A Government's Network Scenario Report

Computer Communication Networks (CT-376)

BCIT

Section A

Group Members

Aleeza Mahsood	CT-003
Fatima Nadeem	CT-011
Aisha Shahzad	CT-015
Arfa Ahsan	CT-021

Index

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY
BACHELORS OF SCIENCE IN COMPUTER SCIENCE

Complex Computing Problem Assessment Rubrics

Course Code: CT-376			**Course Title: Computer Communication Networks**
Criteria and Scales			
Excellent **(3)**	**Good** **(2)**	**Average** **(1)**	**Poor** **(0)**
<u>Criterion 1:</u> Understanding the Problem: How well the problem statement is understood by the student			
Understands the problem clearly and identify the underlying issues and functionalities.	Adequately understands the problem and identifies the underlying issues and functionalities.	Inadequately defines the problem and identifies the underlying issues and functionalities.	Fails to define the problem adequately and does not identify the underlying issues and functionalities.
<u>Criterion 2:</u> Research: The amount of research that is used in solving the problem			
Contains all the information needed for solving the problem	Good research leads to a successful solution	Mediocre research which may or may not lead to an adequate solution	No apparent research
<u>Criterion 3:</u> Code: How complete the code is along with the assumptions?			
Complete the code according to the selected functionalities of the given case with clear assumptions	Incomplete code according to the selected functionalities of the given case with clear assumptions	Incomplete code according to the selected functionalities of the given case with unclear assumptions	Wrong code and naming conventions
<u>Criterion 4:</u> Report: How thorough and well organized is the solution?			
All the necessary information is organized for easy use insolving the problem	Good information organized well could lead to a good solution	Mediocre information which may or may not lead to a solution	No report provided
<u>Criterion 5:</u> Labeling: How well defined and labeled is the solution?			
All the necessary information is labelled (i.e. port no.) for better understanding	Good information about the topology is labelled	Incomplete label according to the selected functionalities	Not Labelled

Total Marks: ____________

Teacher's Signature: ____________

Network Scenario Report

1. Introduction

This report presents the network scenario implemented on the eNSP (Enterprise Network Simulation Platform). The network consists of a central cloud system, seven departmental routers, and various switches connecting departmental devices. The following technologies have been implemented in this scenario: Subnetting, Telnet, security (ACL), Eth-Trunk, static route, RIP, STP, VLSM, VLAN, DHCP, and FTP. Each technology will be discussed in detail with appropriate justification and configuration.

2. Background

The Government Cloud network is meticulously designed to cater to the diverse operational needs of various governmental departments. The network is organized in such a way that it spans multiple divisions including Defense, Finance, Home Affairs, Foreign Affairs, and Health, each with dedicated departmental routers. The network infrastructure needs to be designed to support seamless connectivity across various departments and ensure easy access to shared resources such as FTP servers and DNS services.

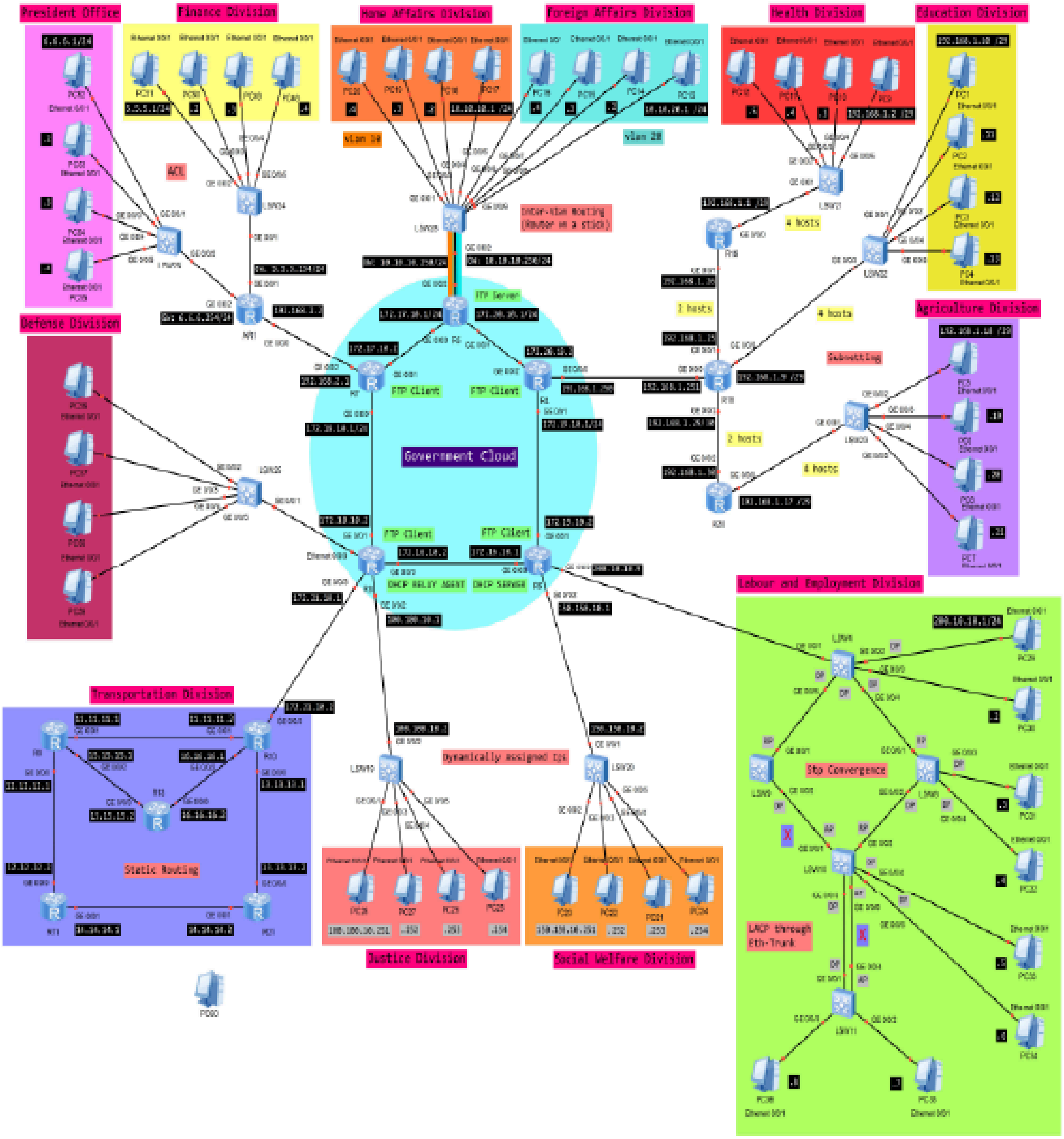
3. Network Topology

The network topology comprises the following devices:

- Central Router (R1)
- DHCP Server (R6)
- Router for President Division and Finance (AR1)
- Router for Home and Foreign Affairs Division (R5)

