

# Company Network Design

Group members:

1. Abdul Rafay (233679)
2. Tayyab Abbas (233681)
3. Muhammad Awais (233680)
4. Arslan Dilawar (233515)

Contents

- 1. Introduction:..... 3
- 2. Network Design:..... 3
  - 1) Topology Diagram:..... 3
  - 2) Justification of Topology:..... 4
- 3. Configuration Details: ..... 4
  - 1) VLAN Configuration:..... 4
  - 2) InterVLAN Routing:..... 4
  - 3) DHCP Configuration: ..... 4
  - 4) RIP Protocol: ..... 5
  - 5) Firewalls:..... 6
- 4. Routing Optimization: ..... 6
- 5. Testing and Validation: ..... 6
  - 1) Functional Testing:..... 6
  - 2) Simulation:..... 7
- 6. Conclusion: ..... 9

## 1. Introduction:

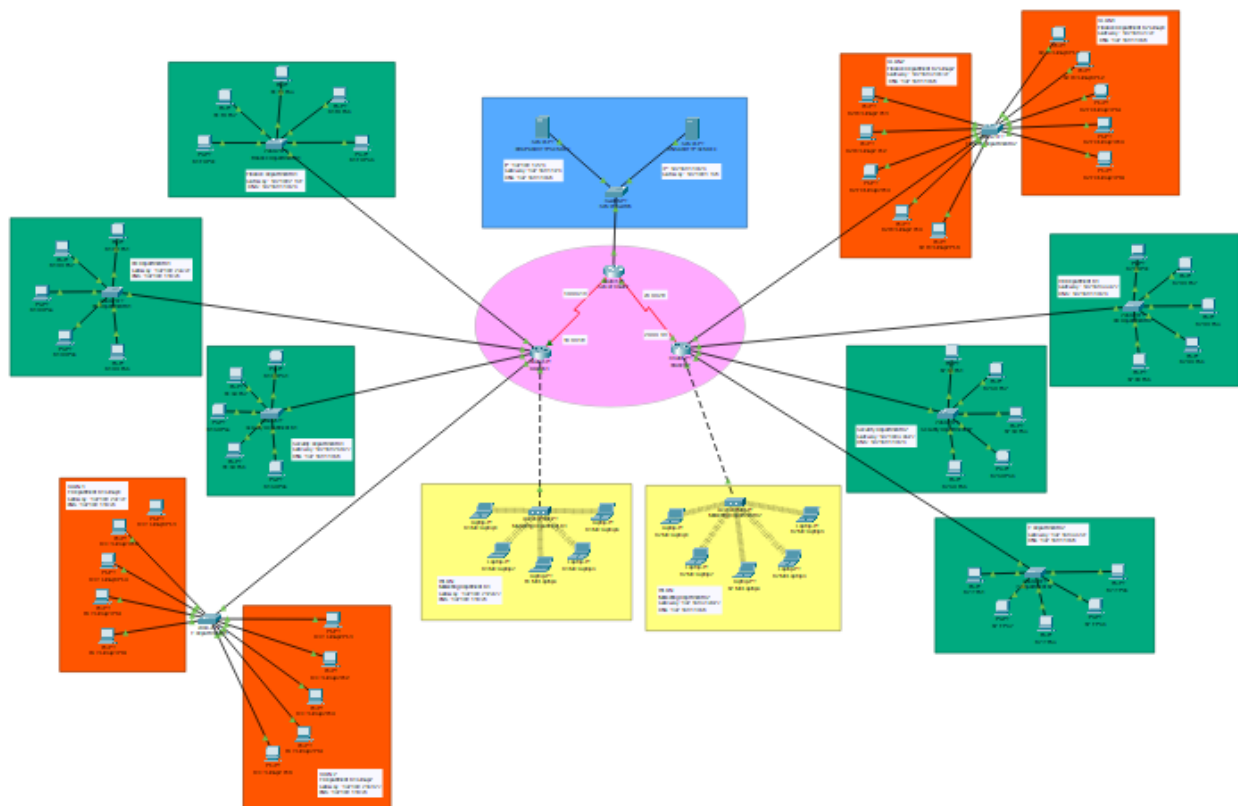
This report outlines the network infrastructure design for a company with two branches located in different states and a central server in another state. The network leverages advanced networking techniques for efficient communication, scalability, and security. The design incorporates static and dynamic IP allocation, VLANs, inter-VLAN routing, and the RIP protocol for seamless connectivity. Additionally, essential network services like DHCP, DNS, and HTTP are configured to meet the operational requirements of the organization. The inclusion of WLAN and VLAN isolation ensures enhanced security and functionality.

