

Institut National des Postes et Télécommunications



Network Design Solutions

BankNet: Enterprise Bank Network Design

Author: El Mahdi ARFAL

Academic Year: 2024/2025



February 20, 2025

Abstract

The BankNet project implements a scalable, segmented, and secure enterprise network tailored to a banking institution. The network uses a collapsed-core architecture with Layer 3 switches handling both core and distribution roles. It includes 12 VLANs (11 departments and a server room), dynamic OSPF routing, inter-VLAN communication, centralized DHCP/DNS services, HSRP redundancy, and FTP, HTTP, and Mail servers for operational functionality. Security is enforced via switchport security and ACLs on the edge router. Though QoS and monitoring were considered, they were not implemented in this version.

Contents

1	Problem Statement	2
2	System Breakdown	2
2.1	Solution Architecture	2
2.2	Hardware Used	3
2.3	Service Selection Rationale	3
3	Tasks Performed	3
3.1	Architecture Design	3
3.2	Device Configuration	3
3.3	Service Deployment	3
4	Challenges Faced	4
5	Service Summary	4
6	Conclusion	4

1. Problem Statement

Bank networks must ensure secure internal segmentation, controlled external access, and uninterrupted access to central services. Requirements include:

- VLAN separation per department
- Central services (FTP, HTTP, Mail, DHCP, DNS)
- Routing and redundancy with high availability
- External security via ACLs and NAT

2. System Breakdown

2.1 Solution Architecture

This network follows a **collapsed core architecture**, where Layer 3 switches serve both distribution and core functions. The design offers high availability and scalability.

- **Access Layer:** 12 switches, each for a department or the server room
- **Collapsed Core Layer:** 4 L3 switches in two redundant pairs with HSRP and OSPF
- **Edge Layer:** 4 routers, with the edge router connecting to the ISP (NAT + ACLs)
- **Servers:** DHCP-DNS, FTP (NAS), HTTP, and Mail servers in the server room

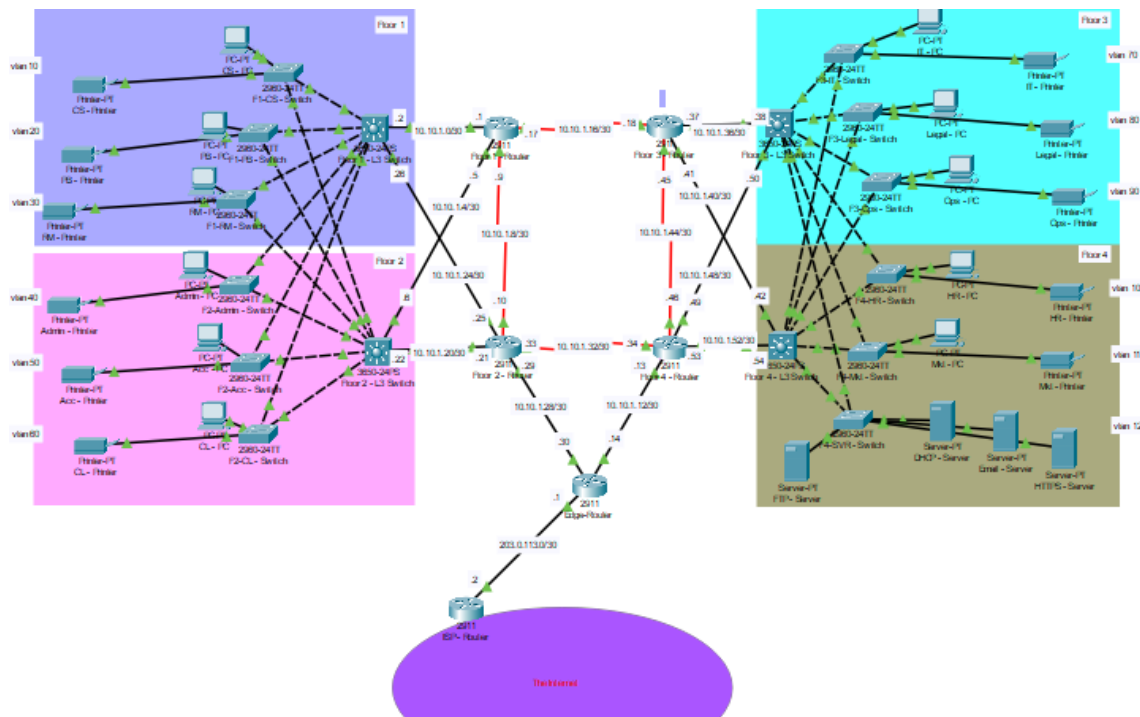


Figure 1: Bank Network Topology

2.2 Hardware Used

Component	Purpose
L3 Switches	Routing, HSRP, OSPF, VLAN gateways
Access Switches	Endpoint access, VLAN enforcement, port security
Routers	Core interconnect, ACLs, NAT at the edge
DHCP-DNS Server	Dynamic addressing and name resolution
FTP Server	NAS for internal file storage
HTTP Server	Hosts internal web applications or portal
Mail Server	Internal email services

2.3 Service Selection Rationale

- **HSRP on L3 Switches:** Ensures gateway redundancy for departments
- **OSPF:** Efficient routing across switches and routers
- **ACLs:** Centralized filtering at the edge router only
- **FTP, HTTP, Mail Servers:** Core operational services hosted internally
- **STP:** Ensures loop prevention and network stability
- **DHCP/DNS:** Unified configuration on a dedicated server

3. Tasks Performed

3.1 Architecture Design

- Designed collapsed core topology with redundancy
- Defined 12 VLANs and access switch assignments
- Implemented dual path via HSRP-enabled L3 switches

3.2 Device Configuration

- SSH-enabled secure management access
- VLANs and switchport security on access switches
- OSPF setup across L3 switches and routers
- ACLs and NAT configured on edge router

3.3 Service Deployment

- DHCP and DNS configured on a central DHCP-DNS server
- Set `ip helper-address` on SVIs for DHCP relay
- Deployed FTP (NAS), HTTP, and Mail servers internally

4. Challenges Faced

- **HSRP Placement:** Choosing L3 switches over routers for redundancy
- **OSPF Convergence:** Forgot to give each pair of layer 3 switches different router-ids since both were assigned the same router-id due to sharing the same SVIs to handle inter-VLAN Routing and have redundancy with HSRP.

5. Service Summary

Service	Status
VLANs	12 total (11 departments + 1 server room)
Inter-VLAN Routing	SVIs on L3 switches
HSRP	Enabled on L3 switch pairs
DHCP/DNS	Configured on dedicated server with relay
FTP Server	Main NAS within the network
HTTP Server	Internal web hosting
Mail Server	Internal email communication
NAT	Edge router translating public access
ACLs	Applied only at the edge
STP	Loop prevention on switching layer
Port Security	Applied on access switches

6. Conclusion

This bank network is a robust implementation of enterprise network principles using a collapsed core architecture. It ensures segmentation, redundancy, centralized services, and secure external access. While QoS and monitoring remain for future enhancements, the current design supports high availability, service delivery, and scalability across all bank departments.