ABSTRACT

This project is to design a suitable network system for universities in developing countries. The aim was to design a network with high security and low cost. This project will help to enhanced education of developing countries. The advantages of networking can be seen clearly in terms of efficiency, security, manageability and cost as it allows collaboration between users in a wide area. To improve college campus network design, the technology used was creating LAN, WLAN and using cheap device to reduce cost of the network. But the network can also become better using routing protocols and other protocol. So, we are going to use such protocols using less number of devices and will also maintain the cost of the network less. To design such network, we are going to use software Cisco-Packet Tracer.

INTRODUCTION

Networking is refereed as connecting computers electronically for the purpose of sharing information. Resources such as a file, applications, printers & software are some common information shared in a networking. The advantages of networking can be seen clearly in terms of security, efficiency, manageability & and cost effectiveness as in allows collaboration between users in a wide range. The Switches and Router this device that play an important role in data transfer from one place to another using different technology such as a radio waves & wire. LAN network is made up of two or more computers connected together in a short distance usually at home, offices buildings or school. WAN is a network that covers wider area than LAN and usually covers cities, countries and the whole world. Several major LAN can be connected together to form a WAN. As a several devices are connected to network, it is important to ensure data collision does not happen when this device attempt to use data channel simultaneously. A set of rules called carrier sense multiple access/collision detection are used to detect and prevent collision in networks

NETWORKING REQUIREMENT

1. The active network components which are required (Routers , Switches).
2. The number of switches , routers which are required for the design.
3. The IP Design schema for the department.
4. Explanation of the details required to be configured on the Switch and how to create different departments with VLAN.
5. Explanation of how to restrict internet connection for R&D Department and allow access for the other departments with Access control lists on the Router.
6. Identify the feature on the router which is required for sharing the Internet for the users.
7. Identify the TCP/IP adapter parameters (IP address, Subnet mask, Default Gateway, DNS Server IP address) for the users.
8. Network Design Diagram.

SYSTEM DEVELOPMENT

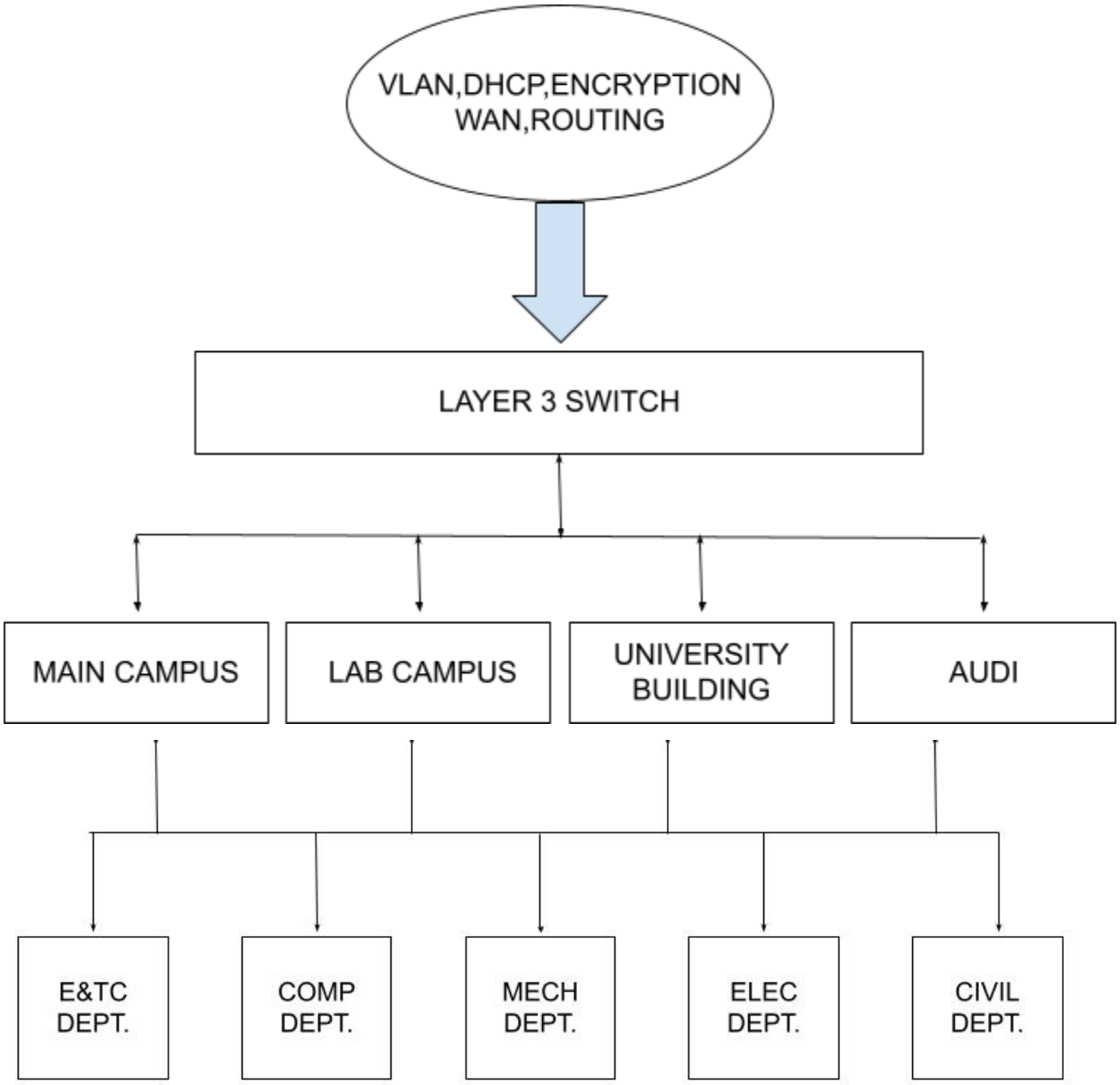
In this growing network area, it has become necessary to protect our network from unauthorized users and prevent it from hacking, so it is necessary to maintain security in our network by using various security option like port security, encryption using most secure routing protocol. To implement this, we need best devices which can support these protocols more efficiently. So, our discussion we decide to use layer 3 switches which work as switch as well as router, and using this router it is possible to implement EIGRP routing protocol. By using EIGRP it is possible for load balancing on parallel links between sites and also manages load balancing.