➤ Each branch contains five departments:

- Finance
- IT
- HR
- Security
- Marketing

## 2. Network Design:

### 1) Topology Diagram:



## 2) Justification of Topology:

The chosen topology ensures efficient communication between branches and the central server. It includes the following components:

- **Branch Offices:** Each branch has five departments with distinct configurations based on their IP allocation and communication method.
- **Central Server:** Hosts DHCP, HTTP, and DNS services to provide centralized management.
- **Routing Protocol (RIP):** Used for dynamic routing between branches to ensure scalability and simplicity.
- **VLAN and WLAN:** VLANs and WLANs are implemented for efficient segmentation and wireless connectivity.
- **Firewalls:** Configured on the DHCP and HTTP server to restrict unauthorized access.

This topology meets project requirements by:

- Allowing seamless communication between branches.
- Centralizing management of DHCP and DNS services.
- Ensuring network segmentation and security through VLANs.

## 3. Configuration Details:

### 1) VLAN Configuration:

The network design includes VLANs for each department in both branches to ensure traffic segmentation and improve network performance. Each VLAN is assigned a unique ID and name corresponding to its department. This setup minimizes broadcast traffic and isolates communication within departments.

### 2) InterVLAN Routing:

To enable communication between VLANs, inter-VLAN routing is configured on a central router in each branch. Sub-interfaces are used on the router, each associated with a specific VLAN. The router assigns a gateway IP address for each VLAN, ensuring proper routing between them.

### 3) DHCP Configuration:

A DHCP server is configured to dynamically assign IP addresses to computers in the dark green and light-yellow departments. This approach reduces administrative overhead and

## Company\_Network\_Design

ensures efficient IP address management. The DHCP pool includes a network range, default gateway, and DNS server information.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Marketing Department B2	192.168.3.129	192.168.1.10	192.168.3.130	255.255.255.224	30	0.0.0.0	0.0.0.0
IT Department B2	192.168.3.97	192.168.1.10	192.168.3.98	255.255.255.224	30	0.0.0.0	0.0.0.0
Security Department B2	192.168.3.65	192.168.1.10	192.168.3.66	255.255.255.224	30	0.0.0.0	0.0.0.0
HR Department B2	192.168.3.33	192.168.1.10	192.168.3.34	255.255.255.224	30	0.0.0.0	0.0.0.0
Finance Department B2	192.168.3.1	192.168.1.10	192.168.3.2	255.255.255.224	30	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.1.0	255.255.255.0	255	0.0.0.0	0.0.0.0
Marketing Department B1	192.168.2.129	192.168.1.10	192.168.2.130	255.255.255.224	30	0.0.0.0	0.0.0.0
IT Department B1	192.168.2.97	192.168.1.10	192.168.2.98	255.255.255.224	30	0.0.0.0	0.0.0.0
Security Department B1	192.168.2.65	192.168.1.10	192.168.2.66	255.255.255.224	30	0.0.0.0	0.0.0.0
HR Department B1	192.168.2.33	192.168.1.10	192.168.2.34	255.255.255.224	30	0.0.0.0	0.0.0.0
Finance Department B1	192.168.2.1	192.168.1.10	192.168.2.2	255.255.255.224	30	0.0.0.0	0.0.0.0
Server	192.168.1.1	192.168.1.10	192.168.1.3	255.255.255.0	32	0.0.0.0	0.0.0.0

### 4) RIP Protocol:

RIP is configured on the routers to dynamically share routing information between the branches and the central server. This ensures all routers maintain updated routes for seamless communication across the network.

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

INTERFACE

FastEthernet0/0

FastEthernet1/0

Serial2/0

Serial3/0

FastEthernet4/0

FastEthernet5/0

RIP Routing

Network

10.0.0.0

20.0.0.0

192.168.1.0

Add

Remove

## 5) Firewalls:

To enhance security, firewalls are implemented on the DHCP and HTTP servers. These firewalls control access to the services, allowing only authorized devices to connect while blocking unauthorized attempts.

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Deny	ICMP	0.0.0.0	255.255.255.255	-	-
2	Allow	IP	0.0.0.0	255.255.255.255	-	-

## 4. Routing Optimization:

In this project, RIP (Routing Information Protocol) is used to enable dynamic routing between branches and the central server. RIP is chosen for its simplicity and compatibility with smaller-scale networks. It ensures a dynamic exchange of routing information between routers, facilitating seamless communication.

## 5. Testing and Validation:

### 1) Functional Testing:

- DHCP: Verified IP allocation to light-yellow and dark-green departments.
- VLAN Communication: Successfully tested inter-VLAN routing for orange departments.
- WLAN: Validated wireless connectivity for dark green departments.
- DNS and HTTP: Accessed web pages using DNS resolution.

