The Network comprises of the following elements:

-First floor- (Sales and Marketing Department-120 users expected, Human Resource and Logistics Department-120 users expected).

-Second floor- (Finance and Accounts Department-120 users expected, Administrator and Public Relations Department-120 users expected).

-Third floor- (ICT-120 users expected, Server Room-12 devices expected).

-Use Cisco Packet Tracer to design and implement the network solution.

-Use hieratical model providing redundancy at every layer i.e. two routers and two multilayer switches are expected to be used to provide redundancy.

-The network is also expected to connect to at least two ISPs to provide redundancy and each router to the connected to the two ISPs.

-Each department is required to have a wireless network for the users.

-Each department should be in a different VLAN and in different subnetwork.

-Provided a base network of 172.16.1.0, carry out subnetting to allocate the correct number of IP addresses to each department.

-The company network is connected to the static, public IP addresses (Internet Protocol) 195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30 and 195.136.17.12/30 connected to the two Internet providers.

-Configure basic device settings such as hostnames, console password, enable password, banner messages, disable IP domain lookup.

-Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.

-The Multilayer switches are expected to carry out both routing and switching functionalities thus will be assigned IP addresses.

-All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server room.

-Devices in the server room are to be allocated IP address statically.

-Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.

-Configure SSH in all the routers and layer three switches for remote login.

-Configure port-security for the Finance and Accounts department to allow only one device to connect to a switchport, use sticky method to obtain mac-address and violation mode shutdown.

-Configure NAT to use the respective outbound router interface IPv4 address, implement the necessary ACL rule.

-Test Communication, ensure everything configured is working as expected.

Technologies Implemented

-Creating a network topology using Cisco Packet Tracer.

-Hierarchical Network Design.

-Connecting Networking devices with Correct cabling.

-Configuring Basic device settings.

-Creating VLANs and assigning ports VLAN numbers.

-Subnetting and IP Addressing.

-Configuring Inter-VLAN Routing on the Multilayer switches (Switch Virtual Interface).

-Configuring Dedicated DHCP Server device to provide dynamic IP allocation.

-Configuring SSH for secure Remote access.

-Configuring OSPF as the routing protocol.

-Configuring NAT Overload(Port Address Translation PAT).

-Configuring standard and extended Access Control Lists ACL.

-Configuring switchport security or Port-Security on the switches.

-Configuring WLAN or wireless network (Cisco Access Point).

-Host Device Configurations.

-Configuring ISP routers.

-Test and Verifying Network Communication.

ISP Routers :

ISP1:

interface Serial0/0/0

ip address 195.136.17.2 255.255.255.252
clock rate 64000
exit
interface Serial0/0/1
ip address 195.136.17.10 255.255.255.252
clock rate 64000
exit
router ospf 10
router-id 5.5.5.5
network 195.136.17.0 0.0.0.3 area 0
network 195.136.17.8 0.0.0.3 area 0
exit
do wr

ISP2:
interface Serial0/0/0
ip address 195.136.17.6 255.255.255.252
clock rate 64000
exit
interface Serial0/0/1
ip address 195.136.17.14 255.255.255.252
clock rate 64000
exit
router ospf 10
router-id 6.6.6.6
network 195.136.17.4 0.0.0.3 area 0
network 195.136.17.12 0.0.0.3 area 0
exit
do wr