LAYER 3 SWITCHES

A layer 3 switch is a specialized hardware device used in network routing. Layer 3 switches technically have a lot in common with typical routers, and not just in physical appearance. Both can support the same routing protocols, inspect incoming packets and make dynamic routing decisions based on the source and destination addresses inside.

The key difference in layer 3 switches and routers lies in the hardware internals. The hardware inside a layer 3 switch blends that of typical switches and routers replacing some of router's software logic with integrated circuit hardware to offer better performance for local network

BLOCK DIAGRAM



NETWORK DESIGN STRATEGY

VLAN technology would be used to create the networks associated with different departments. Every department would be associated with an IP network and mapped with a specific vlan. Appropriate restrictions would be provided between the departments using access control lists. A DHCP server would used for providing dynamic IP addresses to the users on the network.

VLAN AND IP NETWORK DESIGN

VLAN's are created and mapped with each department.
1. VLAN 2 – SIRTC
2. VLAN 3 – SIEM
3. VLAN 4 – SIP
4. VLAN 5 - SIPS

IP networks are created for each VLAN and mapped with the same. The IP address range for users and systems which can be used on the specific department is also included.

VLAN	IP NETWORK ADDRESS	IP ADDRESS RANGE
VLAN 2	192.168.10.0/24	192.168.10.1 - 192.168.10.5
VLAN 3	172.168.10.0/24	172.168.10.1 - 172.10.5
VLAN 4	192.168.11.0/24	192.168.11.1 - 192.168.11.5
VLAN 5	172.168.11.0/24	172.168.11.1 - 172.168.11.2

REQUIREMENTS ANALYSIS OF ACTIVE NETWORKING COMPONENTS

SWITCHES

An normal university usually has 5 departments BIOT,ELEC,MECH,CIVIL,COMP, and each department has many systems which are connected to their respective servers and then used. The total number of LAN users is 60, which consists of the teachers and the students. As the modern world these connections are on the wireless networks, 3 access points are proposed for accommodating the 100 users. This would require 60 ports for the LAN users, 3 ports for the access points, one port for the authority handling the network and 1 for DHCP. So a total of 65 ports are required. Switches are available as 24 or 48 port capacity. So 3 nos of 24 port switches, which support vlans are proposed.

ROUTERS

A router which supports high speed internet connection, with the appropriate interface is required. The router also requires an interface which supports 802.1q, which would be used for routing between vlans and access restriction between the vlans. 1 nos router is required.

ACCESS POINTS

As the estimated number of users are 100, a total of 3 access points are proposed. This is proposed based on the load which can be shared on the access points.

DHCP

A DHCP server is required for assigning dynamic IP addresses to users on the network. The DHCP server service on Windows 2008 is leveraged for the purpose.

NETWORK IMPLEMENTATION PLAN

Ports on the switches are made members of respective vlans. The computers belonging to the respective departments are connected to the respective ports. Intervlan routing is setup on the router, where appropriate access control lists are provided for restricting communication as per the project requirement. The access points are connected to the ports which are on VLAN 4 on the switch as it is used for students vlan. The DHCP server is setup on VLAN 2, and configured with multiple DHCP scopes to provide IP addresses from respective vlans to the users on the network. IP Helper-address feature is configured on the router for users belonging to the flight services provider and guest network to receive dynamic IP addresses from the DHCP server residing on the university authority network.

