Machina WAN Network Design Project
Team Contribution Report

Prepared by: Aaron Foster

Project Manager & Documentation Lead

Course: WAN Technologies

Course: CS 351

Date: November 2025

Aaron Foster – Project Manager & Documentation Lead

As Project Manager and Documentation Lead, I directed the full planning, coordination, and execution of the Machina WAN Network Design Project. After the previous presentation cycle, I transitioned into the Documentation Lead role while continuing to oversee project direction, task management, and team communication.

I also created and managed the GroupMe team communication channel, ensuring consistent updates, quick responses, and a unified workflow. This kept every team member aligned throughout all network topology versions and documentation phases.

Project Contributions

1. Project Vision & Overview

- Created the main Project Overview used in the final report and presentation.
- Defined core project goals: security, scalability, Quality of Service (QoS), redundancy, automation, and disaster recovery.
- Ensured the team shared a unified understanding of deliverables, timelines, and expectations.

2. Team Coordination & Workflow Management

- Acted as the central communication and organization lead for the project.
- Assigned tasks based on team members' strengths and availability.
- Clarified project objectives and kept the team aligned with instructor milestones.
- Established and maintained the GroupMe group chat as the primary communication method for collaboration and status updates.

3. Presentation Creation & Polishing

- Designed, structured, and polished the entire final presentation.
- Organized slides for clarity, technical accuracy, and smooth logical flow.
- Integrated key visuals, including:
  - Evolution of the network topology (v0–v5)
  - Color-coded departmental overlays
  - Final physical rack diagram and layout
- Ensured consistent formatting, visual style, and professional quality across all slides.

4. Documentation Leadership

- Led the creation, editing, and organization of the final technical report.
- Ensured alignment between Packet Tracer implementation and documentation, including:
  - IP addressing tables
  - OSPF router IDs
  - VLAN schemas
  - DHCP pools
  - Security and DRP sections
- Maintained version control as the network topology evolved through multiple iterations.
- Reviewed and integrated all team member contributions into a cohesive final document.

5. Quality Assurance & Final Review

- Double-checked all critical network configurations for correctness, including:
  - Routing and OSPF
  - VLANs and inter-VLAN routing
  - IP addressing and subnetting
  - DHCP assignments and scope alignment
  - Security controls and Disaster Recovery Plan (DRP) elements

- Verified that diagrams, descriptions, and explanations aligned with the completed v5 topology and Packet Tracer build.
- Performed the final polish pass on both the written report and the presentation to ensure they were complete, accurate, and ready for submission.

Summary

My role ensured the project stayed organized, technically accurate, visually polished, and fully aligned with the assignment goals. I coordinated the team's workflow, created and managed the GroupMe communication structure, designed the final presentation, and led the documentation effort to produce a professional and cohesive final deliverable.

Network Design and Implementation Report

Prepared by: Marquis Buckley Course/

Project: CS 350

Date: November 18, 2025

1. Network Overview

1.1.WAN (Network Layer)

Routers: Cisco 2811

Modules Installed:

- NM-4E (4 Ethernet expansion ports)
- HWIC-4ESW (4-port switch module)

Cabling Between Routers:

- Primary links: Copper straight-through
- Secondary/backup links: Copper cross-over

Purpose:

- Provide a redundant, scalable backbone
- Support dynamic routing and reliable inter-departmental communication

1.2.Distribution Layer

Switches: Cisco 2960
Cabling: Straight-through or cross-over depending on interface type
Purpose:

- Connect core routers to departmental LANs
- Extend access to end devices

1.3.Access Layer

End Devices: PCs, laptops, and department-specific equipment
Cabling: Copper straight-through
Purpose:

- Provide user access to LAN and WAN services

2. Router Configuration

General configuration was applied to all six Cisco 2811 routers, including hostnames, interfaces, routing, and verification.