- Router for Education Division (R20)
- Router for Agriculture Division (R18)
- Router for Health Division (R19)
- Router for Labor and Employment Division (R6)
- Router for Social Welfare Division (R6)
- Router for Justice and Transportation Division (R8)
- FTP Server (R5)
- Multiple switches connecting PCs for all the Divisions respectively

3.1: Overall Implemented Scenario

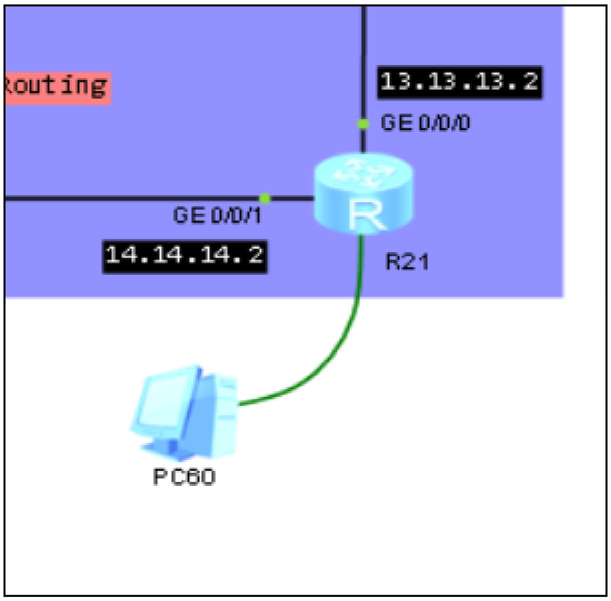


4. Implemented Technologies and Justification

4.1 Telnet

Telnet is a network protocol used to provide a command-line interface for communication with remote devices or servers. It allows users to manage network devices, such as routers and switches, over a network. Telnet operates on a client-server model and typically uses TCP port 23.

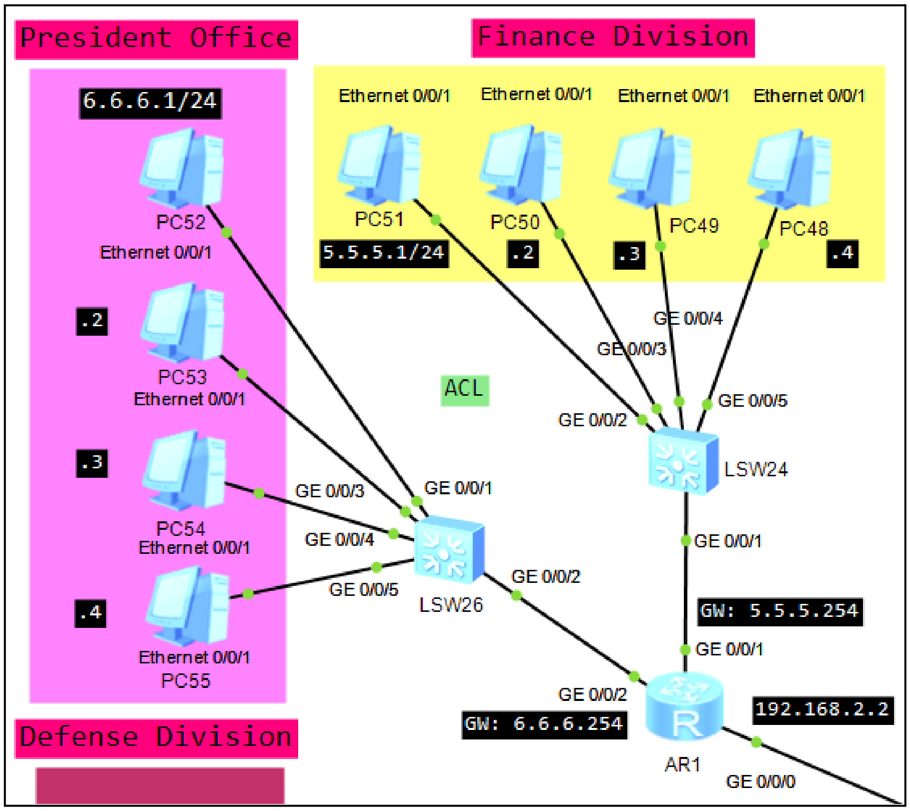
In this government network topology, Telnet has been implemented to manage and configure the routers remotely.



4.2 Access Control List (ACL)

An ACL is a set of rules used to control network traffic and limit access to network resources. ACLs are crucial for enhancing network security by defining which packets are allowed or denied through network devices, such as routers and switches.

4.2.1 Implemented Scenario



In this scenario, ACL is configured on the router AR2220 Router labeled AR1, to restrict and allow access to specific IP addresses.

- All PCs in the President Office can access each other.
- All PCs in the Finance Division can access each other.
- According to rule 5 of acl number 3000, all devices in the Finance Division (5.5.5.0 network) are allowed to access all devices in the President's Office (6.6.6.0 network).

  acl number 3000

```
    rule 5 permit ip source 5.5.5.0 0.0.0.255 destination 6.6.6.0 0.0.0.255
```

- According to rule 5 of acl number 3001, the device with IP address 6.6.6.1 in the President's Office network is allowed to access all devices in the Finance Division.

  ```
  acl number 3001
     rule 5 permit ip source 6.6.6.1 0 destination 5.5.5.0 0.0.0.255
  ```

- According to rule 10 of acl number 3001, all other devices in the President's Office network are denied access to all devices in the Finance Division.

  ```
  acl number 3001
     rule 10 deny ip source 6.6.6.0 0.0.0.255 destination 5.5.5.0 0.0.0.255
  ```

- Because ACL 3001 rule 10 would deny access from any device in the 6.6.6.0 network (except 6.6.6.1) to the 5.5.5.0 network, *this will override the broader permissions set by ACL 3000 rule 5* in this case.

AR1 Configuration:

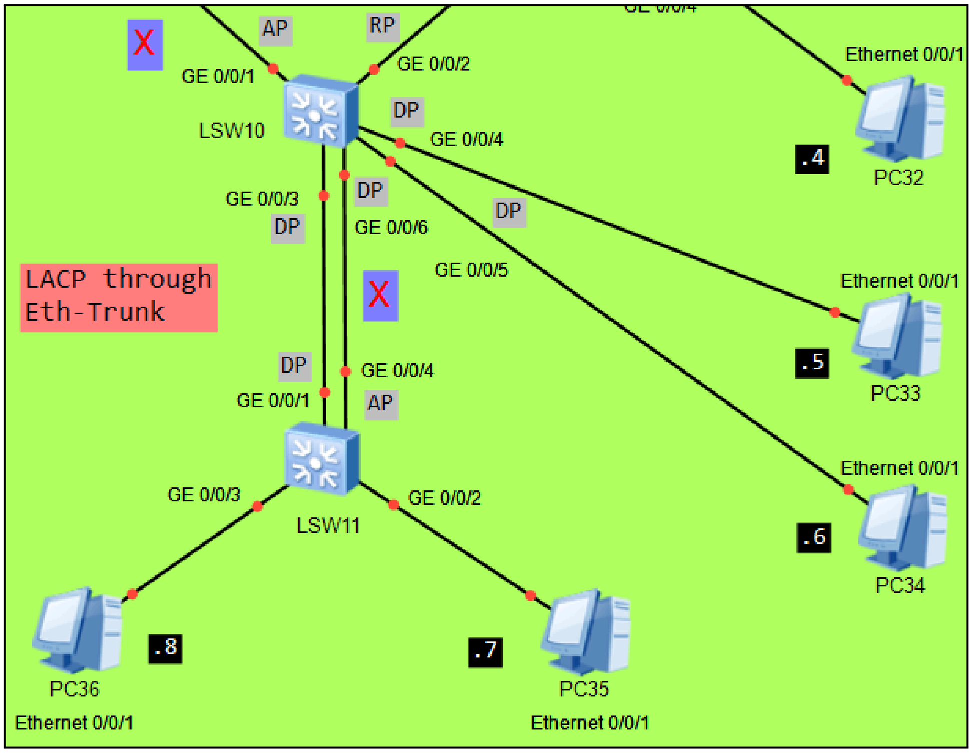
```
#
 sysname AR1
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
acl number 3000
  rule 5 permit ip source 5.5.5.0 0.0.0.255 destination 6.6.6.0 0.0.0.255
acl number 3001
  rule 5 permit ip source 6.6.6.1 0 destination 5.5.5.0 0.0.0.255
  rule 10 deny ip source 6.6.6.0 0.0.0.255 destination 5.5.5.0 0.0.0.255
#
aaa
 authentication-scheme default
 authorization-scheme default
```

```
 accounting-scheme default
 domain default
 domain default_admin
 local-user ar1 password cipher %$%$!)iDRF+IYASFkm705TE<oty[%$%$
 local-user ar1 privilege level 3
 local-user ar1 service-type telnet terminal
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
firewall zone Local
  priority 15
#
interface GigabitEthernet0/0/0
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 5.5.5.254 255.255.255.0
 traffic-filter inbound acl 3000
#
interface GigabitEthernet0/0/2
 ip address 6.6.6.254 255.255.255.0
 traffic-filter inbound acl 3001
#
interface NULL0
#
rip 1
 version 2
 network 192.168.2.0
#
user-interface con 0
 authentication-mode aaa
 user privilege level 3
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
user-interface vty 16 20
#
wlan ac
#
return
```

4.3 Link Aggregation (LACP mode)

Link Aggregation Control Protocol (LACP) is a network protocol that allows multiple physical Ethernet links to be combined into a single logical link. This increases bandwidth and provides redundancy, enhancing both performance and reliability.

4.3.1 Implemented Scenario



In this scenario we have created Eth-Trunk in LACP mode on switches LSW10 and LSW11.

LSW10 Configuration

```
[LSW10] interface Eh-Trunk 1
[LSW10-Eh-Trunk1] mode lacp
[LSW10-Eh-Trunk1] q
[LSW10] interface GigabitEthernet 0/0/6
```

```
[LSW10-GigabitEthernet0/0/6] Eth-Trunk 1
[LSW10-GigabitEthernet0/0/6] q
[LSW10] interface GigabitEthernet 0/0/3
[LSW10-GigabitEthernet0/0/3] Eth-Trunk 1
[LSW10-GigabitEthernet0/0/3] q
```

LSW11 Configuration

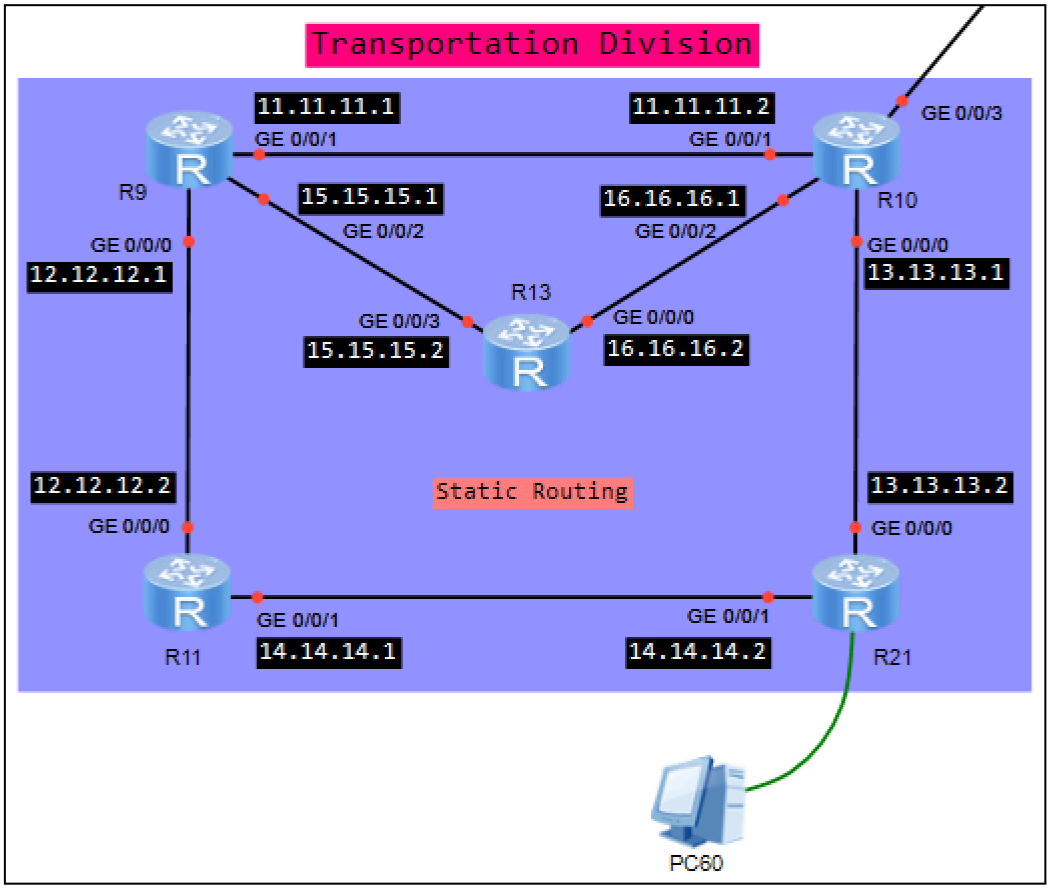
```
[LSW11] interface Eh-Trunk 1
[LSW11-Eh-Trunk1] mode lacp
[LSW11-Eh-Trunk1] q
[LSW11] interface GigabitEthernet 0/0/1
[LSW11-GigabitEthernet0/0/1] Eth-Trunk 1
[LSW11-GigabitEthernet0/0/1] q
[LSW11] interface GigabitEthernet 0/0/4
[LSW11-GigabitEthernet0/0/4] Eth-Trunk 1
[LSW11-GigabitEthernet0/0/4] q
```

4.4 Static Routes

In static Routing, routes are manually configured on the router by a network administrator. Unlike dynamic routing protocols, which automatically adjust routes based on the current network topology, static routes do not change unless manually updated. They are useful for small networks, stable environments, or for specific routing requirements.