The DHCP server and the student authority server are connected to ports on the switch, which are members of VLAN 2, the student authority VLAN. The respective PC's belonging to the departments are connected to the appropriate ports on the switch. The access points are connected to ports on the switches, which are members of VLAN 4, which is associated with the guest VLAN. The student users connect to the access points and are assigned IP address in the appropriate VLAN range.

NETWORK CONFIGURATION

1. The DHCP server is connected to a port, which is a member of VLAN 2. The IP address of the DHCP Server is 172.168.11.1 and the IP address of the university authority server is 172.168.11.2.
2. The access point is configured with IP addresses belonging to the VLAN 4 network address range.

3. Switch configuration

The following configuration details the actual setup which needs to be performed on a Cisco switch.

a. Create VLAN's, VLAN 2, VLAN 3, VLAN 4 AND VLAN 5 with respective names on the switch.

switch(config)#vlan 2

switch(config-vlan)#name University authority

switch(config-vlan)#exit

switch(config)#vlan 3

switch(config-vlan)#name Students service providers

switch(config-vlan)#exit

switch(config)#vlan 4

switch(config-vlan)#name Students

switch(config-vlan)#exit

switch(config)#vlan 5

switch(config-vlan)#name Guests

switch(config-vlan)#exit

b. Configure appropriate ports on the switch as members of respective VLAN. Only two ports for each vlans are displayed. This can be added based on requirement.

switch(config)#interface fastethernet 0/2

switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 2

```
switch(config-if)#exit
switch(config)#interface fastethernet 0/3
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2
switch(config-if)#exit
switch(config)#interface fastethernet 0/10
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 3
switch(config-if)#exit
switch(config)#interface fastethernet 0/11
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 3
switch(config-if)#exit
switch(config)#interface fastethernet 0/20
switch(conf ig-if)#switchport mode access
switch(config-if)#switchport access vlan 4
switch(config-if)#exit
switch(config)#interface fastethernet 0/21
switch(config-if)#switchport mode access
```

switch(config-if)#switchport access vlan 4

switch(config-if)#exit

switch(config)#interface fastethernet 0/21

switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 5

switch(config-if)#exit

4.Router configuration

The following configuration details the actual setup which needs to be performed on a Cisco router.

a. The interface connected to the internet is configured with the appropriate IP address (192.168.10.1).

Note: In real time, this would be the public IP address. The details are shown below.

router(config)#interface fastethernet 0/0

router(config-if)#no shutdown

router(config-if)#exit

router(config)#interface fastethernet 0/1

router(config-if)#ip address 192.168.10.1 255.255.255.0

router(config-if)#no shutdown

Note: In real time environment, PAT (Port address translation) is configured on the interface for sharing the internet. A default route is also setup on the router to forward all packets to the gateway IP address, which the ISP provides.

b. Sub interfaces on the router on the physical interface fastethernet 0/0 are mapped with appropriate VLAN and IP address. The IP address configured on the router, would be the default gateway address for users belonging to the respective vlan. IP addresses 192.168.10.1, 172.168.10.1,192.168.11.1 and 172.168.11.1 are mapped with the VLAN's, VLAN 2,3,4,5.

router(config)#interface fastethernet 0/0.1

router(conf ig-subif)#encapsulation dot1Q 2

router(config-subif)#ip address 192.168.10.1 255.255.255.0

router(config-subif)#no shutdown

router(config-subif)#exit

router(config)#interface fastethernet 0/0.2

router(config-subif)#encapsulation dot1Q 3

router(config-subif)#ip address 172.168.10.1 255.255.255.0

router(config-subif)#no shutdown

router(config-subif)#exit

router(config)#interface fastethernet 0/0.3

router(config-subif)#encapsulation dot1Q 4

router(config-subif)#ip address 192.168.11.1 255.255.255.0

router(config-subif)#no shutdown

router(config-subif)#encapsulation dot1Q 5

router(config-subif)#ip address 172.168.11.1 255.255.255.0

router(config-subif)#no shutdown

c. The IP Helper –address is configured on the VLAN 4 and VLAN 5 interfaces of the router. This is configured for users belonging to the respective vlans, to reach the DHCP server for obtaining dynamic IP addresses. The configurations are shown below. The IP address of the DHCP server is 192.168.10.2.

router(config)#interface fastethernet 0/0.2

router(config-subif)#ip helper-address 172.168.10.2

router(config-subif)#exit

router(config)#interface fastethernet 0/0.3

router(config-subif)#ip helper-address 192.168.10.2

router(config-subif)#exit

d. Appropriate access control lists are configured on the router. To deny access from the guest network to the other two networks an extended ACL is configured. The configuration is shown below. The first two lines would deny the access from the students network to the university authority and students service provider networks. The third entry would allow all other traffic. This is for the internet connection. The access control list is applied in the guest vlan interface on the router as inbound.

