


NETWORK ENGINEERING PROJECT

Network Implementation Final Report

Three-Tier Hierarchical Network Design & Deployment

 7 Implementation Modules

 Security Hardened

 Fully Verified

Implementation Roadmap

01

Executive Summary

Project scope, objectives, and key achievements overview

02

Module 1: Infrastructure Foundations

Three-tier hierarchy, SSH, RSA keys, and device hardening

03

Module 2-3: VLANs & Trunking

VLAN segmentation, 802.1Q trunks, PortFast configuration

04

Module 4-5: LACP & L3 Routing

Link aggregation, Port-Channel, routed ports

05

Module 6: OSPF Dynamic Routing

OSPF configuration, adjacency, Router-ID management

06

Module 7: Security & NAT

PAT, ACLs, default routes, internet egress



Network Topology & Evidence

Complete topology diagram and verification screenshots



Key Learnings

Troubleshooting insights and lessons learned

Executive Summary

🎯 Project Objective

Design and deployment of a **secure, redundant three-tier hierarchical network** supporting enterprise-grade connectivity with segmented VLANs, high-speed backbone aggregation, dynamic routing, and secure internet egress.

✔ Key Achievements

- ✔

VLAN Segmentation
4 functional VLANs deployed
- ✔

LACP Aggregation
Bundled Gigabit links
- ✔

OSPF Routing
Dynamic routing enabled
- ✔

NAT/PAT Security
Secure internet egress

⚠ Troubleshooting Journey

Each module presented unique challenges—from **configuration mode errors** and **Spanning Tree delays** to **Port-Channel mismatches** and **OSPF adjacency failures**. Every struggle led to deeper protocol understanding.

7

Implementation Modules

4

Functional VLANs

100%

Connectivity Verified

Real-world troubleshooting experience gained through hands-on problem resolution

Infrastructure Foundations & Hardening

Three-Tier Hierarchy

Used **Auto-Connect** tool to rapidly build the hierarchical structure, automatically linking Core, Distribution, and Access layers without manual port mapping.



Core Layer



Distribution



Access Layer

Security Implementation



SSH & RSA Keys

Secure remote access enabled



Privileged Passwords

Enable secret configured



Banner Message

Login warning activated

Verification

Enable Secret: class

Console/VTY: cisco

⚠ The Struggle: "Invalid Input" Errors

Problem:

Attempted to run `crypto key generate rsa` command but CLI kept rejecting with "invalid input" errors.

💡 Root Cause Analysis

The command was being executed in **privileged EXEC mode** instead of **global configuration mode**. Additionally, device hostname and domain name must be set before generating RSA keys.

🔧 Resolution Steps

1. Enter global config: `conf t`
2. Set hostname: `hostname Core-SW`
3. Set domain: `ip domain-name network.local`
4. Generate keys: `crypto key generate rsa`

💡 Lesson learned: Always verify configuration mode before executing global commands. The CLI context determines available command sets.

VLAN Segmentation & Trunking

VLAN Design

Divided the network into **four functional VLANs** to segment traffic and improve security and performance.

10**Management**

Network devices

**20****Finance**

Financial systems

**30****IT**

Technical staff

**99****Native**

Trunk native VLAN



802.1Q Trunk Configuration

Configured trunks between all switches to allow VLAN traffic to travel across the network infrastructure.

```
switchport mode trunk
```

```
switchport trunk allowed vlan 10,20,30,99
```

⚠️ Struggle #1: DHCP Failure

Symptom:

Host took too long to get an IP address on specific access port.

🔍 Diagnosis

Spanning Tree delay – Port was in learning/listening states before forwarding.

🔧 Solution

```
spanning-tree portfast
```

Allows immediate transition to forwarding state for host connectivity.

⚠️ Struggle #2: Native VLAN Mismatch

Symptom:

Console flooded with Native VLAN mismatch error logs.

🔧 Solution

Manually synchronized VLAN 99 as native VLAN across all trunk links:

```
switchport trunk native vlan 99
```

Backbone Aggregation & L3 Routing

🔗 LACP Link Aggregation

Bundled Gigabit links using **LACP (Link Aggregation Control Protocol)** to increase backbone bandwidth and eliminate single points of failure.



Increased BW

Combined throughput



Redundancy

Failover protection

// Create Port-Channel interface

```
interface Port-channel1
switchport mode trunk
switchport trunk allowed vlan 10,20,30,99
```

📡 Layer 3 Routing

Converted switch ports to **Routed Ports** for direct core router connection using Point-to-Point IP addressing.

// Convert to routed port

```
interface GigabitEthernet1/0/1
no switchport
ip address 10.0.0.1 255.255.255.252
no shutdown
```

🔥 Major Struggle: Port Suspension

❌ Critical Problem

Switch **suspended the ports** due to configuration mismatches between physical interfaces and the virtual Port-Channel.

