Enterprise Network Design and Implementation Documentation

Introduction

This document presents the design and implementation of a secure, scalable, and highly available enterprise network infrastructure for a multi-department organization operating from a multi-floor headquarters and an external server-side site. The design prioritizes confidentiality, integrity, and availability (CIA) while ensuring redundancy, performance, and future scalability.

The network solution is designed and implemented using Cisco Packet Tracer, following a hierarchical network design model, and incorporates VLAN segmentation, inter-VLAN routing, dynamic and static IP addressing, VoIP services, Access Control Lists (ACLs), Network Address Translation (NAT), and site-to-site IPsec VPN.

Design Objectives

The main objectives of the network design are:

- High availability through redundancy at all layers
- Secure communication between headquarters and external server-side site
- Departmental isolation using VLANs and subnetting
- Support for both data and voice services
- Centralized services (DHCP, DNS, WEB, EMAIL) hosted externally
- Controlled administrative access using SSH and ACLs
- Secure internet access using NAT and ACL policies
- Secure WAN communication using IPsec VPN
- Scalability to support future growth

Network Design Model

The network follows the Hierarchical Network Design Model, consisting of :

Core Layer

- Handles high-speed routing and switching
- Provides redundancy and inter-VLAN routing
- Runs OSPF routing protocol

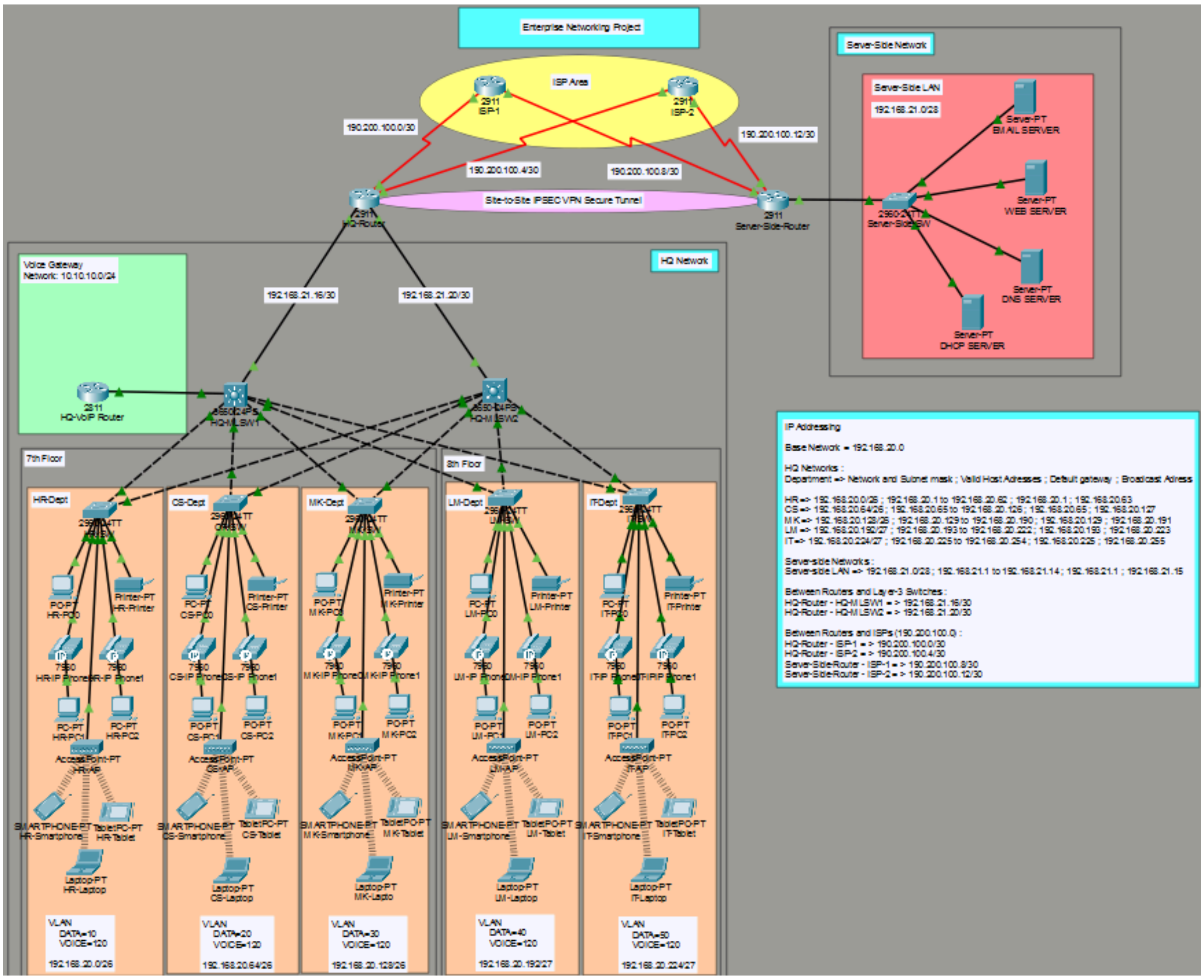
Distribution Layer

- Multilayer switches act as distribution devices
- Enforces VLAN segmentation and routing policies

Access Layer

- Six access switches
- Connects end-user devices, IP phones, and wireless access points
- Implements VLAN assignment and port security

Physical and Logical Network Overview



IP Addressing

Base Network = 192.168.20.0

HQ Networks :
Department => Network and Subnet mask ; Valid Host Adresses ; Default gateway ; Broadcast Adress

