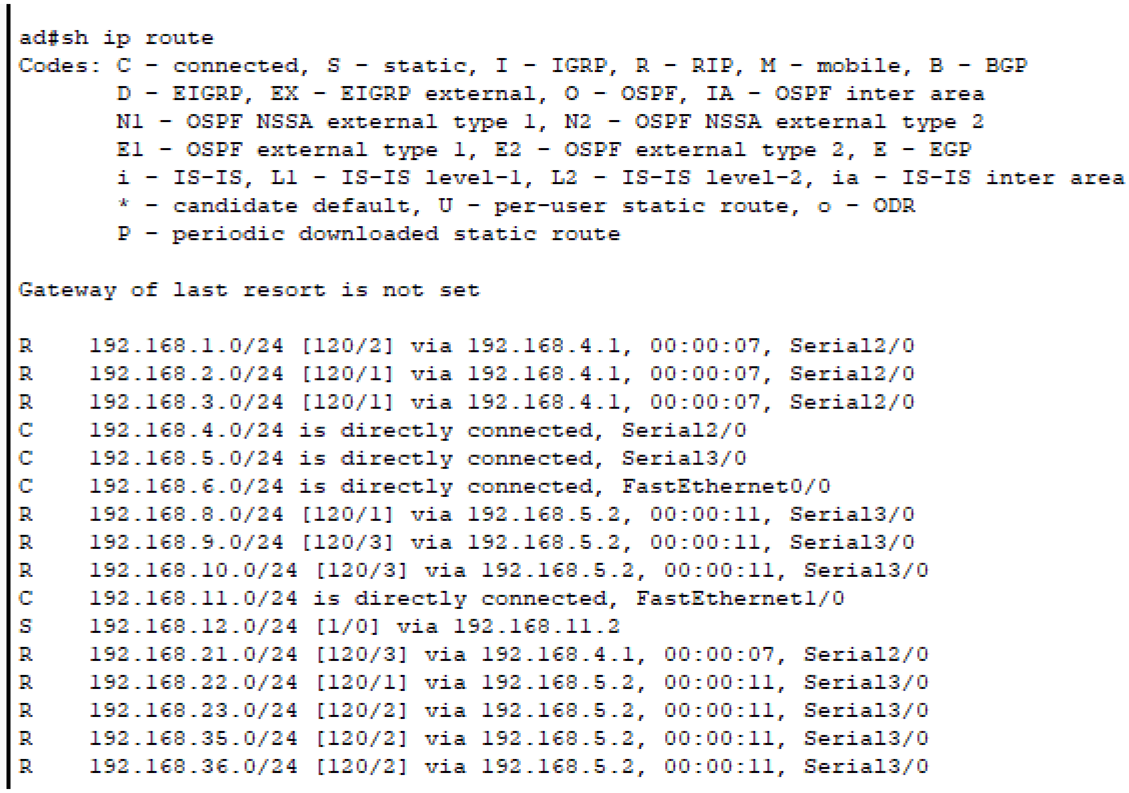
```
C:\>
C:\>ssh -l Admin 10.1.1.1
Open
Password:



r1>en
Password:
r1#ping 8.8.8.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms

r1#
```

Figure 18: Test SSH

Now from r3 router I used ‘ip dhcp pool dataC’ command to access DHCP network from ISP to Gewa building.