In the transportation division we have performed static routing and used 5 routers for this purpose .We have used R9, R10, R11, R13 and R21 for it.

4.4.1 Implemented Scenario:



R9:

We have configured three static routes on r9.

1. The route for the 13.13.13.0/24 network directs traffic to the next hop IP address 11.11.11.2.
2. For the 14.14.14.0/24 network, the route forwards traffic to the next hop IP address 12.12.12.2.
3. The route handling the 16.16.16.0/24 network sends traffic to the next hop IP address 15.15.15.2.

R10:

Three static routes are configured.

1. For the 12.12.12.0/24 network, traffic is directed to the next hop IP address 11.11.11.1.

2. The route for the 14.14.14.0/24 network forwards traffic to the next hop IP address 13.13.13.2.
3. Traffic destined for the 15.15.15.0/24 network is routed to the next hop IP address 16.16.16.2.

R11:

Four static routes are configured.

1. For the 11.11.11.0/24 network, traffic is directed to the next hop IP address 12.12.12.1.
2. For the 13.13.13.0/24 network, traffic is forwarded to the next hop IP address 14.14.14.2.
3. For the 15.15.15.0/24 network, traffic is routed to the next hop IP address 12.12.12.1.
4. For the 16.16.16.0/24 network, traffic is sent to the next hop IP address 14.14.14.2.

R21:

Four static routes are configured.

1. For the 11.11.11.0/24 network, traffic is directed to the next hop IP address 13.13.13.1.
2. For the 12.12.12.0/24 network, traffic is forwarded to the next hop IP address 14.14.14.1.
3. For the 15.15.15.0/24 network, traffic is routed to the next hop IP address 14.14.14.1.
4. For the 16.16.16.0/24 network, traffic is sent to the next hop IP address 13.13.13.1.

R13:

Four static routes are configured.

1. For the 11.11.11.0/24 network, traffic is directed to the next hop IP address 15.15.15.1.
2. For the 12.12.12.0/24 network, traffic is forwarded to the next hop IP address 15.15.15.1.
3. For the 13.13.13.0/24 network, traffic is routed to the next hop IP address 16.16.16.1.
4. For the 14.14.14.0/24 network, traffic is sent to the next hop IP address 16.16.16.1.

4.5 Dynamic Route - RIP (Routing Information Protocol)

RIP is a dynamic routing protocol that allows routers to exchange routing information. It uses hop count as a metric to determine the best path for forwarding packets. Implementing RIP between the routers in this scenario will enable dynamic routing and automatic updating of routing tables. We implemented RIP on all routers, to enable communication of the one Division to Other.

First, RIP 1, version 2 is enabled on all of the routers. Network statements are configured to specify the networks that participate in RIP routing updates. Each router includes the network addresses it is directly connected to, ensuring that RIP exchanges routing information for those networks.

Implemented Configuration on each Router:

```
[R5]rip 1
[R5-rip-1] version 2
[R5-rip-1] network 172.17.0.0
network 172.20.0.0
```

for each router the networks specified change respectively according to the networks adjacent to it.

R5:

R5 has implemented RIP and is advertising four networks: 172.17.0.0 and 172.20.0.0.

R4:

R4 is running RIP and advertising three networks, 172.20.0.0, 172.19.0.0, and 192.168.1.0.

R6:

R6 has implemented RIP and is advertising four networks: network 172.16.0.0 , 172.19.0.0 , 150.150.0.0. and 200.10.10.

R7:

R7 has implemented RIP and is advertising three networks: network 172.17.0.0, 172.18.0.0 and 192.168.2.0.

R8:

R8 has implemented RIP and is advertising four networks: network 172.16.0.0 , 172.18.0.0 , 100.0.0.0. and 172.21.0.0.

R9:

R9 has implemented RIP and is advertising three networks: network 11.0.0.0 , 12.0.0.0 and 15.0.0.0.

R10:

R10 has implemented RIP and is advertising three networks: network 11.0.0.0 ,13.0.0.0 and 16.0.0.0.

R11:

R11 has implemented RIP and is advertising two networks: network 12.0.0.0 and 14.0.0.0.

R13:

R13 has implemented RIP and is advertising two networks: network 15.0.0.0 and 1.0.0.0.

R18:

R18 is running RIP and advertising a single network, 192.168.1.0.

R19:

R19 is running RIP and advertising a single network, 192.168.1.0.

R20:

R20 is running RIP and advertising a single network, 192.168.1.0.

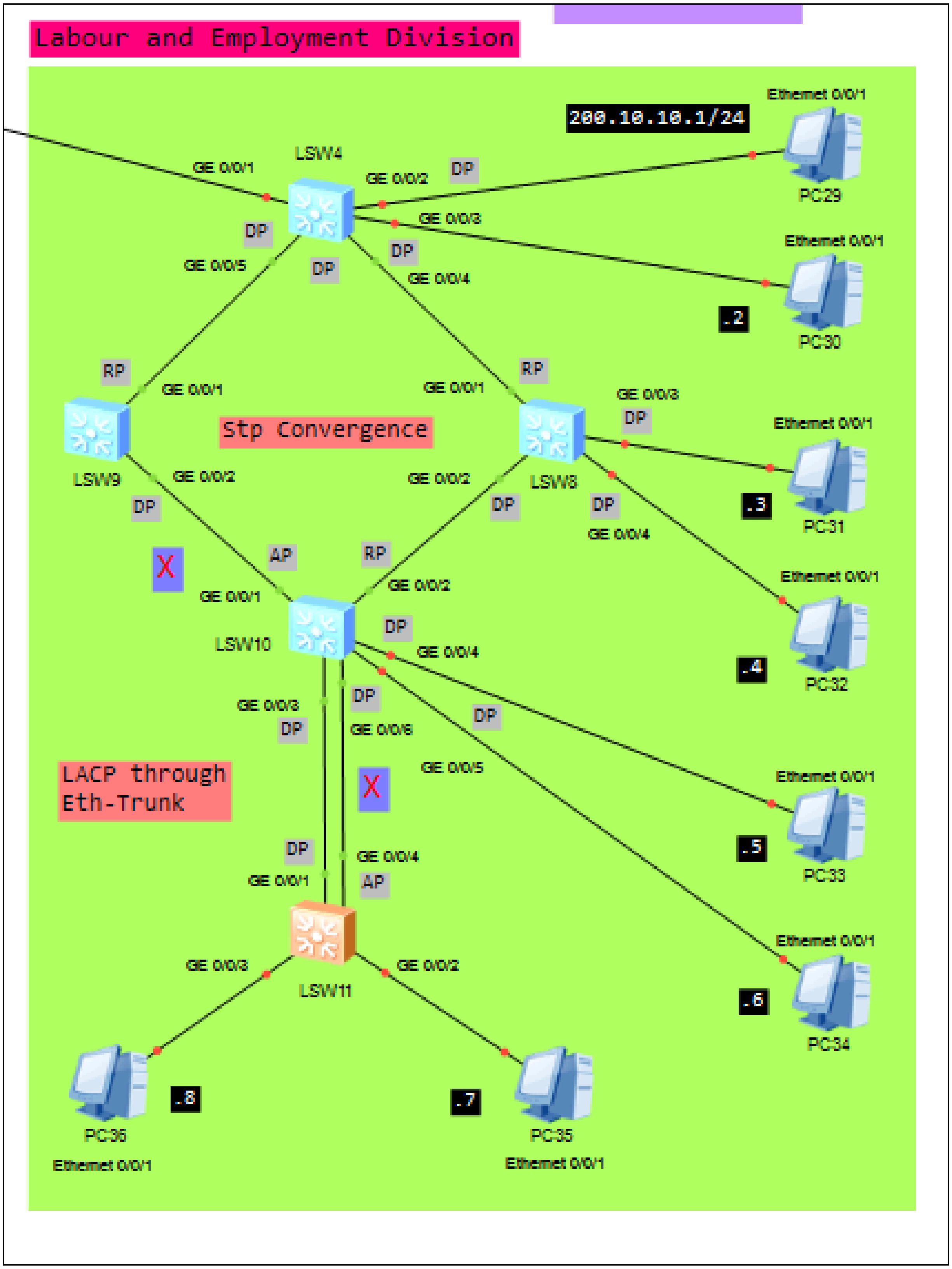
R21:

R21 has implemented RIP and is advertising two networks: network 13.0.0.0 and 14.0.0.0.

4.6 STP (Spanning Tree Protocol)

STP is a network protocol that prevents loops in Ethernet networks. It ensures a loop-free topology by dynamically selecting the best path and blocking redundant links. By enabling STP, we can prevent broadcast storms and ensure a stable network environment. STP has been enabled in the Labour and Employment Division.We have used LSW4, LSW8, LSW9, LSW10 and LSW11 for it. Following are the details of the enabled STP Protocol:

4.6.1 Implemented Scenario:


Labour and Employment Division
200.10.10.1/24
Ethernet 0/0/1
PC29
LSW4
GE 0/0/1
GE 0/0/2
DP
GE 0/0/3
DP
GE 0/0/5
DP
DP
GE 0/0/4
Ethernet 0/0/1
.2
PC30
RP
GE 0/0/1
GE 0/0/1
RP
GE 0/0/3
DP
Stp Convergence
Ethernet 0/0/1
LSW9
GE 0/0/2
GE 0/0/2
LSW8
DP
DP
DP
.3
PC31
GE 0/0/4
X
AP
RP
Ethernet 0/0/1
GE 0/0/1
GE 0/0/2
LSW10
DP
GE 0/0/4
.4
PC32
GE 0/0/3
DP
DP
GE 0/0/6
DP
GE 0/0/5
LACP through
Eth-Trunk
X
Ethernet 0/0/1
.5
PC33
DP
GE 0/0/4
GE 0/0/1
AP
Ethernet 0/0/1
GE 0/0/3
GE 0/0/2
LSW11
.6
PC34
.8
.7
PC36
PC35
Ethernet 0/0/1
Ethernet 0/0/1

Labour and Employment Division:

- **LSW4 (Root Bridge):**

  MAC Address: 4c1f-cc62-4e3b

  Priority: 4096

  Designated Port: GE0/0/2, GE0/0/3, GE0/0/4,
  GE0/0/2, GE0/0/5

- **LSW9:**

  MAC Address:32768.4c1f-cca7-14bb

  Root Port: GE0/0/1

  Designated Port: GE0/0/2

- **LSW8:**

  MAC Address: 4c1f-cc8e-3ffc

  Priority: 32768

  Root Port: GE0/0/1

  Designated Port: GE0/0/2, GE0/0/3, GE0/0/4

- **LSW10:**

  MAC Address: 4c1f-cc13-382e

  Priority: 32768

  Alternate Port: GE0/0/1

  Root Port: GE0/0/2

  Designated Port: EthTrunk1 GE0/0/3, GE0/0/4, GE0/0/5, EthTrunk1 GE0/0/6

- **LSW11:**
  MAC Address: 4c1f-ccb7-4847

  Priority: 32768

  Alternate Port: EthTrunk 1,GE0/0/4

Designated Port: EthTrunk1, GE0/0/1

Authentication on each Switch:

```
<LSW4>u t m
Info: Current terminal monitor is off.
<LSW4>system-view
Enter system view, return user view with Ctrl+Z.
[LSW4]aaa
[LSW4-aaa]local-user lsw4 password cipher huawei123
Info: Add a new user.
[LSW4-aaa]local-user lsw4 service-type telnet terminal
[LSW4-aaa]local-user lsw4 privilege level 3
[LSW4-aaa]q
[LSW4]user-interface con 0
[LSW4-ui-console0]authentication-mode aaa
[LSW4-ui-console0]user privilege level 3
[LSW4-ui-console0]q
[LSW4]user-interface vty 0 4
[LSW4-ui-vty0-4]authentication-mode aaa
[LSW4-ui-vty0-4]user privilege level 3
[R8-ui-vty0-4]q
[LSW4]q
<LSW4>save
```

LSW4 (Root Bridge) Configurations:

```
<LSW4> system-view
[LSW4] stp enable
[LSW4] stp priority 4096
```

LSW8, LSW9, LSW10, LSW11 Configurations:

```
<LSW9> system-view
[LSW9] stp enable
[LSW9] q
<LSW9> display stp

<LSW10> system-view
[LSW10] stp enable
[LSW10] q
<LSW10> display stp
```

