Enterprise Network Design for Multi-Branch Company

Team Members:

Waheed Saied
Youssef Ali
Ahmed Rashed
Ahmed Kamal
Ziad Reda

1. Project Overview

The Enterprise Network Design for Multi-Branch Company project focuses on building a secure, scalable, and reliable network infrastructure that connects multiple branches of a company under one integrated system. The main objective is to ensure seamless communication, centralized management, and high availability between all branches using Huawei routers and switches within the eNSP simulation environment.

The network design includes three company branches connected through a core router that manages traffic routing, redundancy, and secure data transfer. Each branch is equipped with its own LAN, DHCP service for dynamic IP allocation, and VLAN segmentation to enhance security and performance.

Additionally, a central server infrastructure is implemented to host essential services such as Web, DNS, and Backup systems to ensure business continuity and efficient data management. The backup server provides redundancy in case of primary system failure, ensuring data protection and reliability.

This project demonstrates a real-world enterprise environment where network engineers can apply practical configurations, routing strategies, and security mechanisms to achieve efficient communication and operational resilience across distributed locations.

2. Project Planning

The planning phase includes defining the network topology, assigning IP addressing, selecting routing protocols, and planning services such as DHCP and backup servers. Each branch is assigned a subnet, and static routes are configured for inter-branch connectivity.

Task	Description	Duration
Network Design	Topology and IP Planning	2 weeks
Configuration	Router and Switch setup	3 weeks
Testing	Connectivity and redundancy tests	1 week
Deployment	Final implementation and validation	1 week

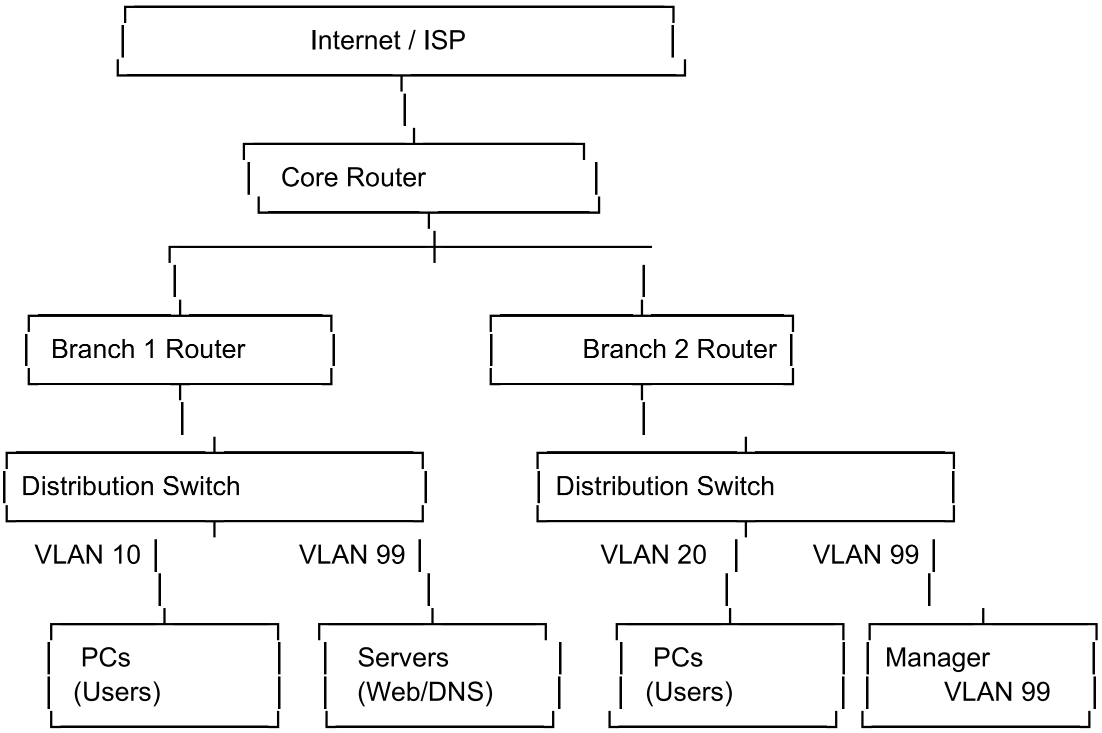
3. Stakeholder Analysis

Stakeholder analysis identifies key individuals and groups involved in the project, their roles, and influence levels.