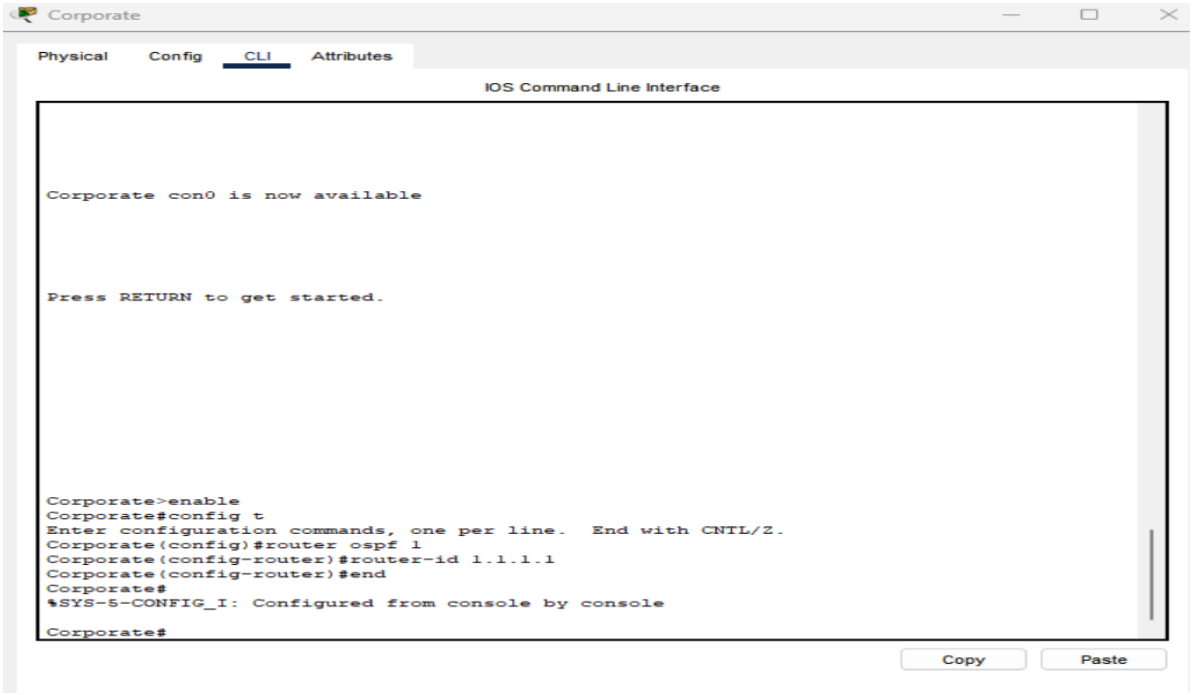
2.1.Basic Setup

Assign Router Name

configure terminal
hostname <RouterName>

Set OSPF Router ID

router ospf 1
router-id <X.X.X.X>



2.2.Interface Configuration

Configure Interfaces

interface <interface-name>
ip address <IP> <mask>
no shutdown

Interfaces Included:

- Router-to-router links (straight-through primary / cross-over secondary)

- Redundant/backup links
- Router-to-switch departmental links

2.3.OSPF Routing

Enable OSPF

router ospf 1

Advertise Networks

network <network> <wildcard> area 0

OSPF Notes:

- All routers use Area 0
- Only directly connected networks are advertised
- Each router has a unique router-ID