5.3.5 Administrator and Hospital Management

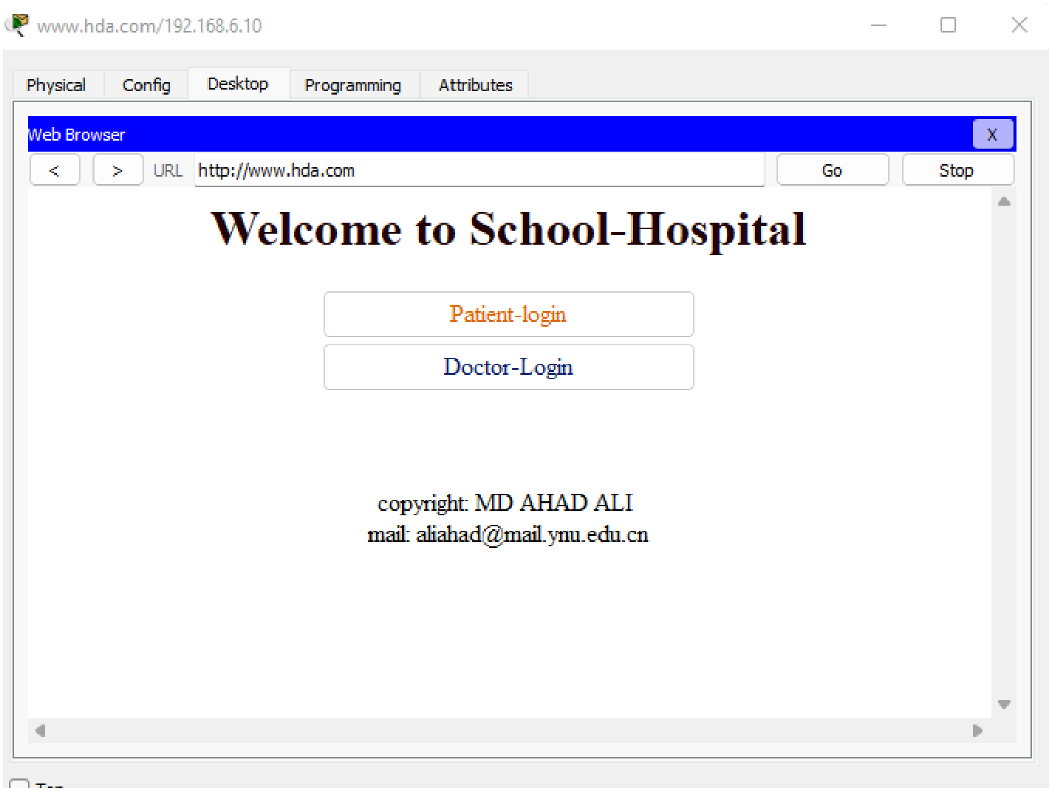
Here administrator router from Datacenter to cloud router I used RIPv2 Protocol. Administrator to Hospital router I used Static protocol. From connect RIPv2 to Static protocol I used redistribute static matric technology.



```
ad#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.1.0/24 [120/2] via 192.168.4.1, 00:00:07, Serial2/0
R    192.168.2.0/24 [120/1] via 192.168.4.1, 00:00:07, Serial2/0
R    192.168.3.0/24 [120/1] via 192.168.4.1, 00:00:07, Serial2/0
C    192.168.4.0/24 is directly connected, Serial2/0
C    192.168.5.0/24 is directly connected, Serial3/0
C    192.168.6.0/24 is directly connected, FastEthernet0/0
R    192.168.8.0/24 [120/1] via 192.168.5.2, 00:00:11, Serial3/0
R    192.168.9.0/24 [120/3] via 192.168.5.2, 00:00:11, Serial3/0
R    192.168.10.0/24 [120/3] via 192.168.5.2, 00:00:11, Serial3/0
C    192.168.11.0/24 is directly connected, FastEthernet1/0
S    192.168.12.0/24 [1/0] via 192.168.11.2
R    192.168.21.0/24 [120/3] via 192.168.4.1, 00:00:07, Serial2/0
R    192.168.22.0/24 [120/1] via 192.168.5.2, 00:00:11, Serial3/0
R    192.168.23.0/24 [120/2] via 192.168.5.2, 00:00:11, Serial3/0
R    192.168.35.0/24 [120/2] via 192.168.5.2, 00:00:11, Serial3/0
R    192.168.36.0/24 [120/2] via 192.168.5.2, 00:00:11, Serial3/0
```

Figure 19: IP route.

I added hospital server to Administrator area. So We can connect from Hospital network with redistribution technology.