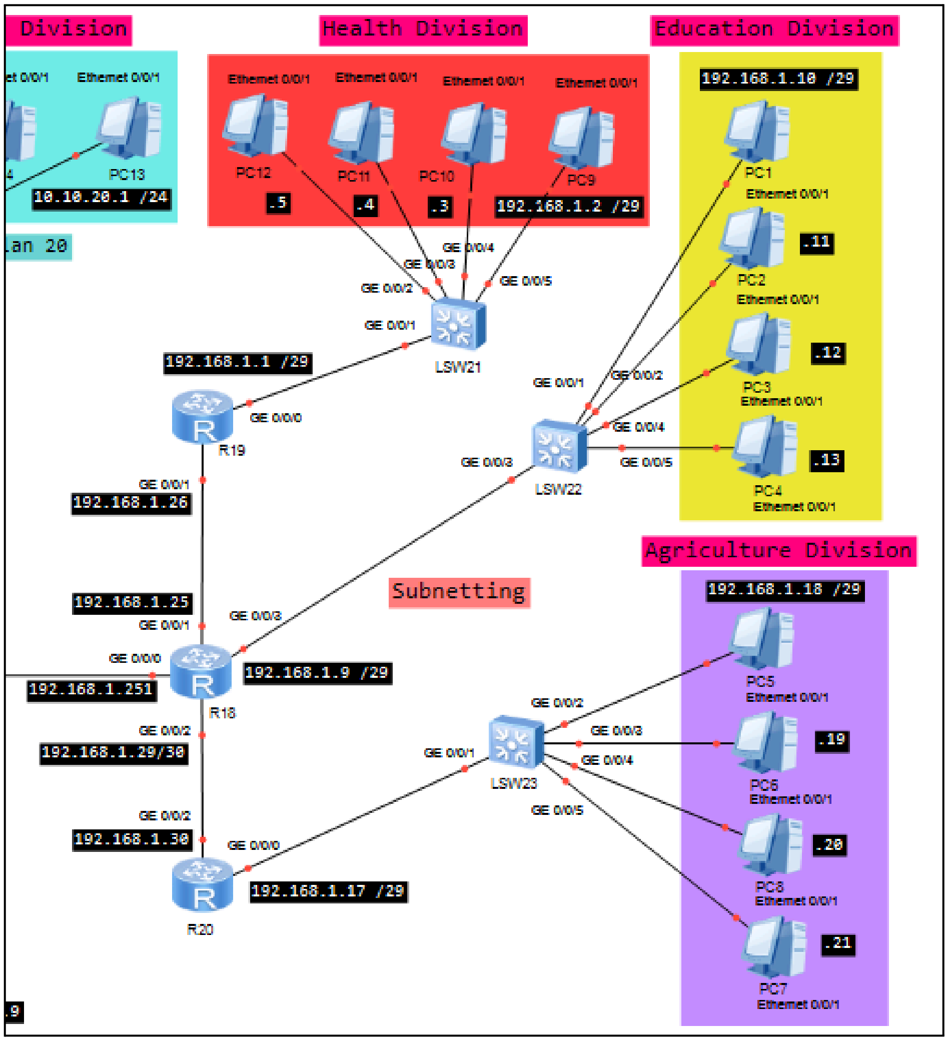
```
<LSW11> system-view
[LSW11] stp enable
[LSW11] q
<LSW11> display stp
```

```
<LSW8> system-view
[LSW8] stp enable
[LSW8] q
<LSW8> display stp
```

4.7 VLSM (Variable Length Subnet Masking)

VLSM is a technique used to allocate IP addresses efficiently by subnetting a network into smaller subnets. It allows for the conservation of IP addresses and better address space utilization. Implementing VLSM in this scenario helped allocate IP addresses to different departments according to their requirements. Following is the calculation of VLSM that we implemented:

Implemented Scenario:



Major Network: 192.168.1.0/24

- **Subnet 1:4 Hosts**

  Subnet Address: 192.168.1.0/29

  Broadcast Address: 192.168.1.7/29

  Usable Host Range: 192.168.1.1-192.168.1.6

- **Subnet 2: 4 Hosts**

  Subnet Address: 192.168.1.8/29

  Broadcast Address: 192.168.1.15/29

Usable Host Range: 192.168.1.9 - 192.168.1.14/29

- **Subnet 1: 4 Hosts**

  Subnet Address: 192.168.1.16/29

  Broadcast Address: 192.168.1.23/29

  Usable Host Range: 192.168.1.17 - 192.168.1.22/29

- **Subnet 2: 2 Hosts**

  Subnet Address: 192.168.1.24/30

  Broadcast Address: 192.168.1.27/30

  Usable Host Range: 192.168.1.25 - 192.168.1.26/30

- **Subnet 2: 2 Hosts**

  Subnet Address: 192.168.1.28/30

  Broadcast Address: 192.168.1.31/30

  Usable Host Range: 192.168.1.29 - 192.168.1.30/30

4.8 VLAN (Virtual Local Area Network)

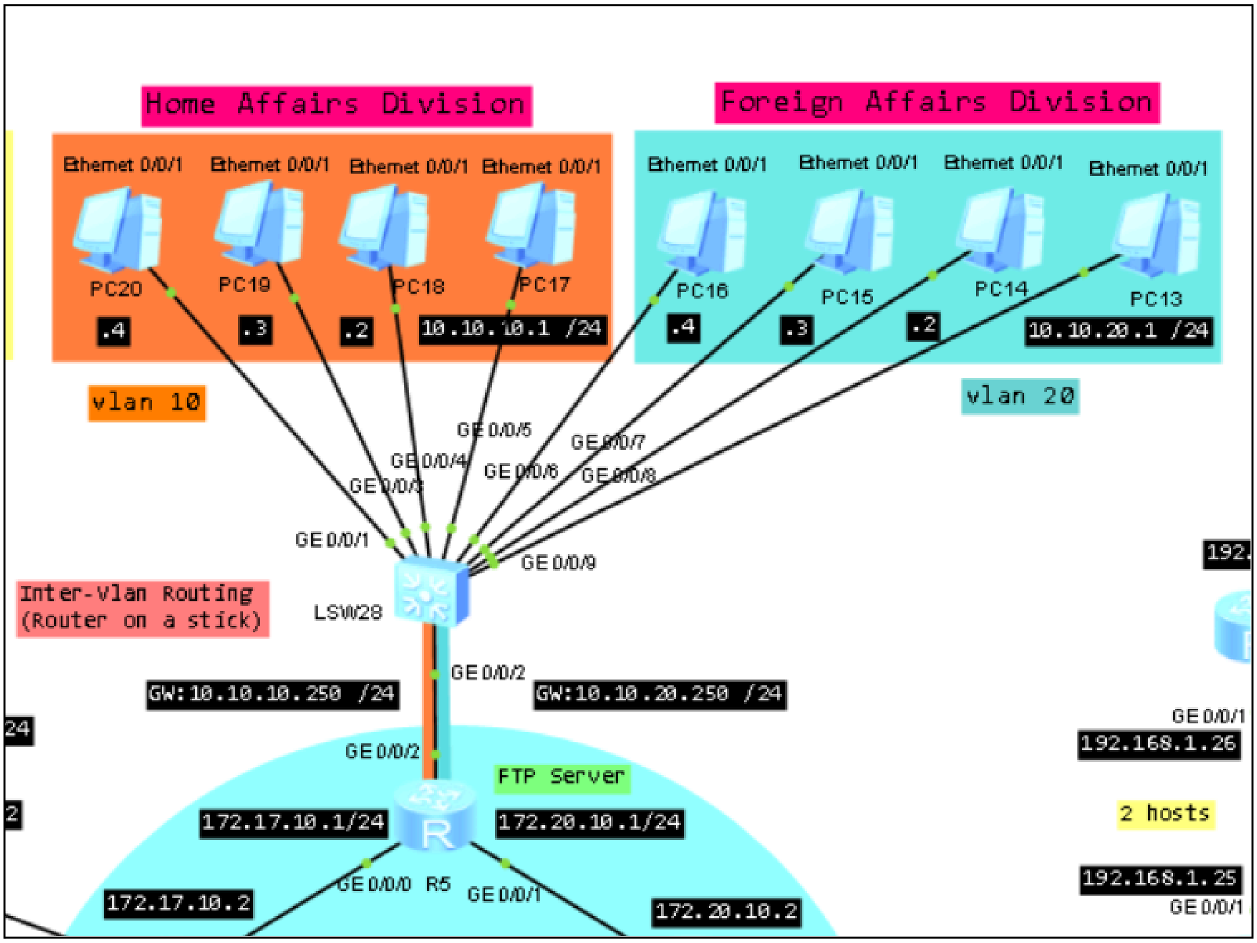
A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch.Vlans divide the broadcast domain in a LAN environment .So,by default only hosts that are members of the same VLAN can communicate .