router(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255 192.168.2.0 0.0.0.255

router(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255

router(config)#access-list 101 permit ip any any

router(config)#interface fastethernet 0/0.3

router(config-subif)#ip access-group 101 inbound

e. Access control lists are configured to restrict access from the student service network to the university authority network. The first line allows the student service provider network to access the university authority server. The second line denies all other communication to the university authority network as per the requirement. The third line allows all other communication, which would be internet. The access list is applied as inbound on the VLAN interface corresponding to the university authority network.

router(config)#access-list 102 permit ip 192.168.3.0 0.0.0.255 host 192.168.2.3

router(config)#access-list 102 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255

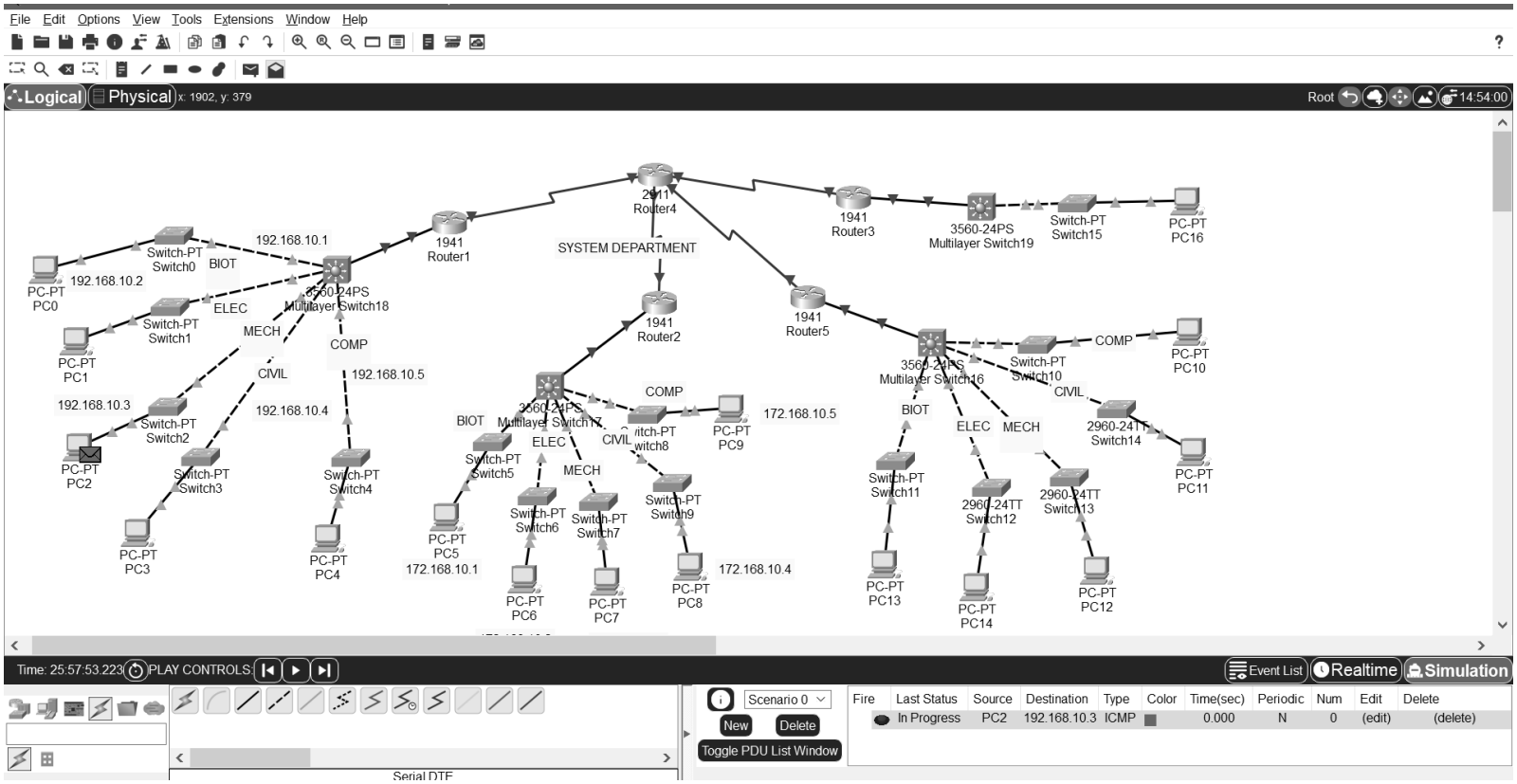
router(config)#access-list 101 permit ip any any