www.hda.com/192.168.6.10

URL http://www.hda.com

Welcome to School-Hospital

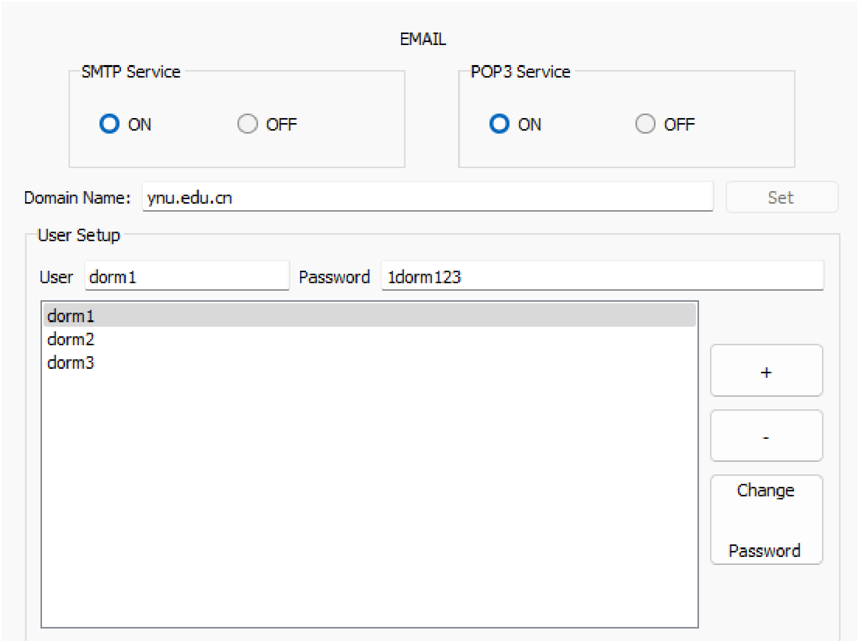
Patient-login

Doctor-Login

copyright: MD AHAD ALI
mail: aliahad@mail.ynu.edu.cn

Figure 20: Brows the Internet

InAdminstrator are I also setup Email server that who registered can access.



EMAIL

SMTP Service ● ON ○ OFF

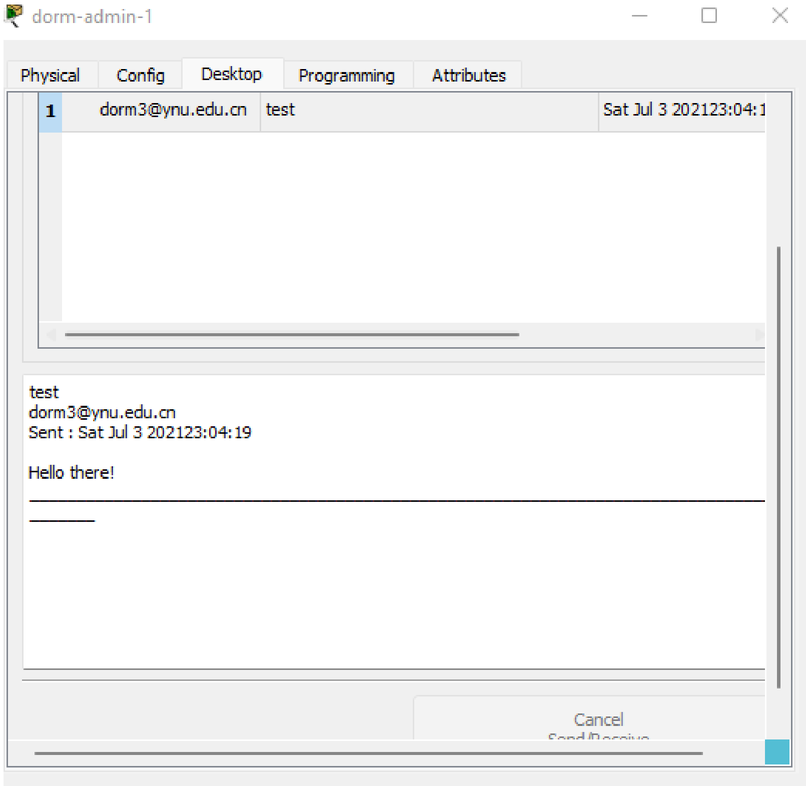
POP3 Service ● ON ○ OFF

Domain Name: ynu.edu.cn

User dorm1 Password 1dorm123

dorm1
dorm2
dorm3

Figure 21: Email server.



1	dorm3@ynu.edu.cn	test	Sat Jul 3 202123:04:1

test
dorm3@ynu.edu.cn
Sent : Sat Jul 3 202123:04:19

Hello there!

Figure 22: Send and receive email.