2.4.Router Verification

Check Interface Status

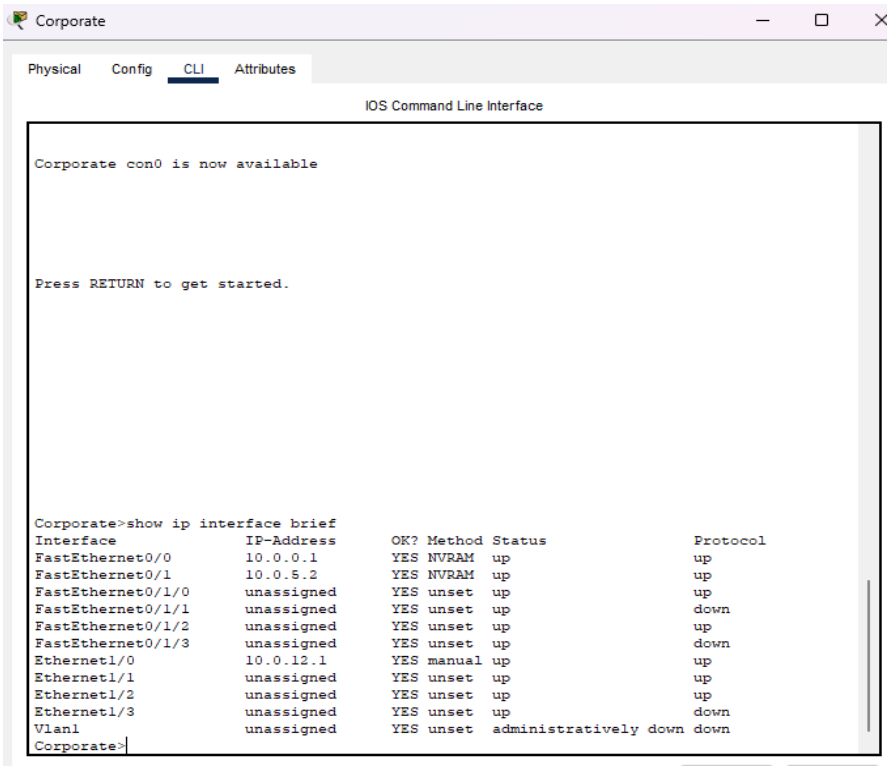
show ip interface brief

Check OSPF

show ip ospf neighbor
show ip route ospf
show ip ospf

Check Routing Table

show ip route



3. Switch Configuration (Distribution Layer)

Cisco 2960 switches were configured for basic connectivity. No VLANs were used.

3.1.Basic Setup

Assign Hostname

configure terminal
hostname <SwitchName>

Save Configuration

write memory

3.2.Port Configuration

Enable Router-to-Switch Ports

interface <port>
no shutdown

Enable End Device Ports

interface <port>
no shutdown

Cabling:

- Straight-through (router → switch)
- Straight-through (switch → end devices)

3.3.Switch Verification

Check Port Status

show interface status

Check Connectivity

show interfaces

4. End Device Configuration

All end devices used DHCP for IP assignments and were connected directly to the distribution switches.

4.1.Device Overview

- PCs
- Laptops
- Department-specific devices
- Connected via copper straight-through cables

4.2.IP Configuration

All devices were set to **DHCP**, receiving:

- IP address
- Subnet mask
- Default gateway
- DNS server

All assigned by a central server.

4.3.Connectivity Testing

Check IP Assignment

ipconfig

Ping Default Gateway

ping <gateway-IP>

Ping Other Subnets

ping <remote-IP>

5. Server Configuration

A dedicated server provides core network services for all departments.

5.1.Server Services

The server was configured to provide:

- **DHCP**
- **DNS**
- **Email**
- **Web hosting**

These services support automatic device configuration, internal communication, and access to shared resources.

5.2.DHCP

- Assigned IP addresses to all end devices
- Delivered default gateway and DNS settings
- Maintained separate DHCP scopes for each departmental subnet

5.3.DNS

- Provided internal hostname resolution
- Mapped server names and internal service names to IP addresses
- Allowed devices to access internal web services using simple hostnames

5.4.Email Service

- Enabled internal email communication
- Supported sending/receiving messages between departments
- Ran entirely on the internal network

5.5.Web Hosting

- Hosted internal webpages
- Accessible using http://<Server-IP> or http://<Server-Hostname>