HR => 192.168.20.0/26 ; 192.168.20.1 to 192.168.20.62 ; 192.168.20.1 ; 192.168.20.63
CS => 192.168.20.64/26 ; 192.168.20.65 to 192.168.20.126 ; 192.168.20.65 ; 192.168.20.127
MK => 192.168.20.128/26 ; 192.168.20.129 to 192.168.20.190 ; 192.168.20.129 ; 192.168.20.191
LM => 192.168.20.192/27 ; 192.168.20.193 to 192.168.20.222 ; 192.168.20.193 ; 192.168.20.223
IT => 192.168.20.224/27 ; 192.168.20.225 to 192.168.20.254 ; 192.168.20.225 ; 192.168.20.255

Server-side Networks :
Server-side LAN => 192.168.21.0/28 ; 192.168.21.1 to 192.168.21.14 ; 192.168.21.1 ; 192.168.21.15

Between Routers and Layer-3 Switches :
HQ-Router - HQ-MLSW1 = > 192.168.21.16/30
HQ-Router - HQ-MLSW2 = > 192.168.21.20/30

Between Routers and ISPs (190.200.100.0) :
HQ-Router - ISP-1 = > 190.200.100.0/30
HQ-Router - ISP-2 = > 190.200.100.4/30
Server-Side-Router - ISP-1 = > 190.200.100.8/30
Server-Side-Router - ISP-2 = > 190.200.100.12/30

Headquarter (HQ) Building:

Floor	Departments	Description
Floor 7	HR, CS, MK	Each department has at least 40 user devices plus 40 IP phones, and one WiFi-Access Point.
Floor 8	LM, IT	Each department has at least 20 user devices plus 20 IP phones, and one WiFi-Access Point.

- HR : Human Resource
- CS : Customer Service
- MK : Marketing
- LM : Legal Management
- IT : Information Technology

Remote site:

Server-side	DHCP, DNS, WEB, and EMAIL servers.

IP Addressing

HQ Network					
Department	VLAN	Network and Subnet Mask	Valid Host Addresses	Default Gateway	Broadcast Address
HR	DATA=10 VOICE=120	192.168.20.0/26	192.168.20.1 to 192.168.20.62	192.168.20.1	192.168.20.63
CS	DATA=10 VOICE=120	192.168.20.64/26	192.168.20.65 to 192.168.20.126	192.168.20.65	192.168.20.127
MK	DATA=10 VOICE=120	192.168.20.128/26	192.168.20.129 to 192.168.20.190	192.168.20.129	192.168.20.191
LM	DATA=10 VOICE=120	192.168.20.192/27	192.168.20.193 to 192.168.20.222	192.168.20.193	192.168.20.223
IT	DATA=10 VOICE=120	192.168.20.224/27	192.168.20.225 to 192.168.20.254	192.168.20.225	192.168.20.255
Server-side Network					
Server-side LAN	—	192.168.21.0/28	192.168.21.1 to 192.168.21.14	192.168.21.1	192.168.21.15