5.3.6 Dormitory Management:

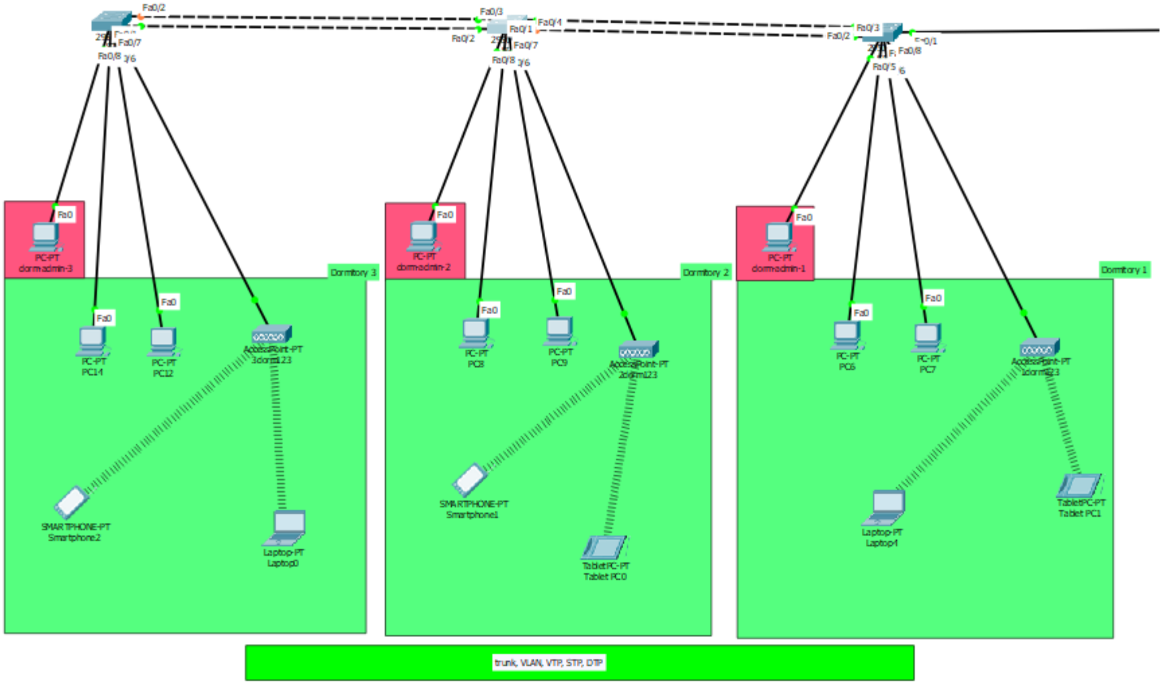
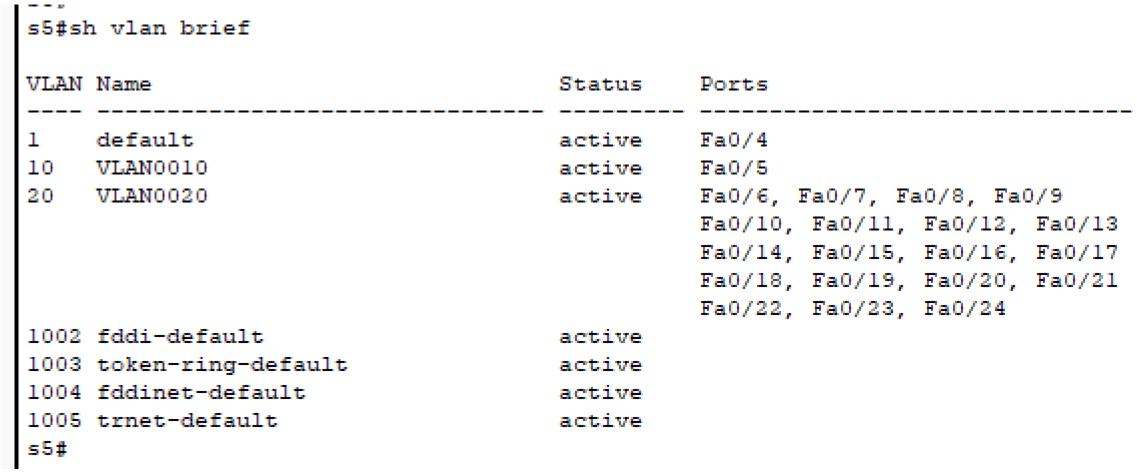