5.6.Server Verification

DHCP

ipconfig

DNS

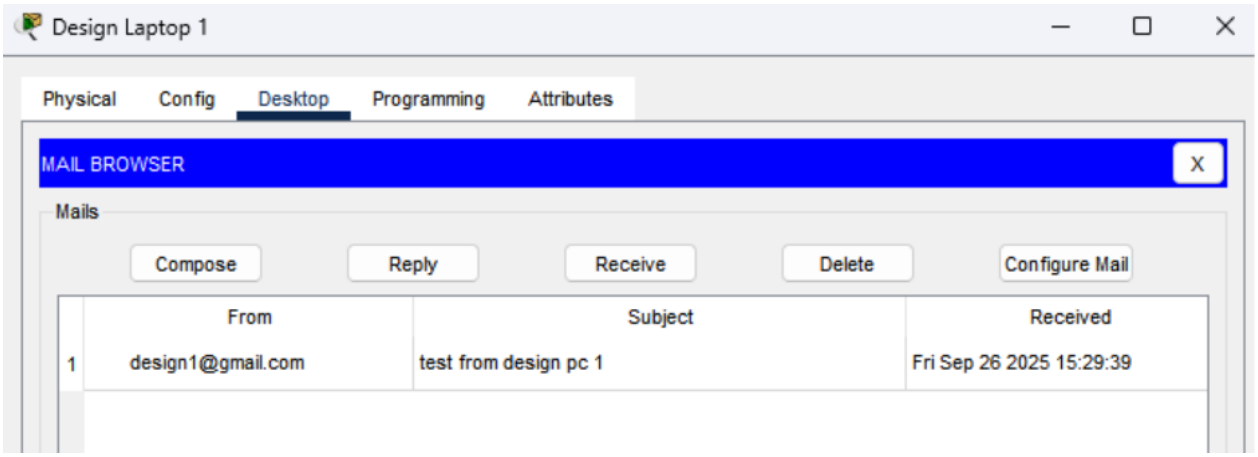
ping <server-hostname>

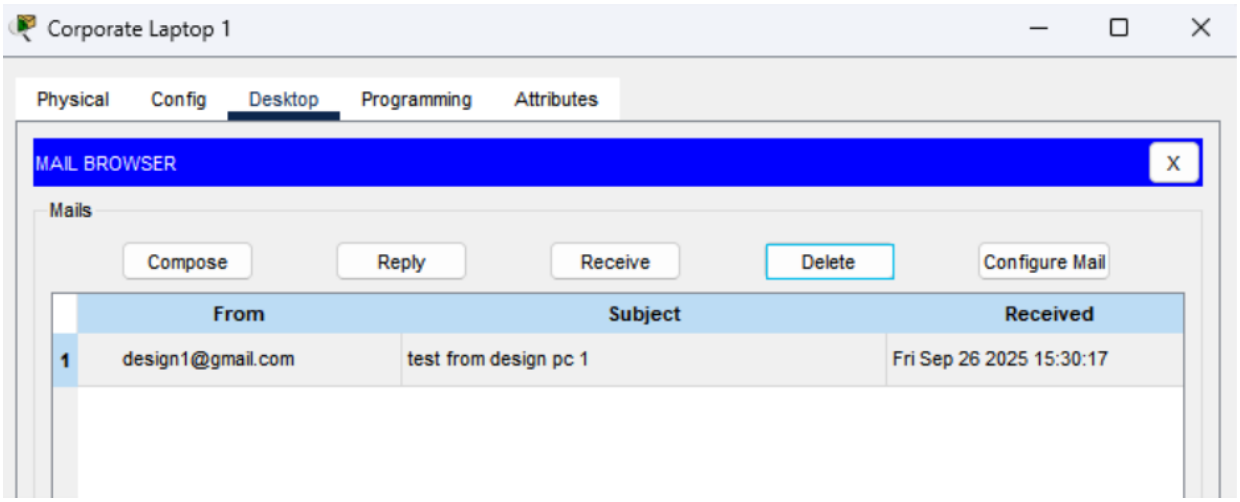
Web
Access via browser:

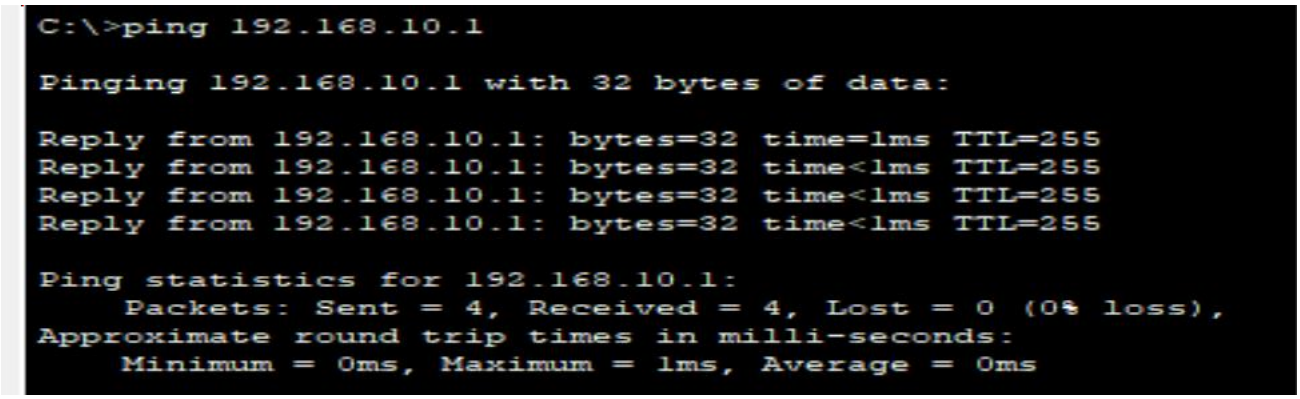
http://<server-IP>

Email
Verified send/receive between test accounts.


Corporate Laptop 1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
https://web.local/
Go
Stop
Wan tech project


Design Laptop 1
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
X
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
design1@gmail.com
test from design pc 1
Fri Sep 26 2025 15:29:39


Corporate Laptop 1
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
X
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
design1@gmail.com
test from design pc 1
Fri Sep 26 2025 15:30:17



Ping Test: I used the ping command to test connectivity between devices. A successful ping confirms that IP addressing, routing, and interfaces are configured correctly. I also pinged hostnames like *web.local* to verify that DNS resolution was working.

Edge and External Network Connectivity

An edge router was implemented to provide controlled access between the internal enterprise network and the external internet. This router forms the boundary between trusted internal resources and the untrusted outside network, represented in the topology by a cloud device.

1. Edge Router Role

The edge router serves as the gateway from the internal network to the external environment. Its primary purposes include:

- Routing traffic between internal routers and the internet
- Providing a controlled exit point
- Supporting future security configurations (NAT, ACLs, firewalls, etc.)
- Ensuring that external connectivity is separate from core routing functions

It connects directly to the core router for simplified management.

2. Physical Connections

The connection path is as follows:

Internal LAN/Departments → Core Router → Edge Router → Cloud (Internet)

Cabling and Interfaces

- **Core Router to Edge Router:**
    - Copper straight-through cable
    - Interfaces: Fa0/0 → Fa0/1 (or equivalent depending on Packet Tracer device)
- **Edge Router to Cloud:**
    - Copper straight-through cable
    - Internet-facing interface (for example Fa0/0)
    - Cloud configured as an ISP gateway in Packet Tracer

3. Edge Router Configuration (Generalized)

Assign Interface IPs

Internal-facing interface:

```
interface <LAN-facing-interface>
ip address <IP> <mask>
no shutdown
```

External-facing interface (to cloud/ISP):

```
interface <WAN-facing-interface>
ip address <public-or-simulated-IP> <mask>
no shutdown
```

