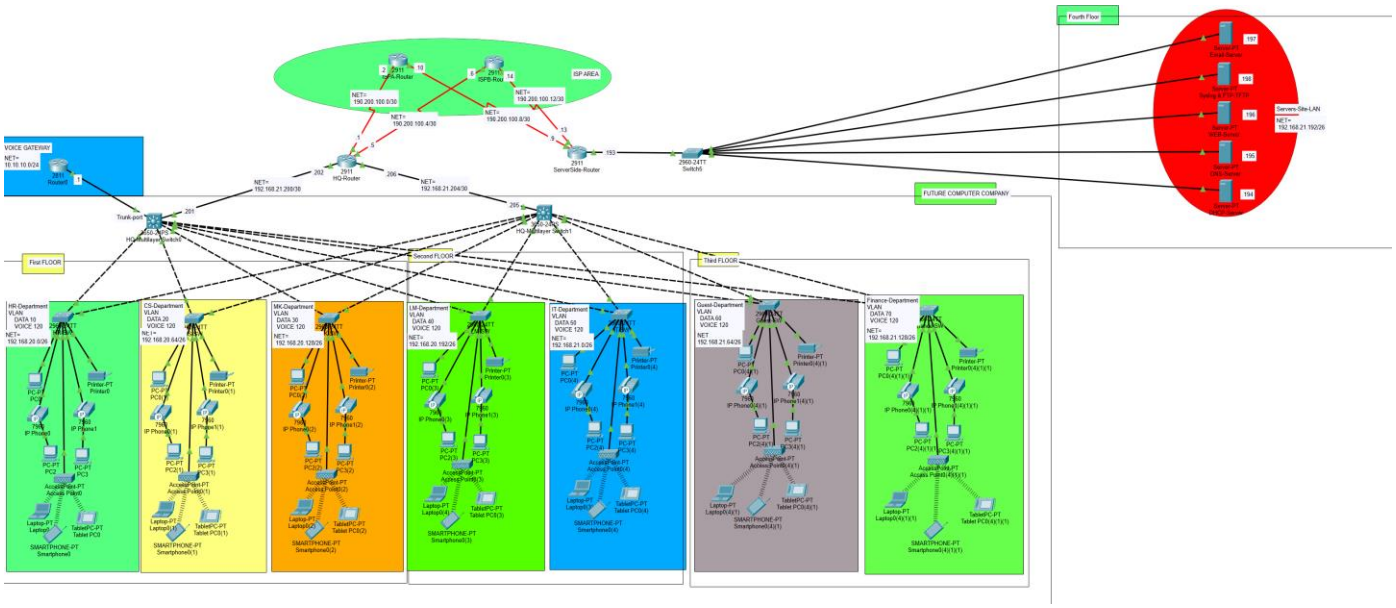
Enterprise Network Infrastructure Project Documentation

1. Objective

Design and implement a robust network infrastructure for an organization that requires seamless integration of various network services and security protocols. The project aims to create a **scalable**, **secure**, and **efficient** network environment to support voice, data, and internet services across multiple departments and floors of the enterprise.

2. Scope of Work

Full Network Design with Security Implementation



2.1 Network Segmentation and OSPF Configuration

- **13 Distinct Networks** were designed across departments and server rooms with appropriate subnetting:
  - Departmental Subnets (HR, CS, MK, LM, IT, Guest, Finance)
  - Server LAN (DHCP, Email, HTTPS)
  - Inter-switch Links and ISP Uplinks
- **OSPF Protocol** is configured for dynamic routing:
  - Supports automatic network discovery
  - Efficient route updates
  - Enhances scalability with area configurations to reduce routing table sizes

Example Configuration Snippet:

```
bash
CopyEdit
router ospf 1
 network 192.168.20.0 0.0.1.255 area 0
 network 192.168.21.0 0.0.1.255 area 0
 network 190.200.100.0 0.0.0.15 area 0
```