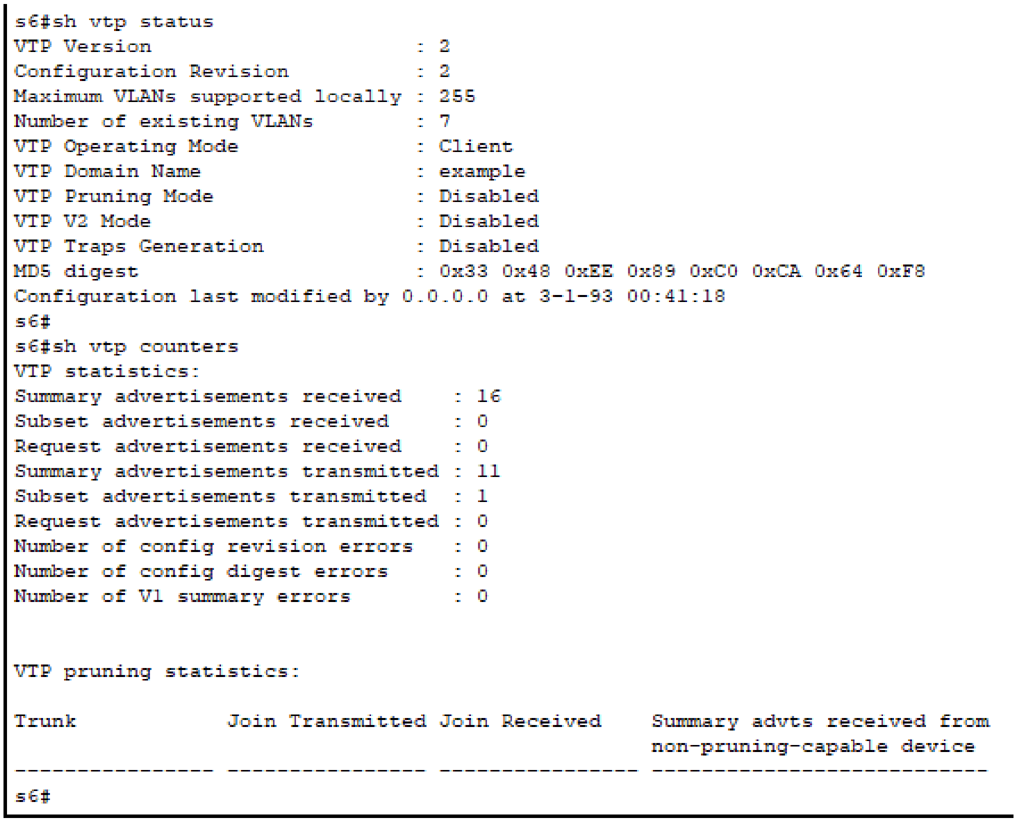
Figure 23: Dormitory

So in this area the dormitory router have to divided communication. One is for use data from database management network to get student information and one is for access ISP network. So I created two vlan vlan10 for access student information and vlan20 for access ISP internet. So I connected with inter VLAN communication. Here I also used VTP, STP and Trunk technology.



```
s5#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4
10   VLAN0010                         active    Fa0/5
20   VLAN0020                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
s5#
```