In the government network topology we have implemented inter-vlan routing through router on a stick on the Home Affairs and Foreign Affairs Division.It allows devices in VLAN 10 to communicate with devices in VLAN 20 through router R5.It ensures that PCs in the Home Affairs Division can communicate with PCs in the Foreign Affairs Division.

Components and Configuration

1. **VLANs and Divisions:**
   - **Home Affairs Division (VLAN 10):**
     - Devices in this division are assigned IP addresses in the 10.10.10.0/24 subnet.
     - Example devices:
       - PC17: 10.10.10.1
       - PC18: 10.10.10.2
       - PC19: 10.10.10.3
       - PC20: 10.10.10.4
   - **Foreign Affairs Division (VLAN 20):**
     - Devices in this division are assigned IP addresses in the 10.10.20.0/24 subnet.
     - Example devices:
       - PC13: 10.10.20.1
       - PC14: 10.10.20.2
       - PC15: 10.10.20.3
       - PC16: 10.10.20.4
2. **Switch (LSW28):**
   - Connects all PCs in both the Home Affairs and Foreign Affairs Divisions.
   - VLANs are configured on this switch:
     - VLAN 10 for Home Affairs.
     - VLAN 20 for Foreign Affairs.
3. **Router (R5):**
   - Configured for inter-VLAN routing (router-on-a-stick).
   - Sub-interfaces are set up for each VLAN:
     - GE 0/0/2.10 for VLAN 10 with IP address 10.10.10.250 /24.
     - GE 0/0/2.20 for VLAN 20 with IP address 10.10.20.250 /24.

Implemented Scenario:



Inter Vlan Routing (Router -On-a-Stick) Configuration

Switch (LSW28):

```
#
sysname LSW28
#
vlan batch 10 20
#
cluster enable
```

```
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
 local-user lsw28 password cipher -J&7(SW'E2AI>,Z,88J\:Q!!
 local-user lsw28 privilege level 3
 local-user lsw28 service-type telnet terminal
#
interface Vlanif1
#
interface MEth0/0/1
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 10
```

```
#
interface GigabitEthernet0/0/6
 port link-type access
 port default vlan 20
#
interface GigabitEthernet0/0/7
 port link-type access
 port default vlan 20
#
interface GigabitEthernet0/0/8
 port link-type access
 port default vlan 20
#
interface GigabitEthernet0/0/9
 port link-type access
 port default vlan 20
#
interface NULL0
#
user-interface con 0
 authentication-mode aaa
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
#
return
```

Router(R5):

```
#
sysname R5
#
FTP server enable
set default ftp-directory flash:/
#
undo nap slave enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user r5 password cipher uxEn6$5\xNd.'8Eha)49DN+#
 local-user r5 privilege level 3
 local-user r5 service-type telnet terminal
 local-user user password cipher ^Xn6)~DXE"]@l3D+mKgUDN+#
 local-user user privilege level 3
 local-user user ftp-directory flash:/
 local-user user service-type ftp
 local-user admin password cipher gH4*"IogBI]@l3D+mKgUDN+#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface GigabitEthernet0/0/0
 ip address 172.17.10.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 172.20.10.1 255.255.255.0
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/2.10
 dot1q termination vid 10
 ip address 10.10.10.250 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/2.20
 dot1q termination vid 20
 ip address 10.10.20.250 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
rip 1
 version 2
 network 172.17.0.0
 network 172.20.0.0
#
user-interface con 0
 authentication-mode aaa
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
user-interface vty 16 20
#
```

```
return
```

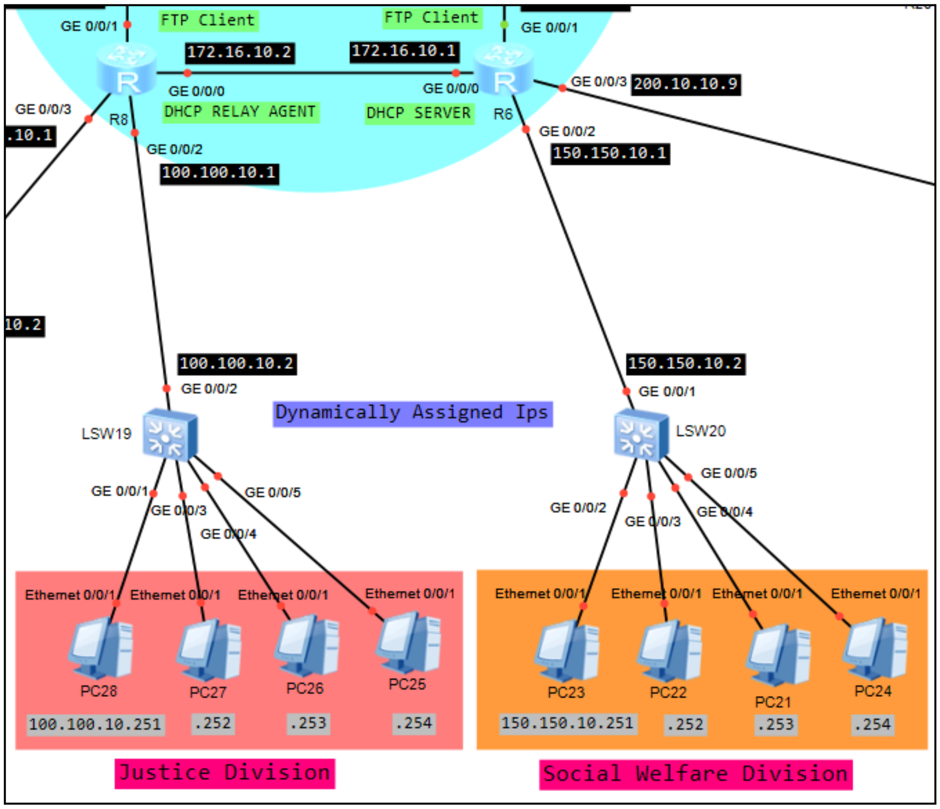
4.9 DHCP (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to hosts dynamically .It allows easier administration and works well in small as well as very large network environments.DHCP can provide the information of IP addresses ,Subnet Mask and DNS .