router(config)#interface fastethernet 0/0.2

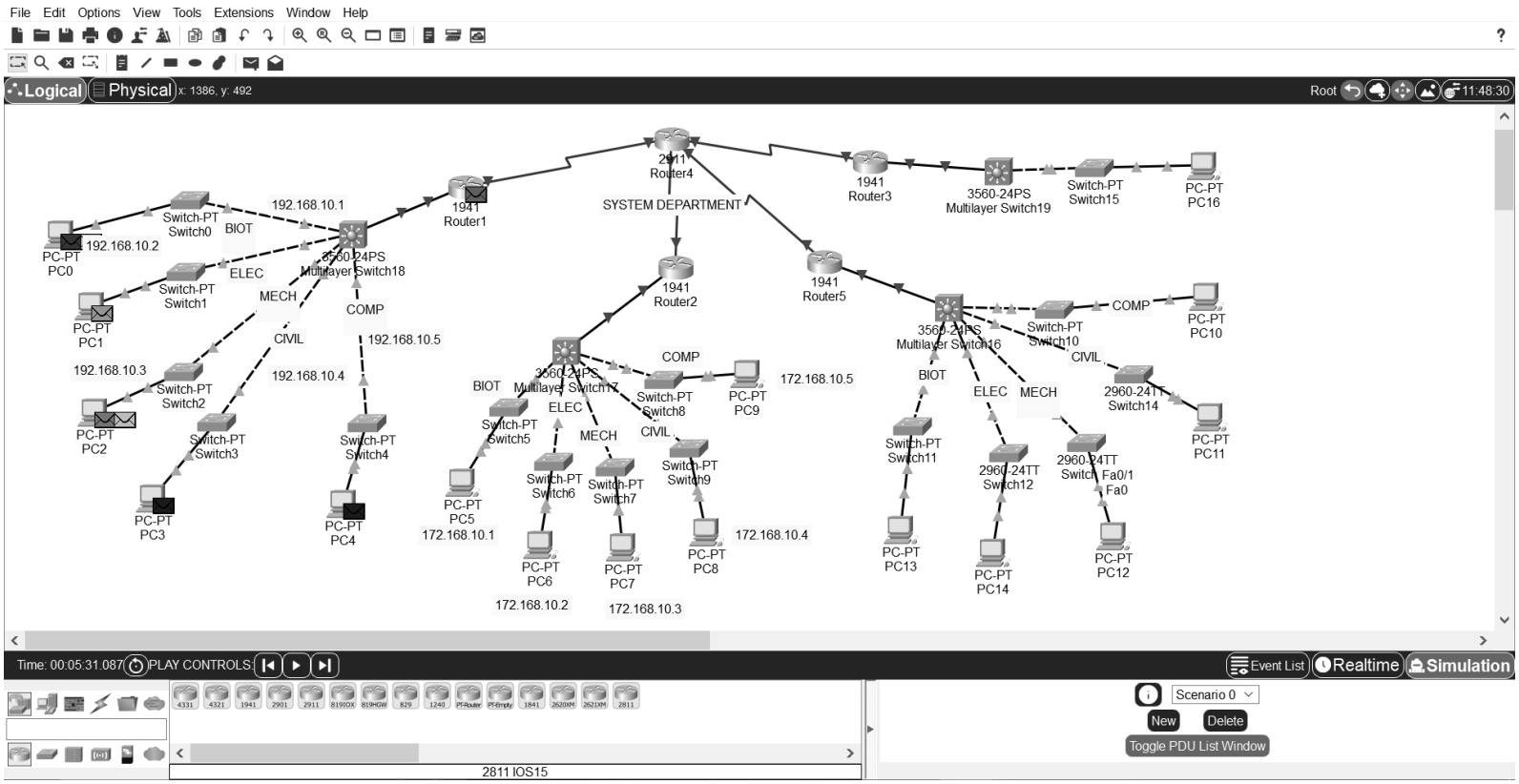
router(config-subif)#ip access-group 102 inbound

5. DHCP Configuration
The DHCP server is configured on Windows 2008. There are four DHCP scopes, which are created for each of the four VLAN's.
a. Start the DHCP service
b. Create new scope for the university authority network.
c. Configure the gateway address as the IP address of the VLAN interface configured on the router.
d. Configure the DNS server for the scope following the same above steps. This can be the DNS server provided by the ISP or can also be the router and the router point to the appropriate DNS server provided by the ISP.
e. Activate the Scope.
f. The similar steps are followed for the other networks.