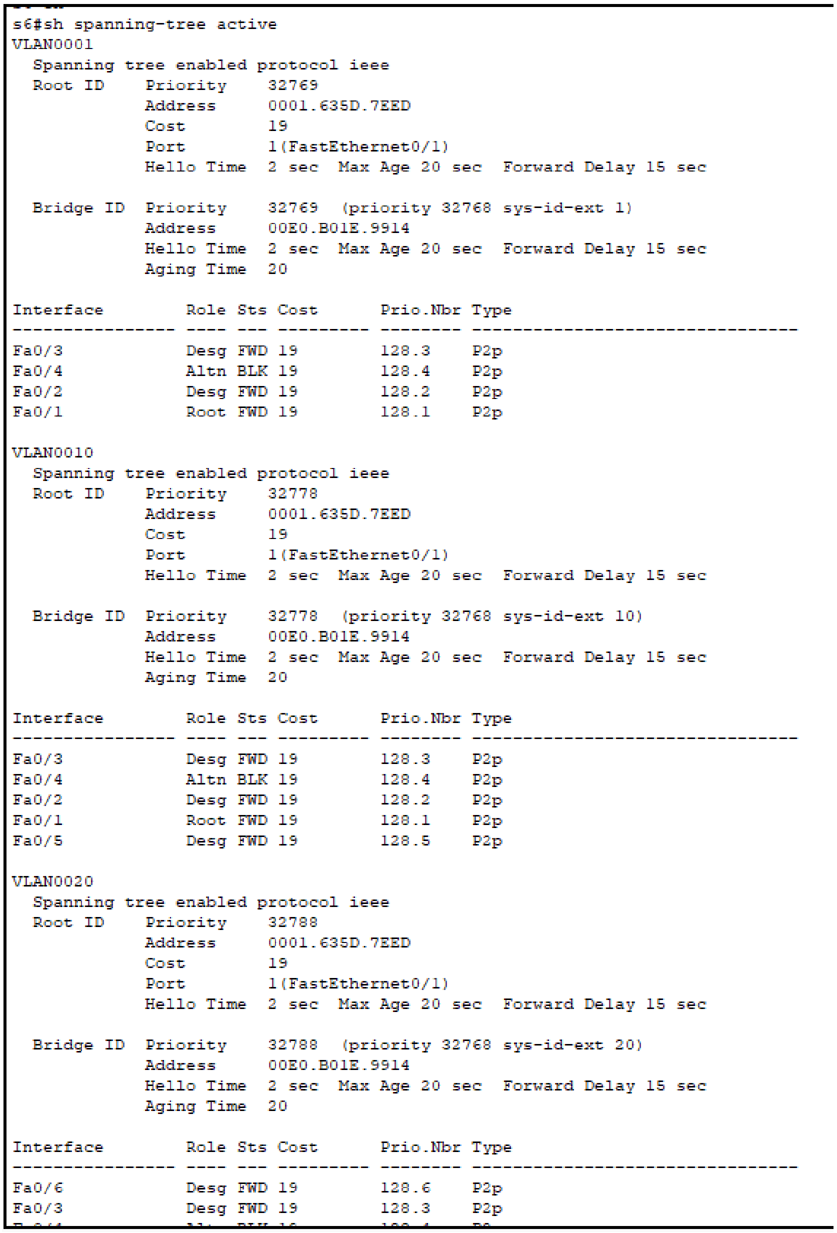
Figure 24: vlan brief in S5



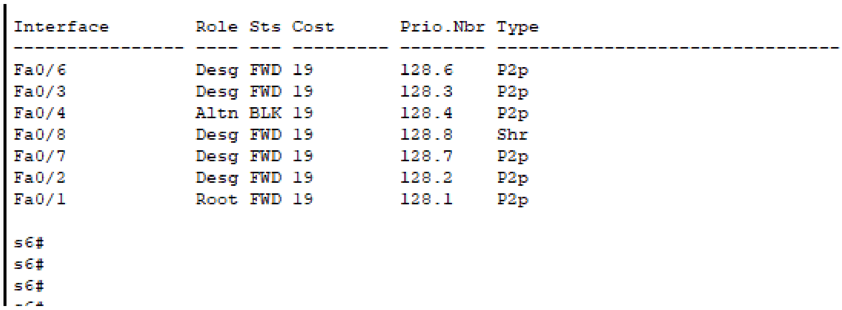
```
s6#sh vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : example
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x33 0x48 0xEE 0x89 0xC0 0xCA 0x64 0xF8
Configuration last modified by 0.0.0.0 at 3-1-93 00:41:18
s6#
s6#sh vtp counters
VTP statistics:
Summary advertisements received    : 16
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 11
Subset advertisements transmitted  : 1
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0


VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
s6#
```

Figure 25: VTP information in S6.

We can verify STP



```
s6#sh spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.635D.7EED
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00E0.B01E.9914
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.635D.7EED
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00E0.B01E.9914
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p
Fa0/5            Desg FWD 19        128.5    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     0001.635D.7EED
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     00E0.B01E.9914
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```



```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/8            Desg FWD 19        128.8    Shr
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p