## 2) Simulation:

### a) HTTP:

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

HTTP

HTTP

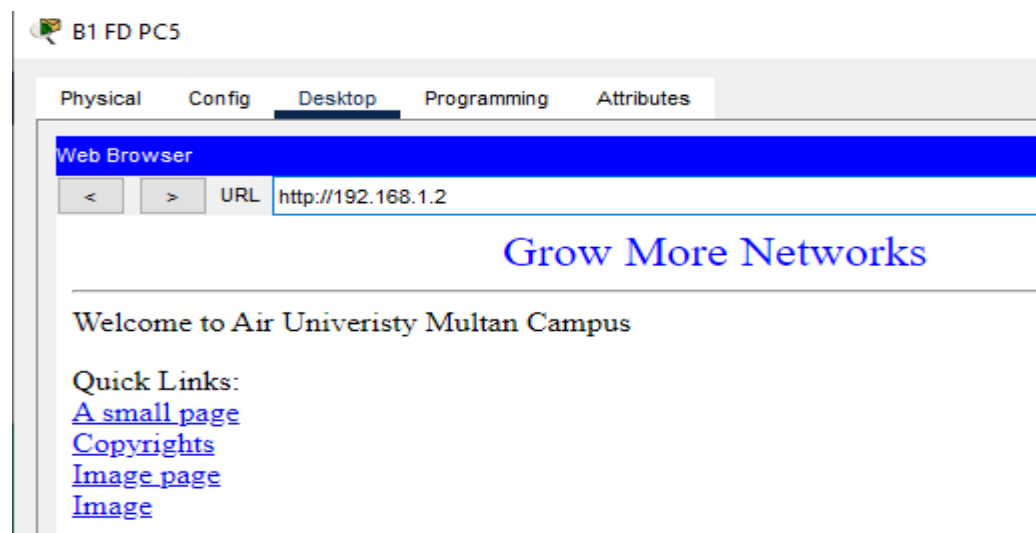
☒ On ☐ Off

HTTPS

☒ On ☐ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)



## Company\_Network\_Design

### b) DNS:

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name  Type A Record

Address

Add

Save

Remove

No.	Name	Type	Detail
0	default	A Record	192.168.1.10
1	www.growmorenetwork...	A Record	192.168.1.2

B1 FD PC4

Physical

Config

Desktop

Programming

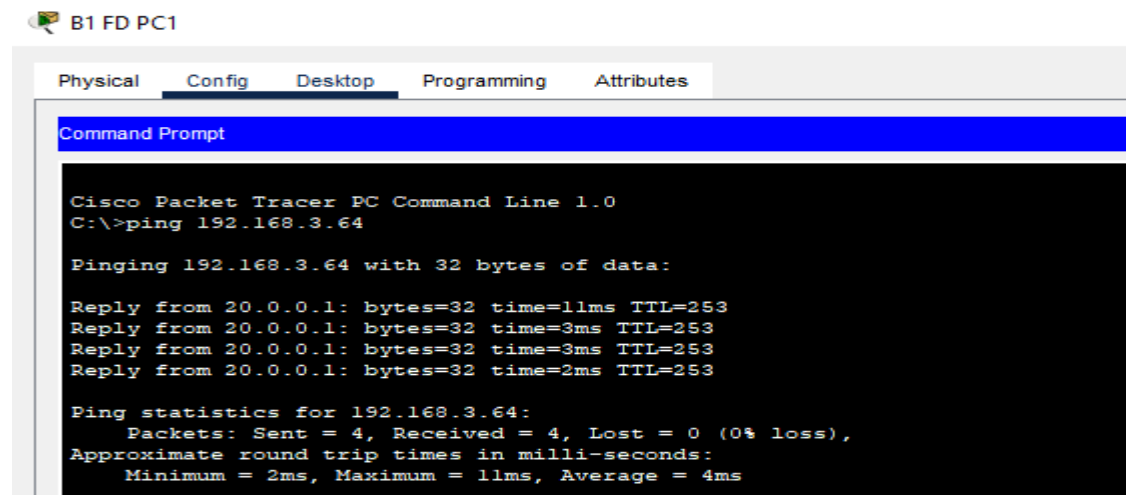
Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0  
C:\>ping default  
  
Pinging 192.168.1.10 with 32 bytes of data:  
  
Reply from 192.168.1.10: bytes=32 time=11ms TTL=126  
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126  
Reply from 192.168.1.10: bytes=32 time=33ms TTL=126  
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126  
  
Ping statistics for 192.168.1.10:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 33ms, Average = 11ms



c) ICMP:



The screenshot shows the Cisco Packet Tracer PC Command Line interface for B1 FD PC1. The interface has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected, and the Command Prompt window is open. The command prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.64

Pinging 192.168.3.64 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time=11ms TTL=253
Reply from 20.0.0.1: bytes=32 time=3ms TTL=253
Reply from 20.0.0.1: bytes=32 time=3ms TTL=253
Reply from 20.0.0.1: bytes=32 time=2ms TTL=253

Ping statistics for 192.168.3.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 4ms
```

## 6. Conclusion:

This project successfully demonstrates the design, configuration, and testing of a robust network infrastructure for a company with multi-branch operations. The use of VLANs, RIP, DHCP, and DNS ensures efficient communication, scalability, and centralized management. Future improvements could include implementing OSPF for faster convergence and enhanced security measures like intrusion detection systems (IDS).