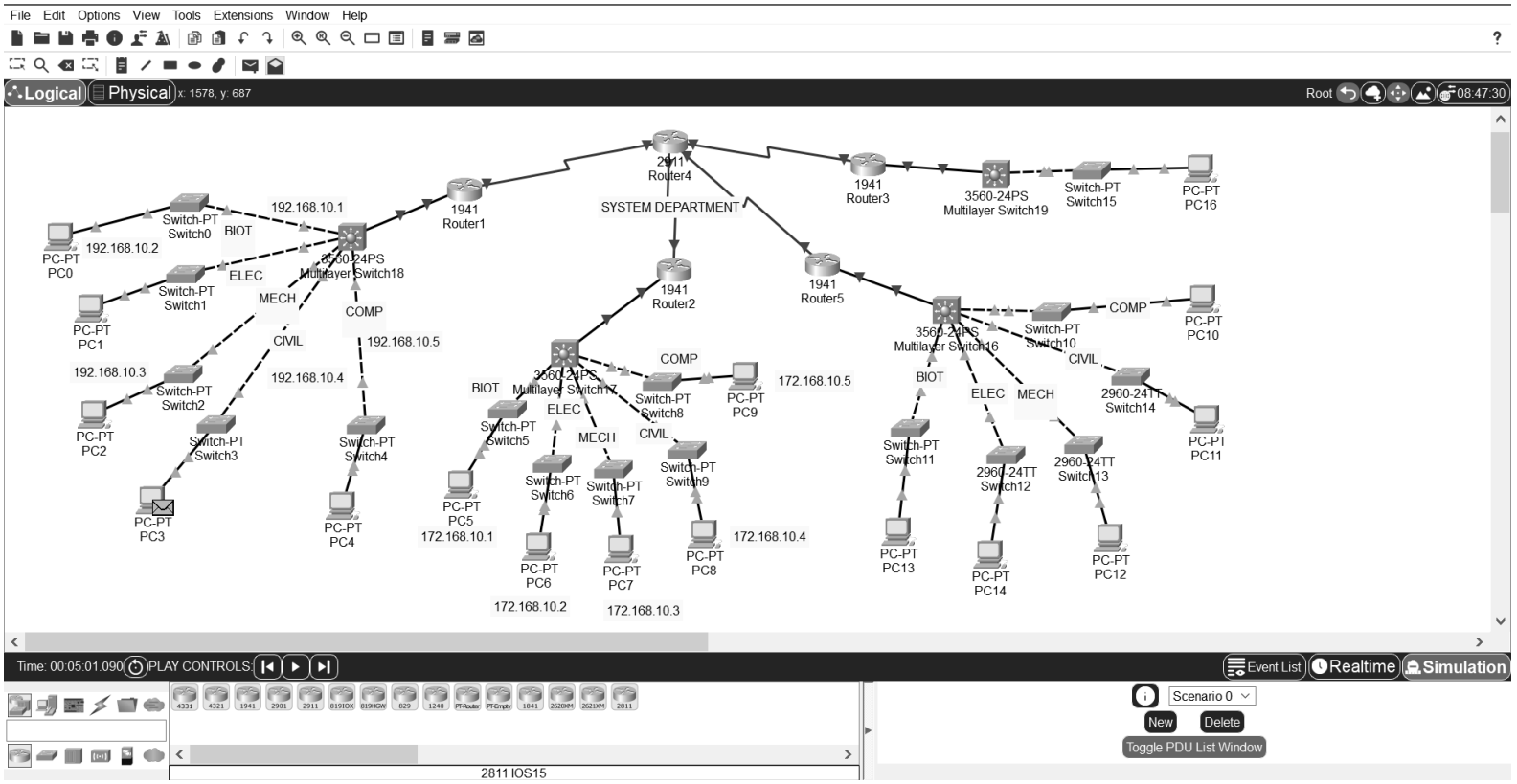
CISCO DIAGRAM OF NETWORK IMPLEMENTATION(COLLEGE CAMPUS)