🔍 Root Cause

Physical interfaces had conflicting configurations (speed, duplex, trunk settings) that didn't match the Port-Channel interface parameters. LACP requires **identical configurations** on all bundled ports.

🔑 Resolution Strategy

1 Default the Ports

```
default interface gig1/0/1-2
```

2 Build from Port-Channel First

```
interface Port-channel1
```

Configure trunk settings here

3 Add Physical Interfaces

```
channel-group 1 mode active
```

Inherits settings from Port-Channel

Redundant Routed Backbone with OSPF

OSPF Configuration

Configured **OSPF dynamic routing** between Multilayer Switches and Core Routers to enable automatic route advertisement and failover.

// OSPF Configuration on Multilayer Switch

```
router ospf 1
router-id 1.1.1.1
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 10.0.0.0 0.0.0.3 area 0
```



Dynamic Updates

Auto route propagation



Load Balancing

Equal-cost paths

Verification Commands

```
show ip ospf neighbor // Check adjacencies
```

```
show ip route ospf // View OSPF routes
```

```
show ip protocols // Verify OSPF status
```

OSPF Adjacency Failure

Problem

OSPF adjacency **would not form** between Core-R2 and multilayer switches. Neighbor table remained empty.

Dual Root Causes



Physical Port Mismatch

Cabling didn't match the configured interface assignments in the topology.



Missing Router-ID

Core-R2 had no explicit router-id, causing OSPF process instability.

Resolution

- ✓ Corrected physical cabling to match topology documentation
- ✓ Assigned explicit Router-ID on Core-R2:

```
router ospf 1
router-id 2.2.2.2
```

✓ **Result:** Full end-to-end connectivity verified from all VLAN PCs through OSPF routing table.

Security, NAT & Internet Egress

PAT Configuration

Configured **Port Address Translation (PAT)** to allow multiple internal hosts to share a single public IP address for internet access.

```
// NAT Access List
```

```
access-list 1 permit 192.168.0.0 0.0.255.255
```

```
// PAT Configuration
```

```
ip nat inside source list 1 interface Gig0/0/0 overload
```

GUEST_RESTRICTION ACL

Implemented access control list to **block internal network access** while allowing verified internet traffic for guest VLAN.

```
// ACL Rules
```

```
deny ip 192.168.99.0 0.0.0.255 10.0.0.0 0.0.0.255  
deny ip 192.168.99.0 0.0.0.255 172.16.20.0 0.0.0.255  
permit ip any any
```

"Destination Host Unreachable"

Problem

Internet pings failed with **"Destination host unreachable"** errors. No external connectivity despite NAT configuration.

Root Causes Identified



Missing Default Route

No gateway of last resort configured on multilayer switches.



NAT Scope Too Small

ACL didn't include all 192.168.x.x VLAN ranges.


Resolution

1. Added Static Default Route:

```
ip route 0.0.0.0 0.0.0.0 10.0.0.6
```

2. Expanded NAT ACL:

```
access-list 1 permit 192.168.0.0 0.0.255.255
```

 **Final Status:** All VLANs routing, Internet link active, GUEST_RESTRICTION confirmed on both multilayer switches with 151+ matches.

Key Learnings & Troubleshooting Insights

01 Configuration Mode Awareness

The Struggle

"Invalid input" errors when generating RSA keys

The Lesson

Always verify you're in **global configuration mode (conf t)** before executing global commands. CLI context determines available command sets.

02 Spanning Tree Behavior

The Struggle

DHCP failures due to port learning/listening delays

The Lesson

Apply **PortFast** on access ports connecting to end hosts. This bypasses STP learning states for immediate connectivity.

03 Port-Channel Build Sequence

The Struggle

Ports suspended due to configuration mismatches

The Lesson

Always build Port-Channels from the **virtual interface down**. Default physical ports first, then configure Port-Channel, then add members.

04 OSPF Router-ID & Physical Connectivity

The Struggle

OSPF adjacency wouldn't form

The Lesson

Verify **physical cabling matches topology** and always assign explicit Router-ID for OSPF stability.

05 NAT Scope Planning

The Struggle

"Destination host unreachable" errors

The Lesson

Ensure **NAT ACL includes all internal subnets** and always configure a default route for internet egress.



Overall Insight

Every struggle was an opportunity to understand the **"why"** behind the configuration. Troubleshooting not only aided in fixing errors but also improved my practical knowledge on the subject of networking



Project Complete

All configurations saved to **startup configuration**

Network operational with full redundancy, security policies enforced, and internet connectivity verified



Fully Redundant

LACP + OSPF failover



Security Hardened

SSH, ACLs, VLAN segmentation



Internet Ready

NAT/PAT verified operational



Real-world troubleshooting experience gained through hands-on problem resolution