Components and Configuration

1. **Routers and Switches**
   - **R6 and R8 Routers:**
     - **R6:**
       - Functions as the DHCP Server with an IP address of 172.16.10.1
     - **R8:**
       - Acts as a DHCP Relay Agent, relaying DHCP requests to the DHCP server with the ip address of 172.16.10.2
   - **Switches (LSW19 and LSW20):**
     - **LSW19:** Connected to the Justice Division.
     - **LSW20:** Connected to the Social Welfare Division.

Implemented Scenario:



DHCP CONFIGURATIONS

DHCP Server (R6):

```
#
sysname R6
#
undo nap slave enable
#
dhcp enable
#
ip pool 1
 gateway-list 150.150.10.1
 network 150.150.10.0 mask 255.255.255.0
 dns-list 8.8.8.8
#
ip pool 2
 gateway-list 100.100.10.1
 network 100.100.10.0 mask 255.255.255.0
 dns-list 100.100.10.1
```

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user r6 password cipher V<DLU.gAh4&5Ka1*e#A7aM}#
 local-user r6 privilege level 3
 local-user r6 service-type telnet terminal
 local-user admin password cipher (b8}M$^xQ0ani^>"qh^;aM}#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface GigabitEthernet0/0/0
 ip address 172.16.10.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 ip address 172.19.10.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 150.150.10.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
rip 1
 version 2
 network 172.19.0.0
 network 172.16.0.0
 network 150.150.0.0
#
user-interface con 0
 authentication-mode aaa
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
user-interface vty 16 20
#
```

```
return
```

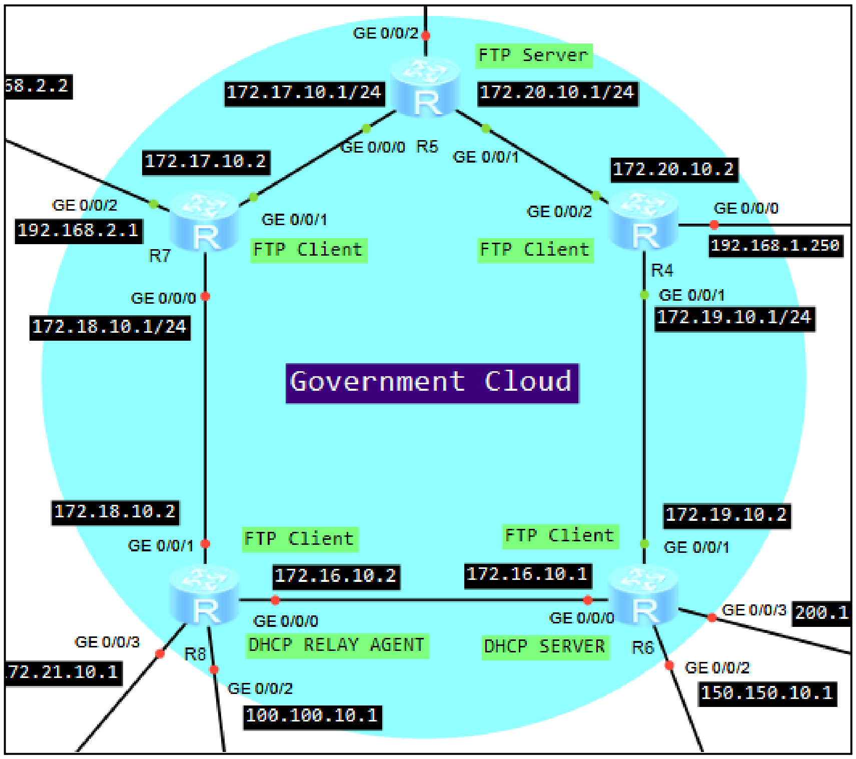
DHCP Relay Agent (R8):

```
#
sysname R8
#
undo nap slave enable
#
dhcp enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user r8 password cipher |WgnF:Q#H5y2v-"5"J{8[M!#
 local-user r8 privilege level 3
 local-user r8 service-type telnet terminal
 local-user admin password cipher d*MN"z:![0pe}@HMNPn@[M!#
 local-user admin service-type http
#
firewall zone Local
#
interface GigabitEthernet0/0/0
 ip address 172.16.10.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 172.18.10.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 100.100.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 172.16.10.1
#
interface GigabitEthernet0/0/3
 ip address 172.21.10.1 255.255.255.0
#
wlan
#
interface NULL0
#
rip 1
 version 2
 network 100.0.0.0
 network 172.16.0.0
 network 172.18.0.0
#
user-interface con 0
 authentication-mode aaa
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
user-interface vty 16 20
#
return
```

4.10 FTP (File Transfer Protocol)

FTP is a standard network protocol used to transfer files between a client and a server over a TCP-based network. In this scenario, the FTP server (R5) is implemented to facilitate file sharing and data exchange between different departments.

Implemented Scenario:



4.10.1. FTP Server Configuration:

```
#
sysname R5
#
FTP server enable
set default ftp-directory flash:/
#
undo nap slave enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user r9 password cipher 1f{qW-Q:7#Q-*uS:iH11py:#
 local-user r9 privilege level 3
 local-user r9 service-type telnet terminal
 local-user user password cipher Fz{[.^Ka:!939O4.(ZGpy:#
 local-user user privilege level 3
 local-user user ftp-directory flash:/
 local-user user service-type ftp
 local-user admin password cipher >:{/T'yS94939O4.(ZGpy:#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface GigabitEthernet0/0/0
 ip address 172.17.10.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 172.20.10.1 255.255.255.0
#
```

FTP Client (R6)

```
<R6>ftp 172.20.10.1
Trying 172.20.10.1 ...
Press CTRL+K to abort
Connected to 172.20.10.1.
220 FTP service ready.
User(172.20.10.1:(none)):user
```

```
331 Password required for user.
Enter password:
230 User logged in.

[ftp]dir
200 Port command okay.
150 Opening ASCII mode data connection for *.
drwxrwxrwx   1 noone    nogroup        0 Aug 07  2015 src
drwxrwxrwx   1 noone    nogroup        0 Jun 21 08:35 pmdata
drwxrwxrwx   1 noone    nogroup        0 Jun 21 08:36 dhcp
-rwxrwxrwx   1 noone    nogroup      667 Jun 23 09:43 private-data.txt
drwxrwxrwx   1 noone    nogroup        0 Jun 21 08:51 mplstpoam
-rwxrwxrwx   1 noone    nogroup      708 Jun 23 11:33 vrpcfg.zip
226 Transfer complete.

[ftp]get vrpcfg.zip
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.zip.

226 Transfer complete.
FTP: 708 byte(s) received in 1.120 second(s) 632.14byte(s)/sec.

[ftp]q
```

5. Conclusion

In conclusion, the implemented network scenario demonstrates the use of various technologies to establish a functional and secure government network environment. Telnet enables remote management, ACLs enhance security, Eth-Trunk provides link aggregation and redundancy, static routes ensure proper routing, RIP allows for dynamic routing, STP prevents loops, VLSM optimizes IP address allocation, VLANs segregate network traffic, DHCP automates IP address assignment, and FTP facilitates file transfer. By implementing these technologies, the network is capable of efficient and reliable communication within and between departments.