Stakeholder	Role	Interest	Influence
Network Engineers	Design & Implementation	High	High
IT Manager	Project Oversight	High	High
End Users	System Usage	Medium	Low
Vendors	Equipment Supply	Medium	Medium

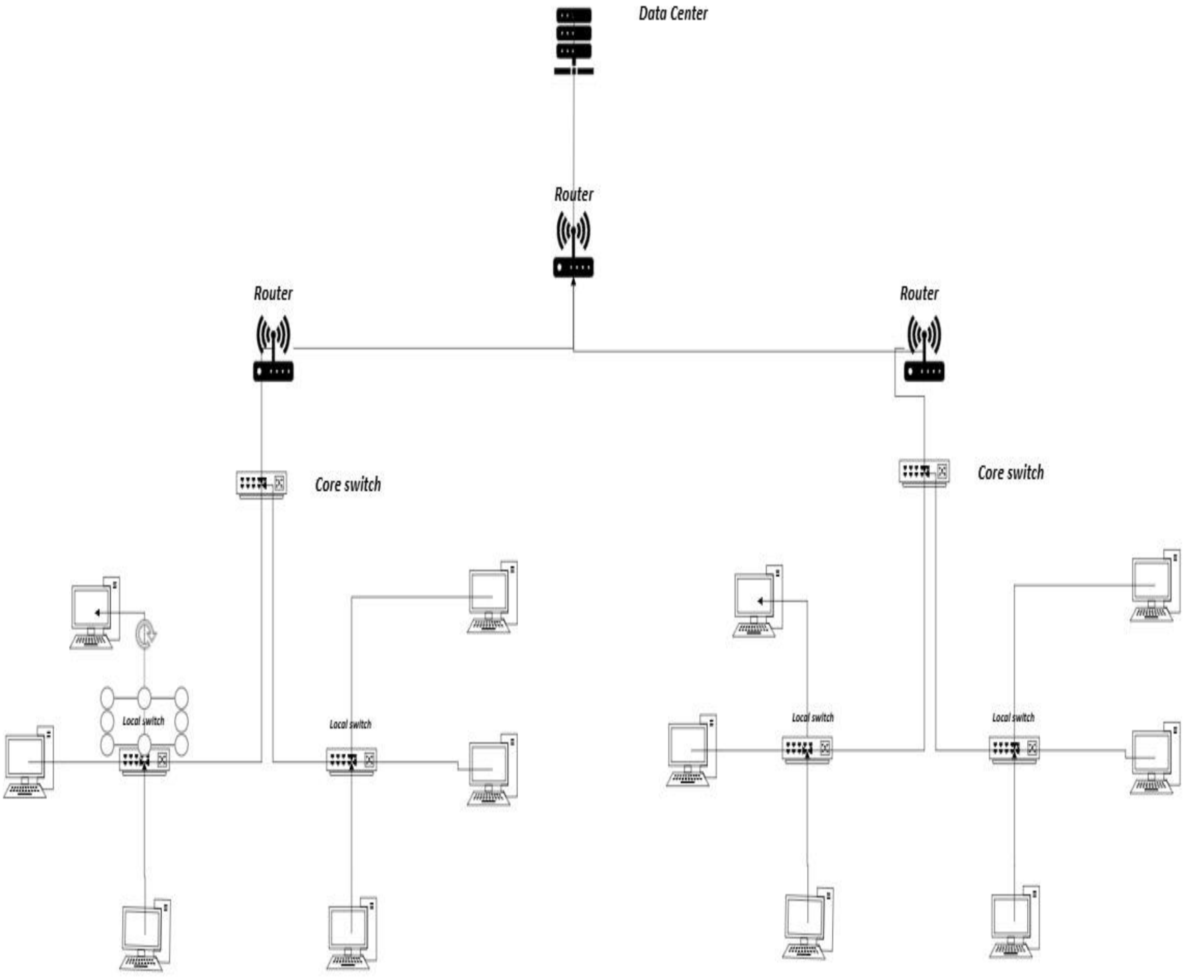
4. Database Design

The project includes a simple database to manage users, devices, and backups. The database design follows normalization rules to ensure data consistency. The main entities include Users, Devices, and BackupLogs.



