MIT Academy of Engineering
(An Autonomous Institute)

Computer Network Project Report

Title of Project

Trading Operations Support Centre – Network Infrastructure Design

MIT ACADEMY OF ENGINEERING, ALANDI (D), PUNE
Department of Computer Engineering

Group Members:

1. Krishna Mungase
2. Srushti Kapase
3. Adhven Patil

Table of Contents

Introduction

The Trading Operations Support Centre is relocating to a new three-floor facility that houses several departments, each requiring reliable network access for up to 120 users. The network must support internal file sharing, email, web access, and business applications hosted in the server room while providing high availability, predictable performance, and basic security.

The design follows a three-layer hierarchical model (Core, Distribution, Access) and uses VLAN segmentation, DHCP, OSPF, and PAT to meet these requirements. Cisco Packet Tracer was used to simulate the network, verify connectivity and failover between two ISP uplinks, and validate DHCP, NAT, and access-control behavior; this report focuses on the design, configuration examples, and verification steps suitable for a student-level project.

Objectives

- Implement a hierarchical network (Core, Distribution, Access).
- Provide Internet redundancy with two ISPs.
- Segment departments using VLANs and subnets.
- Provide DHCP for client IP allocation and static addressing for infrastructure.
- Configure dynamic routing (OSPF) and PAT for Internet access.
- Secure the network with SSH and ACLs.
- Verify design and failover in Packet Tracer.

Tools & Devices

- Cisco Packet Tracer (simulation) — packet file provided.
- Core Routers: Cisco 2900 Series (or similar).
- Distribution / Multilayer Switches: Cisco 3560 (Layer 3 capable).
- Access Switches: Cisco Catalyst series.
- Wireless Access Points (WAPs): 1 per floor for user Wi-Fi.
- Server Room devices: DHCP Server, DNS Server, Mail Server, Application Servers (12 devices).

Physical & Logical Topology

- **Core Layer:** Two core routers (CORE-R1, CORE-R2) with uplinks to two ISPs.
- **Distribution Layer:** Two multilayer switches (DIST-SW1, DIST-SW2) providing inter-VLAN routing and connecting access switches.
- **Access Layer:** Access switches on each floor connecting PCs, printers and WAPs.
- **Server Room:** Separate rack VLAN (VLAN 99) for all servers and infrastructure devices.

Redundant links exist between core and distribution devices; OSPF handles routing between devices.

Departments, VLANs & IP Addressing Plan

Base private network: 172.16.0.0 /16

Department / Area	VLAN ID	Subnet (Example)	Gateway (Example)
Sales	10	172.16.10.0 /24	172.16.10.1
HR & Logistics	20	172.16.20.0 /24	172.16.20.1
Finance	30	172.16.30.0 /24	172.16.30.1
Administration	40	172.16.40.0 /24	172.16.40.1
ICT Operations	50	172.16.50.0 /24	172.16.50.1
Servers	99	172.16.99.0 /24	172.16.99.1

Public ISP links (example /30 subnets):

- ISP-1: 195.136.17.0 /30 (link to CORE-R1)
- ISP-2: 195.136.17.4 /30 (link to CORE-R2)

Note: Replace example addresses with actual assigned public ranges when deploying live.

Protocols Used

- **OSPF (Open Shortest Path First):** Dynamic routing protocol used between routers and Layer 3 switches to share routes and provide redundancy.
- **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses and other settings (gateway, DNS) to client devices.
- **NAT / PAT (Network/Port Address Translation):** Translates private IP addresses to a public IP (PAT) so users can access the Internet.
- **SSH (Secure Shell):** Secure method for remote administration of routers and switches.
- **ACLs (Access Control Lists):** Simple filters to allow or block traffic between networks as per policy.

Security Measures

- Configure **SSH-only** access for device management; disable Telnet.
- Use **enable secret** and local user accounts with strong passwords; enable password encryption.
- Apply **ACLs** to restrict sensitive VLANs (for example, Finance) from accessing unnecessary resources.
- Place servers in a **separate VLAN (99)** and restrict access using ACLs.
- Regularly back up configurations and store them securely.

NAT and Internet Redundancy

- PAT (NAT overload) is configured on the edge router interface connected to the ISP to translate the internal address pool (172.16.0.0/16) to the public IP.
- Two ISP uplinks (different /30 subnets) allow failover. OSPF or static routes with different administrative distances/costs control primary/secondary ISP usage.

Implementation Steps

1. Create topology in Packet Tracer using the provided .pkt file as reference.
2. Configure VLANs on switches and set access/trunk ports correctly.
3. Configure SVI interfaces on multilayer switches (or configure router-on-a-stick where applicable) for inter-VLAN routing.
4. Set up DHCP pools on the DHCP server for each VLAN and exclude static IPs.
5. Configure OSPF on routers and L3 switches, advertise VLAN subnets and ISP links.
6. Configure PAT on the edge router (map internal network to public interface).
7. Secure devices with SSH, set banners, passwords and disable unused services.
8. Test connectivity, failover and security policies. Document test outputs.

Testing & Verification

Packet Tracer tests to perform and capture:

- **DHCP:** Verify clients receive IP from correct DHCP scope.
- **Inter-VLAN routing:** Ping between allowed VLANs and from clients to server VLAN.
- **OSPF:** Verify OSPF neighbor states (show ip ospf neighbor) and routing table (show ip route).
- **NAT/PAT:** Verify translation table (show ip nat translations) and Internet connectivity from a client.
- **ACLs:** Check that blocked flows are denied and allowed flows pass.
- **Failover:** Simulate ISP link failure and verify traffic uses the secondary ISP.

Recommended command outputs to capture as screenshots or logs:

- show ip route
- show ip ospf neighbor
- show ip dhcp binding
- show ip nat translations
- show running-config (relevant sections)

Results

- All clients receive addresses and can reach local servers and the Internet (when allowed by ACLs).
- OSPF converges and all internal routes are visible in routing tables.
- PAT translates internal addresses and Internet sessions succeed.
- ACLs correctly restrict access to sensitive resources.
- Redundant links and dual ISPs provide failover with minimal manual intervention.

Conclusion

The designed network meets the project goals of reliability, security and scalability. VLAN segmentation, OSPF routing, DHCP, PAT for Internet access, and ACLs together create a robust infrastructure for the Trading Operations Support Centre. The Packet Tracer simulation demonstrates expected behavior and provides a testbed for validating configuration before live deployment.

References

- Cisco IOS Command Reference (for OSPF, NAT, DHCP, ACLs, SSH)
- Cisco Packet Tracer documentation and lab guides
- Course lecture notes and instructor materials