Core Layer routers :
CORE-RT1:
enable
configure terminal
hostname CORE_RT1_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption
do write
ip domain name cisco.net
username admin password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface gig0/0
ip address 172.16.3.146 255.255.255.252

```
no shutdown
exit
interface gig0/1
ip address  172.16.3.154 255.255.255.252
no shutdown
exit
interface se0/0/0
ip address 195.136.17.1 255.255.255.252
no shutdown
interface se0/0/1
ip address 195.136.17.5 255.255.255.252
no shutdown
exit
router ospf 10
router-id 3.3.3.3
network 172.16.3.144 0.0.0.3 area 0
network 172.16.3.152 0.0.0.3 area 0
network 195.136.17.0 0.0.0.3 area 0
network 195.136.17.4 0.0.0.3 area 0
exit
ip nat inside source list 1 interface se0/0/0 overload
ip nat inside source list 1 interface se0/0/1 overload
access-list 1 permit 172.16.1.0 0.0.0.127
access-list 1 permit 172.16.1.128 0.0.0.127
access-list 1 permit 172.16.2.0 0.0.0.127
access-list 1 permit 172.16.2.128 0.0.0.127
access-list 1 permit 172.16.3.0 0.0.0.127
access-list 1 permit 172.16.3.128 0.0.0.15
interface range gig0/0-1
ip nat inside
interface se0/0/0
ip nat outside
interface se0/0/1
ip nat outside
exit
ip route 0.0.0.0 0.0.0.0 se0/0/0
ip route 0.0.0.0 0.0.0.0 se0/0/1 70
do wr
---------------------------
CORE-RT2:
enable
configure terminal
hostname CORE_RT2_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption
do write
ip domain name cisco.net
username admin password cisco
crypto key generate rsa
```

```
1024
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface gig0/0
ip address  172.16.3.150 255.255.255.252
no shutdown
exit
interface gig0/1
ip address  172.16.3.158 255.255.255.252
no shutdown
exit
interface se0/0/0
ip address 195.136.17.9 255.255.255.252
no shutdown
interface se0/0/1
ip address 195.136.17.13 255.255.255.252
no shutdown
exit
router ospf 10
router-id 4.4.4.4
network 172.16.3.148 0.0.0.3 area 0
network 172.16.3.156 0.0.0.3 area 0
network 195.136.17.8 0.0.0.3 area 0
network 195.136.17.12 0.0.0.3 area 0
exit
ip nat inside source list 1 interface se0/0/0 overload
ip nat inside source list 1 interface se0/0/1 overload
access-list 1 permit 172.16.1.0 0.0.0.127
access-list 1 permit 172.16.1.128 0.0.0.127
access-list 1 permit 172.16.2.0 0.0.0.127
access-list 1 permit 172.16.2.128 0.0.0.127
access-list 1 permit 172.16.3.0 0.0.0.127
access-list 1 permit 172.16.3.128 0.0.0.15
interface range gig0/0-1
ip nat inside
interface se0/0/0
ip nat outside
interface se0/0/1
ip nat outside
exit
ip route 0.0.0.0 0.0.0.0 se0/0/0
ip route 0.0.0.0 0.0.0.0 se0/0/1 70
do wr
```

Access Layer Layer 3 Switches :

L3S-1 :

```
enable
configure terminal
hostname L3S_1_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
```

```
password cisco
login
exit
enable password cisco
service password-encryption
do write
ip domain name cisco.net
username admin password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface range gig1/0/1-6
switchport mode trunk
exit
vlan 10
name Sales_and_Marketing_Department
vlan 20
name Human_Resource_and_Logistics_Department
vlan 30
name Finance_and_Accounts_Department
vlan 40
name Administrator_and_Public_Relations_Department
vlan 50
name ICT
vlan 60
name Server_Room
exit
interface range gig1/0/7-8
no switchport
exit
interface gig1/0/7
ip address 172.16.3.145 255.255.255.252
no shutdown
exit
interface gig1/0/8
ip address 172.16.3.149 255.255.255.252
no shutdown
exit
ip routing
router ospf 10
router-id 2.2.2.2
network 172.16.1.0 0.0.0.127 area 0
network 172.16.1.128 0.0.0.127 area 0
network 172.16.2.0 0.0.0.127 area 0
network 172.16.2.128 0.0.0.127 area 0
network 172.16.3.0 0.0.0.127 area 0
network 172.16.3.128 0.0.0.15 area 0
network 172.16.3.144 0.0.0.3 area 0
network 172.16.3.148 0.0.0.3 area 0
exit
interface vlan 10
```

```
no shutdown
ip address 172.16.1.1 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 20
no shutdown
ip address 172.16.1.129 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 30
no shutdown
ip address 172.16.2.1 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 40
no shutdown
ip address 172.16.2.129 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 50
no shutdown
ip address 172.16.3.1 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 60
no shutdown
ip address 172.16.3.129 255.255.255.240
ip helper-address 172.16.3.130
exit
ip route 0.0.0.0 0.0.0.0 gig1/0/7
ip route 0.0.0.0 0.0.0.0 gig1/0/8 70
do wr
-------------------------
L3S-2 :
enable
configure terminal
hostname L3S_2_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption
do write
ip domain name cisco.net
username admin password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
```

```
interface range gig1/0/1-6
switchport mode trunk
exit
vlan 10
name Sales_and_Marketing_Department
vlan 20
name Human_Resource_and_Logistics_Department
vlan 30
name Finance_and_Accounts_Department
vlan 40
name Administrator_and_Public_Relations_Department
vlan 50
name ICT
vlan 60
name Server_Room
exit
interface range gig1/0/7-8
no switchport
exit
interface gig1/0/7
ip address 172.16.3.153 255.255.255.252
no shutdown
exit
interface gig1/0/8
ip address 172.16.3.157 255.255.255.252
no shutdown
exit
ip routing
router ospf 10
router-id 1.1.1.1
network 172.16.1.0 0.0.0.127 area 0
network 172.16.1.128 0.0.0.127 area 0
network 172.16.2.0 0.0.0.127 area 0
network 172.16.2.128 0.0.0.127 area 0
network 172.16.3.0 0.0.0.127 area 0
network 172.16.3.128 0.0.0.15 area 0
network 172.16.3.152 0.0.0.3 area 0
network 172.16.3.156 0.0.0.3 area 0
exit
interface vlan 10
no shutdown
ip address 172.16.1.1 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 20
no shutdown
ip address 172.16.1.129 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 30
no shutdown
ip address 172.16.2.1 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 40
```