5. UI/UX Design

The user interface emphasizes clarity, consistency, and ease of use. It allows administrators to view network status, manage devices, and monitor performance. The dashboard uses modern design principles with intuitive navigation and clear icons.



6. Network Design

The network consists of three main branches connected via routers and a central backup server. VLANs are implemented for departmental segmentation, and redundancy ensures network availability in case of link or device failure.

7. Configuration Summary

Each router and switch is configured using Huawei commands in eNSP. DHCP is enabled on each branch router to assign IPs dynamically. Static routes ensure inter-branch connectivity, and the central router manages redundancy between paths.

1. Router Configurations

Router AR1 – Branch 1

- Interfaces:
- G0/0/0 (LAN): 192.168.10.1 /24 → connected to LSW1
- G0/0/1 (WAN): 10.0.0.1 /30 → connected to AR3
- Routing:
- Static route to Branch 2 → 192.168.20.0/24 via 10.0.0.2
- DHCP Configuration:
- DHCP enabled
- IP Pool BRANCH1
- Network: 192.168.10.0 /24
- Gateway: 192.168.10.1
- Excluded range: 192.168.10.1 – 192.168.10.10
- DNS: 8.8.8.8
- Interface G0/0/0 assigned as DHCP Global Interface

Router AR2 – Branch 2

- Interfaces:

- G0/0/0 (LAN): 192.168.20.1 /24 → connected to LSW2
- G0/0/1 (WAN): 10.0.0.5 /30 → connected to AR3
- Routing:
- Static route to Branch 1 → 192.168.10.0/24 via 10.0.0.6
- DHCP Configuration:
- DHCP enabled
- IP Pool BRANCH2
- Network: 192.168.20.0 /24
- Gateway: 192.168.20.1
- Excluded range: 192.168.20.1 – 192.168.20.10
- DNS: 8.8.8.8
- Interface G0/0/0 assigned as DHCP Global Interface

Router AR3 – Core Router

- Interfaces:
- G0/0/0: 10.0.0.2 /30 → connected to AR1
- G0/0/1: 10.0.0.6 /30 → connected to AR2
- Routing:
- Static route to Branch 1 → 192.168.10.0/24 via 10.0.0.1
- Static route to Branch 2 → 192.168.20.0/24 via 10.0.0.5

2. Switch Configurations

Switch LSW1 (Branch 1 Access Switch)

- Ports: GigabitEthernet0/0/1 to 0/0/4
- All interfaces enabled (undo shutdown)
- Connected to AR1 and local PCs

Switch LSW2 (Branch 2 Access Switch)

- Ports: GigabitEthernet0/0/1 to 0/0/4
- All interfaces enabled (undo shutdown)
- Connected to AR2 and local PCs

SW1 / SW2 (Additional Switches)

- Ports Ethernet0/0/1 to Ethernet0/0/3
- All interfaces enabled (undo shutdown

3. Network Summary

- Total Routers: 3 (AR1, AR2, AR3)
- Total Switches: 4 (LSW1, LSW2, SW1, SW2)
- IP Addressing Scheme:
- Branch 1 LAN: 192.168.10.0 /24
- Branch 2 LAN: 192.168.20.0 /24
- WAN Links: 10.0.0.0 /30 and 10.0.0.4 /30
- Routing Type: Static Routing
- DHCP: Configured on Branch Routers
- DNS: 8.8.8.8

8. Security and Backup

To ensure data integrity, confidentiality, and secure access within the enterprise network, several security mechanisms were implemented across all network devices (routers and switches):

SSH Secure Access:

SSH was configured on all routers to replace Telnet for encrypted remote management. Local user accounts with strong passwords and privilege levels were created for administrators to access the devices securely.

Console and VTY Password Protection:

Console and virtual terminal lines were secured with authentication passwords to prevent unauthorized physical or remote access.

Security Banners:

A warning banner was configured on all devices to notify users that access is restricted to authorized personnel only, providing legal protection and clear access policies.

Interface Security:

Unused interfaces on routers and switches were administratively shut down to prevent unauthorized connections and reduce security risks.

Port Security on Switches:

For end-user ports (especially on management VLAN 99), port security was enabled to restrict the number of MAC addresses allowed per port. Sticky MAC learning was used to bind devices automatically.