2.2 VLAN Configuration

- **VLANs Defined:**
  - VLAN 10: HR
  - VLAN 20: CS
  - VLAN 30: Marketing
  - VLAN 40: IT
  - VLAN 50: Management
  - VLAN 60: Finance
  - VLAN 100-120: Server VLANs (DHCP, Email, HTTPS)
- **Switch Types:**
  - Layer 2 (Access) Switches assigned VLANs with access/trunk port configurations
  - Layer 3 (Core) Switch for inter-VLAN routing

Example VLAN Setup:

```
bash
CopyEdit
vlan 10
 name HR
interface range FastEthernet0/1-12
 switchport mode access
 switchport access vlan 10
```

2.3 Wireless Network Setup

(Planned for integration; implementation pending hardware deployment)

- Use of dual SSIDs:
  - **Staff SSID** (secured with WPA3 Enterprise)
  - **Guest SSID** (secured with WPA2 PSK, VLAN-isolated)
- Wireless Controller or APs will ensure:
  - **Segmentation** via VLAN tagging
  - **Authentication** through RADIUS
  - **Traffic control** and monitoring for guests vs. staff

2.4 IP Telephony Integration

- **Voice VLAN 120** configured for IP Phones
- **Router Subinterface** for voice traffic:

```
bash
CopyEdit
interface GigabitEthernet0/0.120
 encapsulation dot1Q 120
 ip address 10.10.10.1 255.255.255.0
```

- **QoS** will be configured to prioritize voice over data traffic
- **DHCP Options (Option 150)** reserved to provide TFTP/IP Phone boot information (to be configured in DHCP server)

2.5 Port Address Translation (PAT)

- PAT allows multiple internal devices to access the Internet via a single **public IP address**
- Configured at the edge router/firewall:

```
bash
CopyEdit
ip nat inside source list 1 interface GigabitEthernet0/1 overload
access-list 1 permit 192.168.20.0 0.0.3.255
```

- Ensures efficient **IP utilization** and **secure outbound communication**

2.6 Dynamic Host Configuration Protocol (DHCP)

- DHCP Server assigned IP scopes for each VLAN
- Subnet-specific **DHCP scopes**:

Department	Scope Range	Subnet Mask
HR	192.168.20.1 – 192.168.20.62	255.255.255.192
CS	192.168.20.65 – 192.168.20.126	255.255.255.192
MK	192.168.20.129 – 192.168.20.190	255.255.255.192
LM	192.168.20.193 – 192.168.20.254	255.255.255.192
IT	192.168.21.1 – 192.168.21.62	255.255.255.192
Guest	192.168.21.65 – 192.168.21.126	255.255.255.192
Finance	192.168.21.129 – 192.168.21.190	255.255.255.192
Server LAN	192.168.21.193 – 192.168.21.254	255.255.255.192

- DHCP Options will include:
    - Default Gateway
    - DNS
    - Option 150 (IP phones)

2.7 Secure Shell (SSH) Access

SSH access is enabled on all core devices for secure remote management.

```
hostname bash
L3-SW
ip domain-name cisco.net
crypto key generate rsa
1024
username cisco password cisco
line vty 0 15
 login local
 transport input ssh
```

- **Local user authentication**
- **Password encryption**
- **Banner warnings** displayed to unauthorized users

2.8 Local Area Network (LAN) Security

Implemented **port-level security** on access switches:

```
bash
CopyEdit
interface range FastEthernet 0/2-5
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security mac-address sticky
 switchport port-security violation shutdown
```

- **MAC filtering** and **port shutdown** on violation
- **Unused ports** assigned to VLAN 99 and administratively shut down
- Planned **802.1X authentication** and **NAC** policies for advanced endpoint control

---

Overall Summary

The network infrastructure is:

- **Logically segmented** using VLANs and subnets
- **Scalable and modular** with OSPF-based dynamic routing
- **Secure** with SSH access, port security, and VLAN isolation
- **Efficient** through the use of PAT and DHCP automation
- **Future-ready**, supporting IP telephony and wireless access

This design ensures **reliable, secure, and maintainable** operations for the organization while enabling future expansions or service integrations with minimal disruption.