Default Route

A default route is typically configured to forward all non-local traffic to the ISP:

```
ip route 0.0.0.0 0.0.0.0 <Cloud/ISP-Gateway-IP>
```

Routing to Internal Network

The edge router learns internal routes either by:

- OSPF from the core router, **or**
- Static routes (depending on your design)

4. Verification

Basic connectivity tests include:

Check Interface Status

show ip interface brief

Ping Internal Network

ping <core-router-interface-IP>

Conclusion

This project resulted in a fully functional enterprise network that provides reliable connectivity across all departments. The design includes a redundant router-based WAN core, stable distribution switches, and an organized access layer for end devices. Centralized services such as DHCP, DNS, email, and web hosting were successfully implemented on a dedicated server, simplifying management and ensuring consistent network operation.

Dynamic routing through OSPF allowed efficient communication between subnets, while the edge router provided controlled access to external networks. All configurations were tested and verified, confirming proper routing, switching, DHCP functionality, and end-to-end connectivity. Overall, the network meets the goals of performance, scalability, and future expandability.

Security Policy Documentation

Organization: Clothing Brand (Machina)

Name: Treymon Dentman (Security Specialist)

Team Members: Aaron Foster, Marquis Buckley, Iguodala Christian, Jerry Edose

Date: 11/19/2025

Overview

This report outlines the design and implementation of a secure network for our Clothing Brand Business (Machina). It also explains the reasoning behind the network topology, key findings, and the main security objectives.

Purpose

The purpose of this security policy is to protect the integrity, confidentiality, and availability of the company's corporate network and its data across all departments: Corporation, Marketing, Sales, Design, Manufacturing, and Supply.

Network Structure

Internal Network

- **Router 1 – Corporation Department:** 1 switch, 1 server, 1 laptop, 1 desktop
- **Router 2 – Marketing Department:** 1 switch, 2 desktops
- **Router 3 – Sales Department:** 1 switch, 2 desktops
- **Router 4 – Design Department:** 1 laptop, 1 desktop
- **Router 5 – Manufacturing Department:** 2 laptops
- **Router 6 – Supply Department:** 2 laptops

External Network

- **Router 1 – Corporation Department:** 1 internal router, 1 internal switch, 1 external router, 1 external switch, 1 firewall, external users/browser

Security Foundation

- Restrict data access to authorized users to protect confidentiality.
- Maintain network availability by preventing disruptions or unauthorized changes.
- Protect data integrity by blocking unauthorized access or alterations.

Security Policy for Users

- Users will browse through HTTP with VPN allowed.
- Users may create shopping accounts with a username and password.
- Optional two-factor authentication will be available.
- All purchases will use safe and trusted encryption.

Security Policy for Company Employees

1. Access Control

- Each department will use a unique VLAN to isolate traffic.
- Employees must authenticate with unique credentials; passwords change every 6 months.
- Role-based access portals will be implemented. For example, Marketing cannot access Supply. Corporate is the main admin for access permissions.

2. Firewall & Router Security

- All routers require strong, encrypted console and enable passwords.
- Access Control Lists (ACLs) will restrict inter-department communication unless permitted.
- Only the Corporation Department's server will host centralized resources and backups.
- The Corporation server requires SSH for remote management. Telnet/Remote Desktop is disabled unless allowed by IT.
- Regular backups must be securely stored.
- Only authorized IT staff may have administrative privileges.
- All desktops and laptops must have updated antivirus software and host-based firewalls.
- USB storage on internal devices is restricted unless approved by IT.

Physical Security

- Networking equipment must be stored in secure areas with limited access.
- Laptops must not be left unattended in public areas.

Incident Reporting and Monitoring

- Router, server, and firewall logs will be reviewed weekly, and daily if suspicious activity occurs.
- Unauthorized access attempts must be reported immediately.

Enforcement

Employees who violate this policy may face disciplinary action, up to and including termination of employment. Anyone who tampers with or any unlawful actions will be subject to prosecution.