Packets (data) Sending from MECHANICAL Department



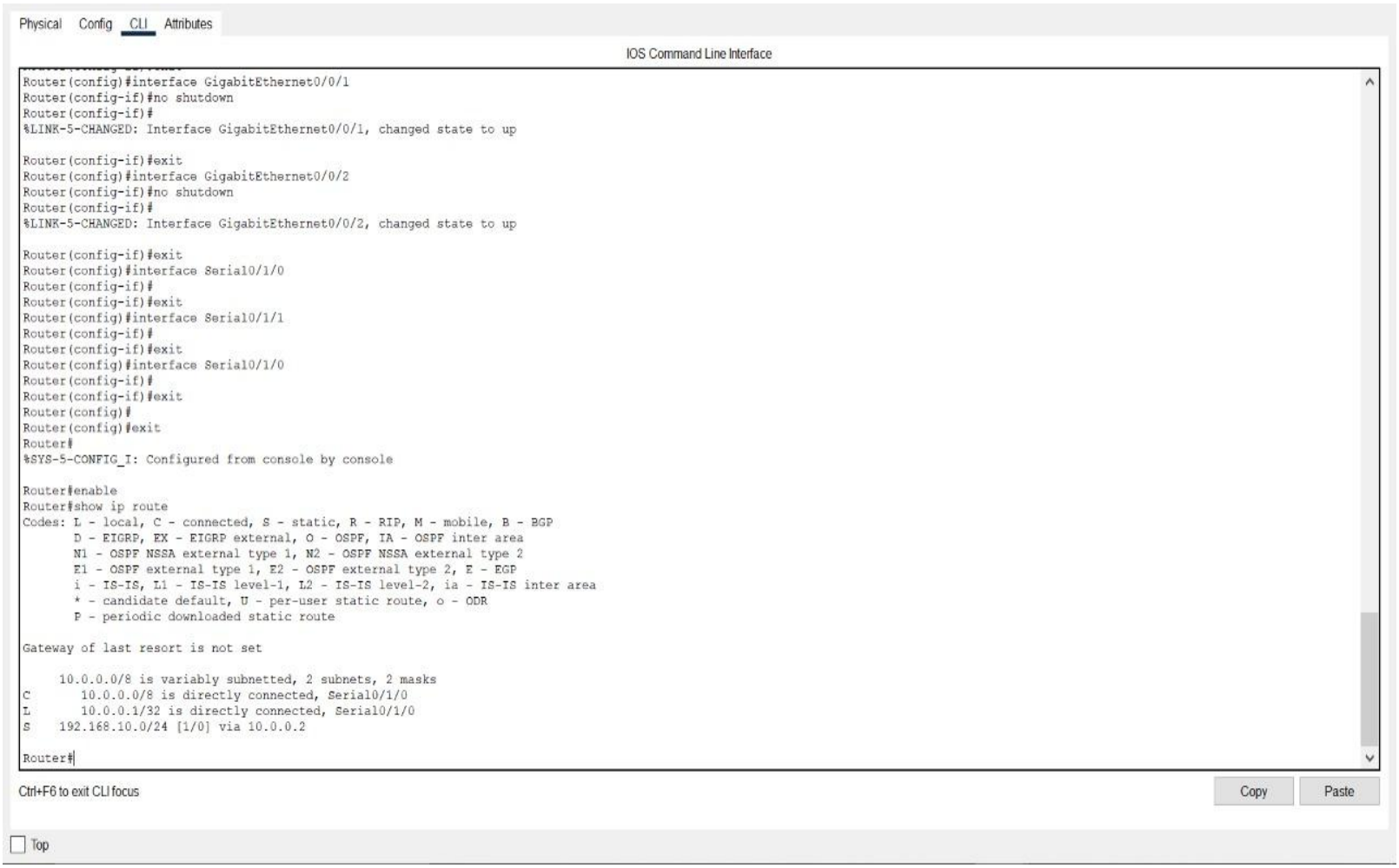
Broadcasting to know the Address.



The Packet (data) Receiving at CIVIL Department.

In Above shown figure shows implemented network on college campus. To check whether the communication is taking place properly or not we tried to send packets (data) between two different departments of MAIN CAMPUS. The data is being transferred from mechanical to department to civil department. But before it sends data it is necessary for the router to know the destination address.Hence, for knowing its address router broadcast the HELLO packet to every machine and learns the machine address and the packet is being received by the machine of civil department. This shows that the communication is being possible and the network is working.

SHOW COMMANDS



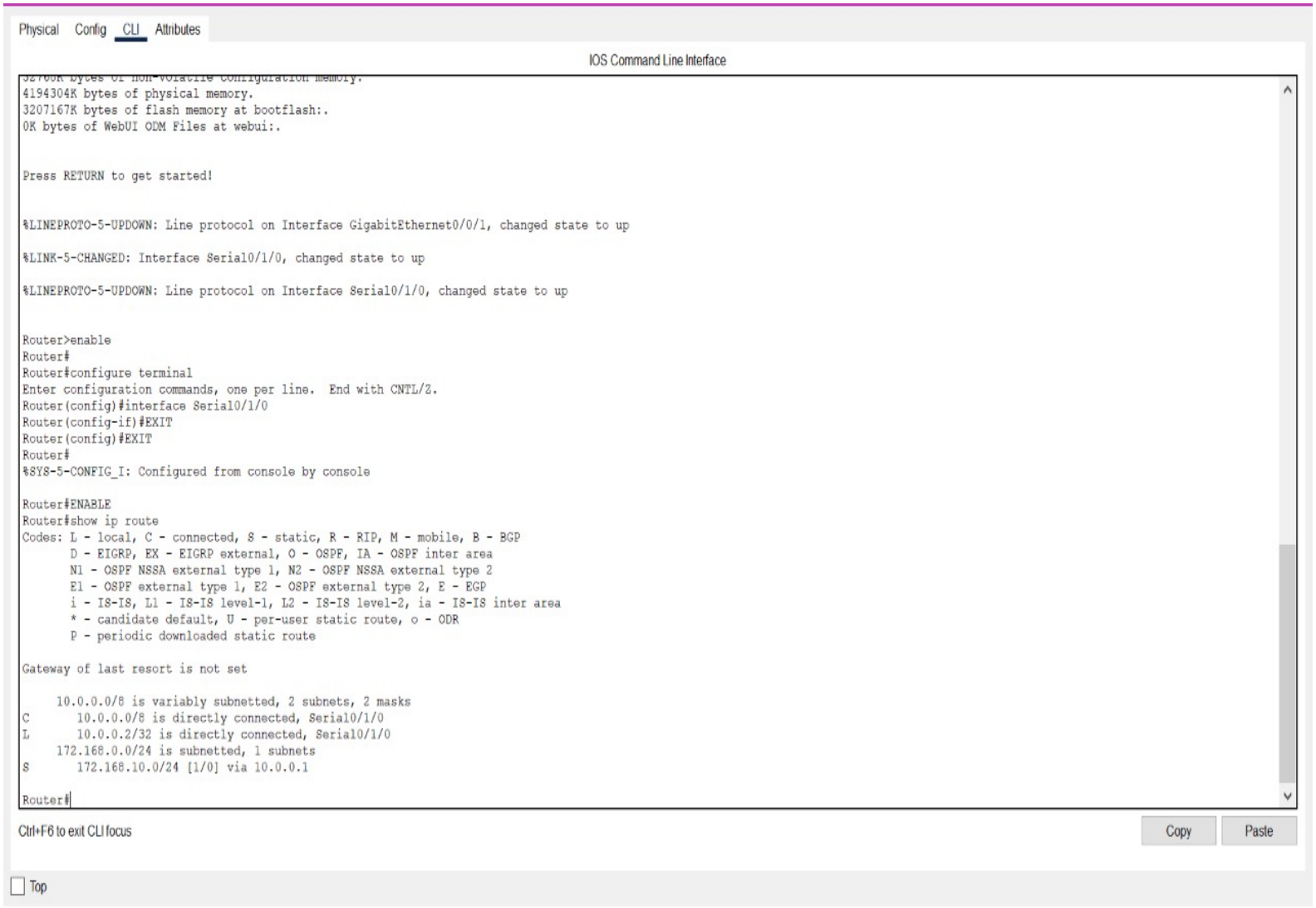
Show ip route command of main campus

```
Router#show ip protocol
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  up                    up
GigabitEthernet0/0/1   unassigned      YES unset  up                    down
GigabitEthernet0/0/2   unassigned      YES unset  up                    down
Serial0/1/0            10.0.0.1        YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Show ip interface brief

