

**1.1. Introduction**

The purpose of this report is to document the design and implementation of a comprehensive computer network for a three-story hotel, Vic Modem Hotel. The goal was to build a scalable, secure, and well-segmented network infrastructure to support the hotel's operational departments. This project was carried out during my internship at TTSET GLOBAL, where I was involved in planning, configuring, and testing network services including VLANs, routing (OSPF), DHCP, SSH, and port security.

**1.2. Project Objectives**

* Connect all departments across the hotel’s three floors.
* Configure and assign VLANs to each department.
* Enable inter-VLAN routing using OSPF.
* Configure DHCP servers for dynamic IP assignment.
* Set up secure remote access using SSH.
* Implement port security using the sticky MAC address method.

**1.3. Network Overview**

**Physical Layout:**

* Three Floors, each with a dedicated router (all located in the IT department's server room).
* Three switches, one per floor.
* WIFI Access Points on each floor.
* Printers and PCs per department.
* Floor Department VLAN and IP Scheme:
* Floor Department VLAN IP Network

1 Reception 80 192.168.8.0/24

Store 70 192.168.7.0/24

Logistics 60 192.168.6.0/24

2 Finance 50 192.168.5.0/24

HR 40 192.168.4.0/24

Sales/Marketing 30 192.168.3.0/24

3 Admin 20 192.168.2.0/24

IT 10 192.168.1.0/24

**Router Interconnection IPs:**

* R1-R2: 10.10.10.0/30
* R2-R3: 10.10.10.4/30
* R1-R3: 10.10.10.8/30

**1.4. Configuration Steps**

**4.1 VLAN Configuration (Switches)**

* Each switch was configured with specific VLANs corresponding to the departments.
* Ports were assigned to their VLAN using switchport access vlan [ID].
* Trunk links were enabled between routers and switches.

**4.2 Inter-VLAN Routing using OSPF**

**OSPF Process ID: 1**

* Each router was configured with router ospf 1 and appropriate network statements using wildcard masks.
* OSPF advertised both inter-router links and VLAN networks.

**Example:**

router ospf 1

network 192.168.1.0 0.0.0.255 area 0

network 10.10.10.0 0.0.0.3 area 0

**4.3 DHCP Configuration (Routers)**

Each router was configured to dynamically assign IPs to its VLANs:

ip dhcp pool VLAN10

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 192.168.1.1

**4.4 SSH Configuration**

For secure remote access to each router:

* ip domain-name gtech
* crypto key generate rsa
* username gtech password gtech
* line vty 0 15
* transport input ssh
* login local

Tested via Test-PC on IT floor.

**4.5 Port Security (IT Switch)**

Test-PC on port Fa0/1 was secured using sticky MAC:

interface fa0/1

switchport port-security

switchport port-security mac-address sticky

switchport port-security maximum 1

switchport port-security violation shutdown

**1.5. Testing & Troubleshooting**

* All PCs were tested for DHCP assignment.
* Inter-department ping tests were conducted.
* PCs with 169.254.x.x were debugged and corrected by checking VLAN configuration, DHCP bindings, and trunk settings.
* OSPF routing tables were validated using show ip route ospf.
* SSH access was successfully tested from Test-PC to router.
* Device connectivity was confirmed using ping tests (sr

**1.6. Challenges & Solutions**

DHCP Not Assigning IP: Solved by confirming trunk/VLAN interface status and correct DHCP pool.

Unreachable Hosts: Caused by missing OSPF network commands or incorrect interface configurations. Resolved by checking all router configs.

Sticky MAC not working: Ensured the PC connected before enabling sticky.

**1.7. Conclusion**

The Vic Modem Hotel Network was successfully designed and implemented to support the hotel's communication needs. By integrating VLANs, OSPF, DHCP, and SSH, the network is scalable, secure, and efficient. This project deepened my practical understanding of real-world network infrastructure design, routing protocols, and network security techniques.

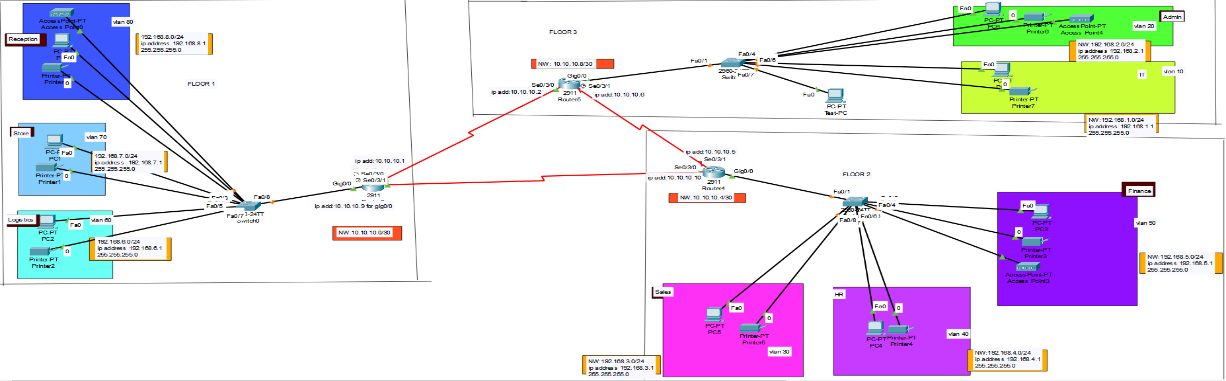
**1.8. Recommendations**

Implement network monitoring tools like SNMP.