Policy Reviews

This policy will be reviewed every 6–12 months or after any major network update.

My Additives / Findings

During development, each department was designed as its own "router" in the topology, though they operate as VLANs. This reduces traffic and allows quick isolation if a threat actor appears in the network. Departments cannot communicate or grant admin permissions except Corporate.

For the external network, an additional line for users to shop was added, including two routers (internal and external). This required updates such as a firewall and internal/external switches. The firewall was assigned a hostname, username, and password for exclusive management.

Configuration steps included identifying the gigabit interfaces (gig 1/1 and gig 1/2), connecting them to the appropriate switches, and assigning IP addresses from the internal and external routers. Interface gig 1/1 received an internal security level of 100, and gig 1/2 was set as DMZ with a security level of 70 to allow partial trust for external traffic. The cloud (external user / browser) is what the consumers will be using to access store products which will be connected to external router (depending on their ISP).

The "no shut" command was applied to enable signal flow from the switches. A final check using "write memory" confirmed the firewall status was up and functioning.

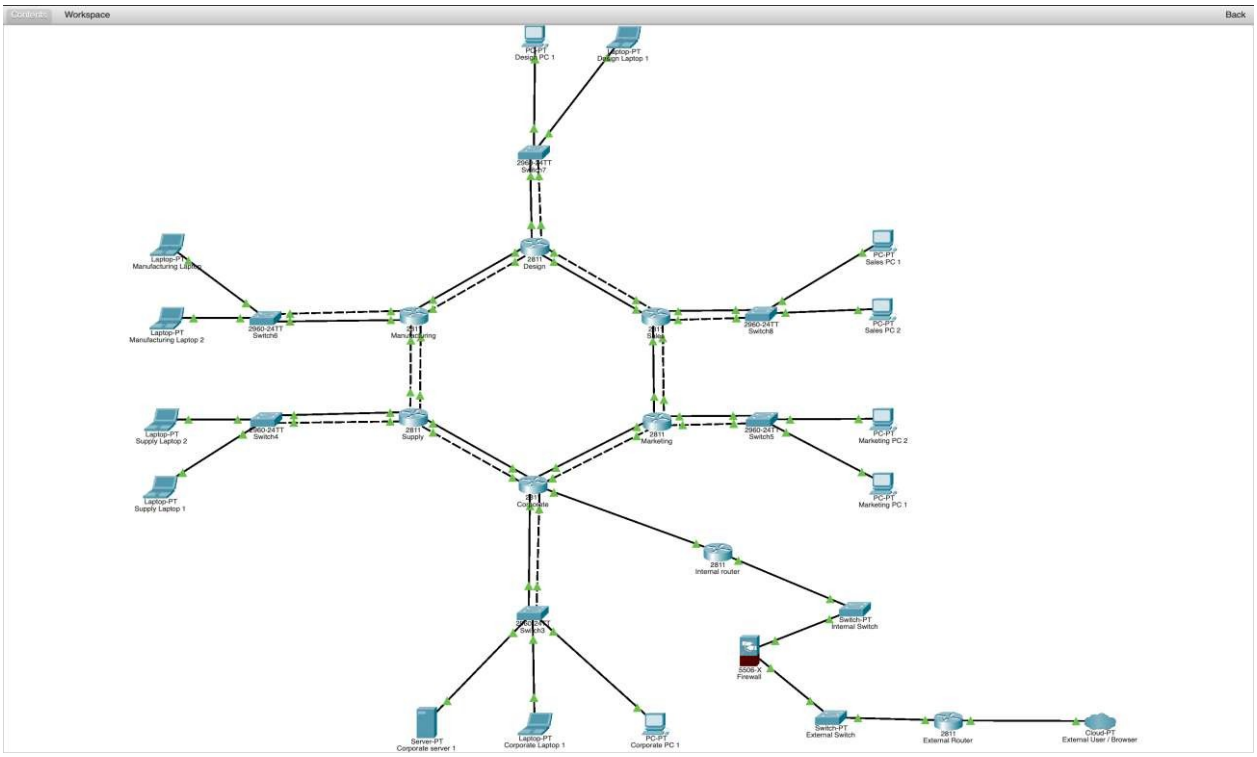
Verification and Validation

```
PERIMETER-FW(config)#
PERIMETER-FW(config)#
PERIMETER-FW(config)#write memory
Building configuration...
Cryptochecksum: 230844a2 7290008b 6d9b5ec2 5ea03836

1191  bytes copied in 1.402 secs (849 bytes/sec)
[OK]
PERIMETER-FW(config)#
```

```
PERIMETER-FW(config)#username ZeroDayTre password ZeroDayTre
PERIMETER-FW(config)#sh Start
: Saved
: Written by enable_15 at 12:18:29 UTC Nov 19 2025
: Call-home enabled from prompt by enable_15 at 12:18:29 UTC Nov 19 2025
!
hostname PERIMETER-FW
names
!
interface GigabitEthernet1/1
 nameif INSIDE
 security-level 100
 ip address 10.0.13.1 255.255.255.252
!
interface GigabitEthernet1/2
 nameif DMZ
 security-level 70
 ip address 10.0.13.2 255.255.255.252
!
interface GigabitEthernet1/3
 no nameif
 no security-level
 no ip address
 shutdown
<--- More --->
```