VLAN Configuration

- Each department operates in a separate data VLAN
- Voice traffic is separated using a dedicated voice VLAN
- Access ports configured with:
  - Data VLAN
  - Voice VLAN

- Trunk links configured between switches using IEEE 802.1Q
- Implemented on multilayer switches using Switch Virtual Interfaces (SVIs)
- Each VLAN has a corresponding SVI acting as the default gateway
- IP routing enabled on multilayer switches
  - Between Routers and Layer-3 Switches :
  - HQ-Router - HQ-MLSW1 = > 192.168.21.16/30

    - HQ-Router - HQ-MLSW2 = > 192.168.21.20/30
- OSPF used to advertise VLAN networks

WAN / ISP Connectivity

- Two ISPs connected to headquarters routers
- Each router connects to both ISPs for:
    - Redundancy
    - Load balancing
- Public IP addresses used on WAN interfaces
- OSPF (Open Shortest Path First) used for route advertisement
    - Between Routers and ISPs (190.200.100.0) :
    - HQ-Router - ISP-1 = > 190.200.100.0/30
    - HQ-Router - ISP-2 = > 190.200.100.4/30
    - Server-Side-Router - ISP-1 = > 190.200.100.8/30
    - Server-Side-Router - ISP-2 = > 190.200.100.12/30
- Single OSPF area used for simplicity and efficiency

Server-Side Site Design

- Servers are not part of the LAN and are accessible only via WAN/Internet.
- All server devices use **static IP addressing.**
    - EMAIL SERVER = 192.168.21.8
    - WEB SERVER = 192.168.21.7
    - DNS SERVER = 192.168.21.6
    - DHCP SERVER = 192.168.21.5
- Devices obtain IP addresses dynamically from the dedicated DHCP server. DHCP scopes are configured per VLAN.

VoIP and Telephony Services

- Cisco 2811 router used as voice gateway
    - Voice subnet = 10.10.10.0/24
- Connected to a multilayer switch at headquarters
- Voice VLAN configured on access ports
    - Voice VLAN ID = 120 (used across the entire network)
    - IP phones obtain IP addresses and line numbers from the VoIP router
- Dial numbers allocated in the format 4XX
- Users within departments can communicate using IP phones

NAT and Internet Access

- PAT (Port Address Translation) configured
- Uses outbound router interface IP address

- Standard ACL defines internal networks allowed NAT access
- Ensures controlled and secure internet connectivity

Network Security Implementation

Basic Device Security

- Hostnames configured on all devices
- Console and enable passwords configured
- Password encryption enabled
- IP domain lookup disabled
- Login banners configured

SSH Configuration

- SSH enabled on all routers and multilayer switches
- Local user accounts created
- RSA keys generated
- Telnet disabled
- Standard ACL applied to VTY lines
- Only IT department subnet allowed SSH access
- All other networks denied administrative access

Switch Port Security

- Implemented on server-site access switch
- One device allowed per port
- Sticky MAC address learning enabled
- Violation mode set to shutdown

Site-to-Site IPsec VPN

- Configured between headquarters router and server-side router
- Ensures encrypted communication over WAN

Testing and Verification

The following tests were performed:

- End-to-end device connectivity (Ping)
- Inter-VLAN communication
- DHCP address allocation
- VoIP call testing between departments
- Internet access via NAT
- Secure SSH access from authorized subnet
- VPN tunnel establishment and encrypted traffic verification

- Server accessibility from permitted networks
- All configurations were verified to be functioning as expected.

Conclusion

The implemented network infrastructure meets all design requirements for performance, redundancy, scalability, and security. By leveraging VLANs, OSPF routing, ACLs, NAT, VoIP services, and IPsec VPN, the network ensures efficient and secure communication across all departments and external resources. The hierarchical design model guarantees resilience and simplifies future expansion.