no shutdown
ip address 172.16.2.129 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 50
no shutdown
ip address 172.16.3.1 255.255.255.128
ip helper-address 172.16.3.130
exit
interface vlan 60
no shutdown
ip address 172.16.3.129 255.255.255.240
ip helper-address 172.16.3.130
exit
ip route 0.0.0.0 0.0.0.0 gig1/0/7
ip route 0.0.0.0 0.0.0.0 gig1/0/8 70
do wr

Distribution Layer Switches Configuration:
Sales and Marketing Department :
enable
configure terminal
hostname Sales_and_Marketing_Department_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption
interface range fa0/1-2
switchport mode trunk
exit
vlan 10
name Sales_and_Marketing_Department
exit
interface range fa0/3-24
switchport mode access
switchport access vlan 10
exit
vlan 99
name BlackHole
exit
interface range gig0/1-2
switchport mode access
switchport access vlan 99
shutdown
exit
do write

Human Resource and Logistics Department :
enable
configure terminal

```
hostname Human_Resource_and_Logistics_Department_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption
interface range fa0/1-2
switchport mode trunk
exit
vlan 20
name Human_Resource_and_Logistics_Department
exit
interface range fa0/3-24
switchport mode access
switchport access vlan 20
exit
vlan 99
name BlackHole
exit
interface range gig0/1-2
switchport mode access
switchport access vlan 99
shutdown
exit
do write
```

Finance and Accounts Department :

```
enable
configure terminal
hostname Finance_and_Accounts_Department_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption
interface range fa0/1-2
switchport mode trunk
exit
vlan 30
name Finance_and_Accounts_Department
exit
interface range fa0/3-24
switchport mode access
switchport access vlan 30
exit
vlan 99
name BlackHole
exit
interface range gig0/1-2
```

switchport mode access
switchport access vlan 99
shutdown
exit
interface range fa0/3-24
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
exit
do write

Administrator and Public Relations Department
enable
configure terminal
hostname Administrator_and_Public_Relations_Department_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption
interface range fa0/1-2
switchport mode trunk
exit
vlan 40
name Administrator_and_Public_Relations_Department
exit
interface range fa0/3-24
switchport mode access
switchport access vlan 40
exit
vlan 99
name BlackHole
exit
interface range gig0/1-2
switchport mode access
switchport access vlan 99
shutdown
exit
do write

ICT :
enable
configure terminal
hostname ICT_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption

```
interface range fa0/1-2
switchport mode trunk
exit
vlan 50
name ICT
exit
interface range fa0/3-24
switchport mode access
switchport access vlan 50
exit
vlan 99
name BlackHole
exit
interface range gig0/1-2
switchport mode access
switchport access vlan 99
shutdown
exit
do write
```

Server Room :

```
enable
configure terminal
hostname Server_Room_Switch
banner motd #NO Unauthorised Access!!!#
no ip domain lookup
line console 0
password cisco
login
exit
enable password cisco
service password-encryption
interface range fa0/1-2
switchport mode trunk
exit
vlan 60
name Server_Room
exit
interface range fa0/3-24
switchport mode access
switchport access vlan 60
exit
vlan 99
name BlackHole
exit
interface range gig0/1-2
switchport mode access
switchport access vlan 99
shutdown
exit
do write
```