s6#
s6#
s6#
```

Figure 26: STP information on s6.

5.3.7 Library management

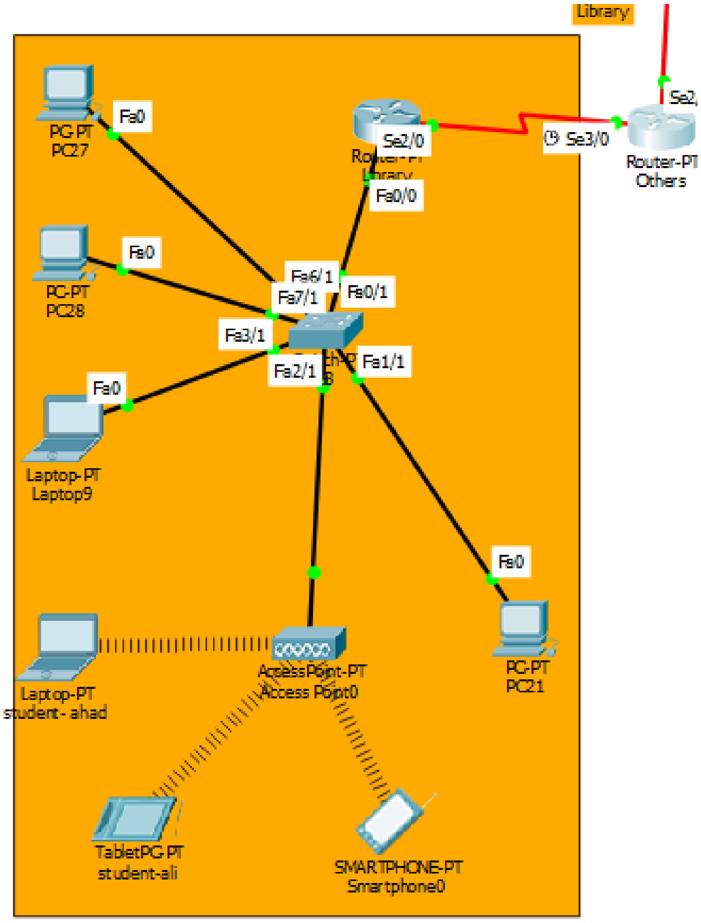
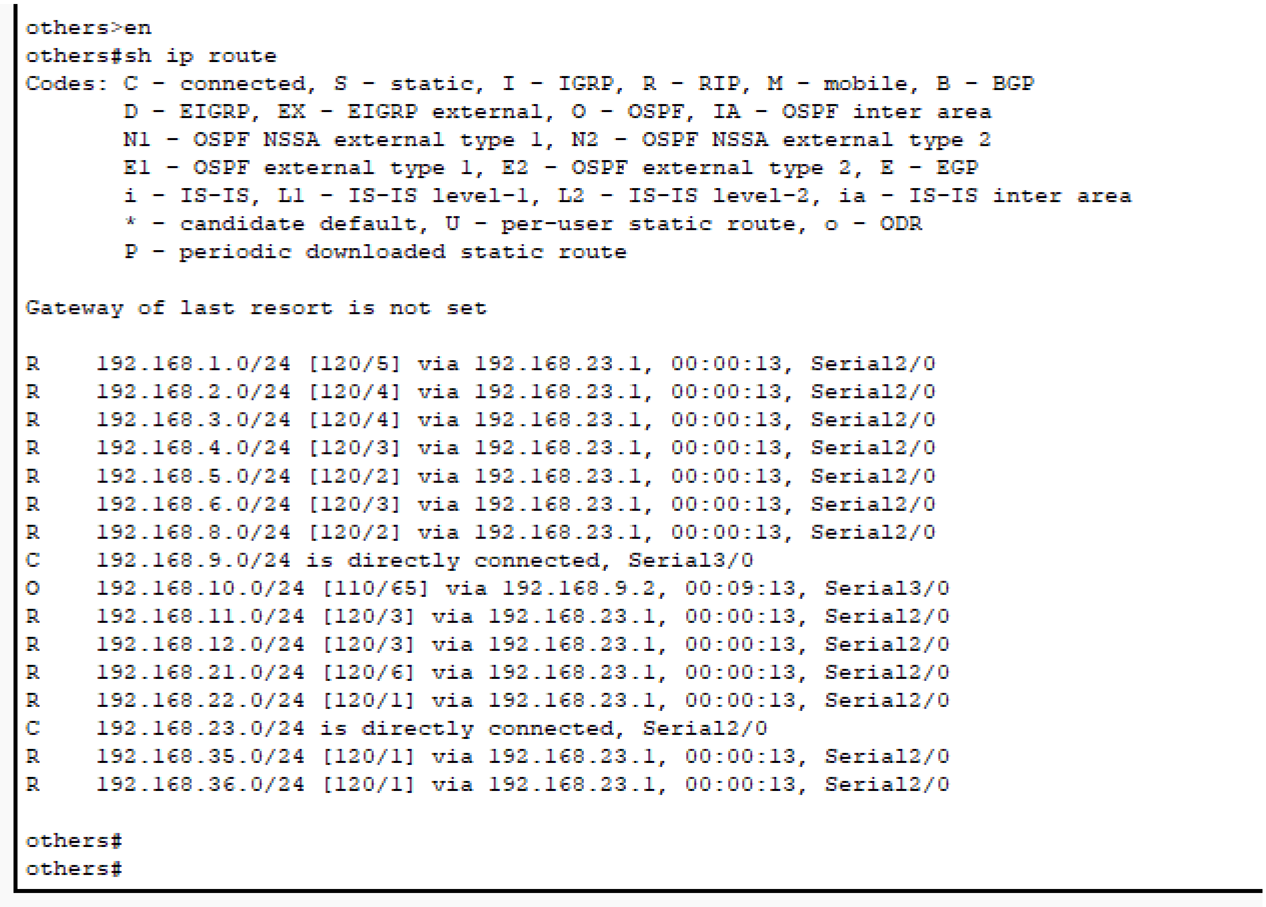


Figure 27: Library topology

In this topology I used OSPF protocol through Others router which connected to RIPv2 protocol. I used here redistribute technology to connect protocols.