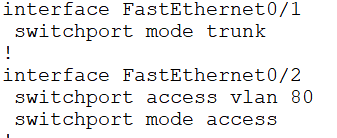
Introduce redundancy using HSRP or VRRP.

Set up firewall rules to enhance security.

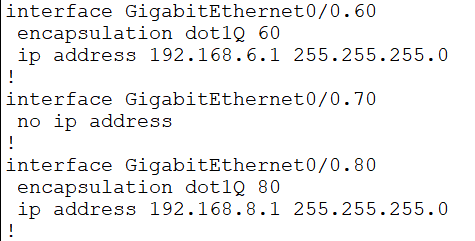
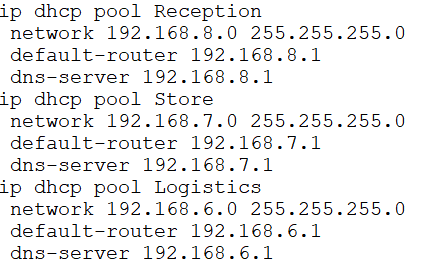
**1.9. Appendices**

****

**Network Diagram**

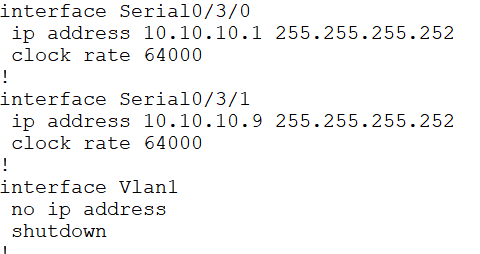
****

**Assigning ports to switch**

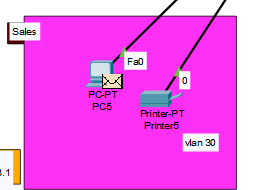
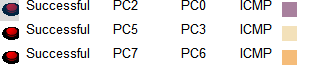
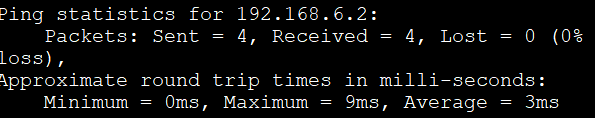
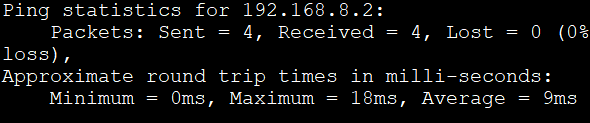
****

**Dhcp configuration**

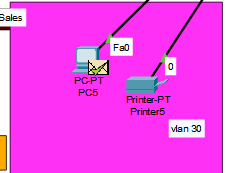
**Inter-vlan configuration and TCP Server**

****

**9.1. Ping Test Results**

****

**Email sent**

**=**

**Communication successful**

**9.2. VLAN Test (Segmentation Verification)**

**VLAN Devices Tested Result**

* VLAN 60 (Logistics) PC1, PC2 Communication OK
* VLAN 80 (Reception) PC3, PC4 Communication OK

**Observation:** Devices within the same VLAN can communicate; inter-VLAN routing works via Router1.

**9.3. Security Test (SSH & Port Security)**

* SSH Access: SSH login to Router1 successful.
* Port Security: Switch1 (fa0/2) blocks unauthorized MAC addresses as configured.
* Observation: Network access and security features are functioning as intended.

**9.4. DHCP Bindings Table**

**VLAN Department Device MAC Address IP Address Lease Expiry**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **80** | **Reception** | | **PC1** | | **00:1A:2B:80:01** | | | **192.168.8.11** | | **23h:59m** | |
| **80** | **Reception** | | **Laptop1** | | **00:1A:2B:80:02** | | | **192.168.8.12** | | **23h:58m** | |
| **80** | **Reception** | | **Phone1** | | **00:1A:2B:80:03** | | | **192.168.8.13** | | **23h:57m** | |
| **80** | **Reception** | | **Printer1** | | **00:1A:2B:80:04** | | | **192.168.8.14** | | **23h:56m** | |
| **70** | **Store** | | **PC2** | | **00:1A:2B:70:01** | | | **192.168.7.11** | | **23h:59m** | |
| **70** | | **Store** | | **Laptop2** | | **00:1A:2B:70:02** | **192.168.7.12** | | **23h:58m** | |
| **70** | | **Store** | | **Phone2** | | **00:1A:2B:70:03** | **192.168.7.13** | | **23h:57m** | |
| **70** | | **Store** | | **Printer2** | | **00:1A:2B:70:04** | **192.168.7.14** | | **23h:56m** | |
| **60** | | **Logistics** | | **PC3** | | **00:1A:2B:60:01** | **192.168.6.11** | | **23h:59m** | |
| **60** | | **Logistics** | | **Laptop3** | | **00:1A:2B:60:02** | **192.168.6.12** | | **23h:58m** | |
| **60** | | **Logistics** | | **Phone3** | | **00:1A:2B:60:03** | **192.168.6.13** | | **23h:57m** | |
| **60** | | **Logistics** | | **Printer3** | | **00:1A:2B:60:04** | **192.168.6.14** | | **23h:56m** | |