```
Router#enable
Router#show ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 12 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/1/0           12 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
        10.0.0.0
        172.168.0.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
Distance: (default is 120)
Router#
```

Show ip protocol



Show ip route command of lab campus

```
Router#show ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 10 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/1/0           12 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
        10.0.0.0
        192.168.10.0
Passive Interface(s):
Routing Information Sources:
        Gateway         Distance      Last Update
Distance: (default is 120)
```

Show ip protocol

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  up                    down
GigabitEthernet0/0/1   unassigned      YES unset  up                    up
GigabitEthernet0/0/2   unassigned      YES unset  up                    down
Serial0/1/0            10.0.0.2        YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Show ip interface brief

HARDWARE AND SOFTWARE INVENTORY LIST

ITEM	MODEL	QUANTITY
ROUTER	Cisco 2600 Series 1941 Router with high speed interface for internet connection	1
SWITCHES	Cisco 2950 Catalyst switch 3 layer switch	15,5
ACCESS POINTS	Cisco airnet 1200 Access Point	5
SERVER	IBM/Dell	1/2
OPERATING SYSTEM	Windows 2008	1 License
PC	IBM/Dell/HP etc.	As per the university strength

CONCLUSION

This project has proven that a standard network system can be designed with less cost. Although we used the cheapest devices in designing the network, the security of this network turned out to be very strong. This is because the firewall and backup devices used in this network are of good quality. All networks need many servers for doing their work. For this research, we did not use all servers because of cost, but we used some important servers such as DHCP. These servers help the network to perform their functions in a smooth way. It can be seen in this research that various costs were minimized in order to maximize the quality of the designed network. Although there may have been some challenges in this project due to some financial constraints, at the end our aim was achieved by designing a network for developing universities with minimal cost. For example, we made use of some devices for the network security, but the most interesting part is that, at the end of the day, all challenges and constraints were overcome.

REFERENCES

[1] Jagdish K.P & Pavan Kumar, 'Enhancing the College Network', Department of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore IJIRSET- International Journal of Innovative Research in Science, Engineering & Technology, ISSN (online):2319-8753, Vol.7, May 2018.
[2] Md. Waliullah, 'Wireless LAN Security Threats & Vulnerabilities', Department of Computer Science & Engineering, IJACSA-International Journal of Advanced Computer Science and Application, Vol. 5,2014.
[3] Shivam Adke & Rutuja Bhawar, 'College Campus Network Design and Security', Department of Electronics & Telecommunication Engineering, Sandip Institute of Technology & Research Centre, Nashik, IJAREEIEInternational Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (online):2278-8875, Vol. 7, March 2018.
[4] Mohammed Nadir Bin Ali, Mohammed Emran Hossain & Md. Masud Parvez, 'Design and Implementation of a Secure Campus Network', Daffodil International University, IJETAE- International Journal of Emerging Technology and Advanced Engineering, ISSN:2250-2459, Vol. 5, July 2015.
[5] Prof. Ms. Swati Pawar, Prof. V.D. Ugale, Ankita Nirmal, Pallavi Badgujar, Swapnali Borade "Review paper Based on NETWORK DESIGN FOR COLLEGE CAMPUS"