```
#router rip

#version 2

#redistribute ospf 100 metric 1

#router ospf 100

#redistribute rip metric 1
```

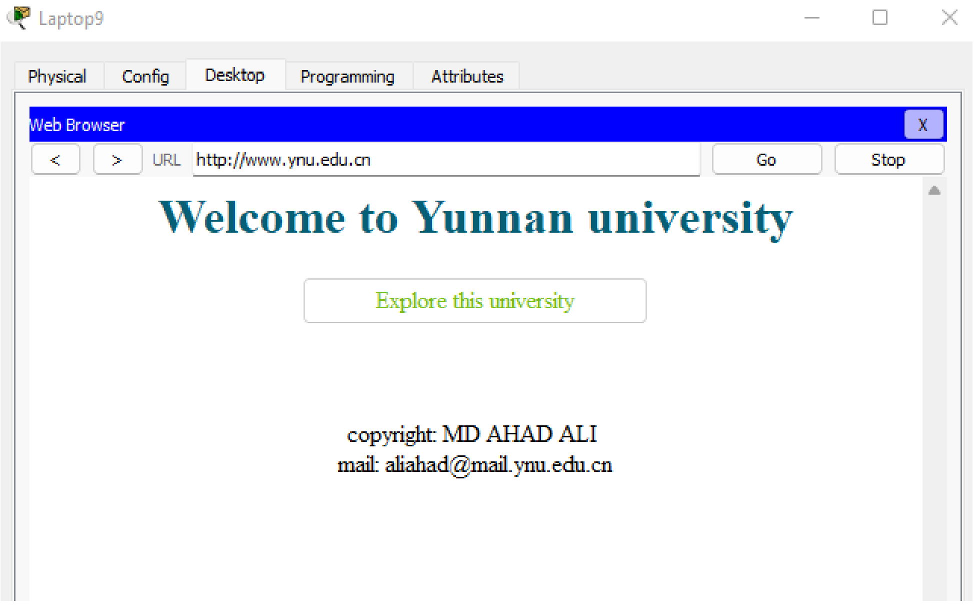
We can see the IP route information from Others router.



```
others>en
others#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.1.0/24 [120/5] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.2.0/24 [120/4] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.3.0/24 [120/4] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.4.0/24 [120/3] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.5.0/24 [120/2] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.6.0/24 [120/3] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.8.0/24 [120/2] via 192.168.23.1, 00:00:13, Serial2/0
C    192.168.9.0/24 is directly connected, Serial3/0
O    192.168.10.0/24 [110/65] via 192.168.9.2, 00:09:13, Serial3/0
R    192.168.11.0/24 [120/3] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.12.0/24 [120/3] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.21.0/24 [120/6] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.22.0/24 [120/1] via 192.168.23.1, 00:00:13, Serial2/0
C    192.168.23.0/24 is directly connected, Serial2/0
R    192.168.35.0/24 [120/1] via 192.168.23.1, 00:00:13, Serial2/0
R    192.168.36.0/24 [120/1] via 192.168.23.1, 00:00:13, Serial2/0

others#
others#
```

Figure 28: IP route

Now we can connect to ISP network.



URL: http://www.ynu.edu.cn

Welcome to Yunnan university

Explore this university

copyright: MD AHAD ALI
mail: aliahad@mail.ynu.edu.cn

Figure 29: Brows the Internet.

6 Conclusion

In the past, network designers had only a limited number of hardware options - routers or hubs - when purchasing a technology for their campus networks. Consequently, it was rare to make a hardware design mistake. Hubs were for wiring closets, and routers were for the data-center or main telecommunications operations. Recently, local-area networking has been revolutionized by the exploding use of LAN switching at Layer 2 (the data link layer) to increase performance and to provide more bandwidth to meet new data networking applications. LAN switches provide this performance benefit by increasing bandwidth and throughput for workgroups and local servers. Network designers are deploying LAN switches out toward the network's edge in wiring closets. These switches are usually installed to replace shared concentrator hubs and give higher-bandwidth connections to the end user.

7 Reference

[1] Computer Networking: A Top-down Approach- Book by Jim Kurose

[2] Networking All-in-One Desk Reference For Dummies- Book by Doug Lowe

[3] CCNA Routing and Switching ICND2 200-101 Official Cert Guide- Book by Wendell Odom