Copy Paste



WAN Project – Automated Provisioning & QA Test Report

Prepared by: Iguodala Christian

Role: Quality Assurance (Originally)

Swapped to Automation Admin

Test Plan Creator: Iguodala Christian

> **Additional Note:** Iguodala Christian swapped roles with Jerry Edose, who became Automation Admin.

Automated Provisioning

1. Standardized Templates for All Routers and Switches

We created standardized configuration templates to automate provisioning. These templates ensured consistency in naming, interface layout, IP addressing, and OSPF configuration. Using one template per router and switch significantly reduced deployment time and minimized human error.

Router Template Example

```
hostname <DEVICE_NAME>
no ip domain-lookup
service password-encryption

interface g0/0
  description Link to <NEIGHBOR>
  ip address <IP> <MASK>
  no shut

interface g0/1
  description Department LAN
  ip address <DEPT_GW> <MASK>
  no shut

router ospf 10
  router-id <ROUTER_ID>
  network <NETWORK> <WILDCARD> area 0

line vty 0 4
  login local
  transport input ssh
```

Switch Template Example

```
hostname <SWITCH_NAME>

vlan 10
  name Manufacturing
vlan 20
  name Design
vlan 30
  name Sales
```

3. Automated Routing Using OSPF

OSPF automated the routing process between all routers in the topology. Each router advertised its local networks, enabling automatic and dynamic route generation.

OSPF Example – Sales Router

```
router ospf 10
  router-id 3.3.3.3
  network 10.30.1.0 0.0.0.255 area 0
  network 172.16.12.0 0.0.0.3 area 0
  network 172.16.14.0 0.0.0.3 area 0
```

4. DNS Configuration for Hostname Resolution

DNS was configured so endpoints could access resources by hostname rather than by IP address. DNS server was placed in the Corporate (Green) segment and integrated with DHCP.

DNS Zone Example

```
company.local.
   manufacturing-laptop1        A    10.10.1.15

   sales-pc2                    A    10.30.1.12

   marketing-pc1                A    10.40.1.14

   corp-server                  A    10.10.0.50

   external-router              A    203.0.113.1
```

Quality Assurance Test Plan

1. Introduction

This test plan ensures the WAN infrastructure supports business operations across all departments with reliability, security, and performance.

2. Objectives

- Verify end-to-end connectivity.

Ensure redundancy and routing failover.

- Validate access control.
- Confirm printers, servers, and IP phones operate correctly.

3. Scope

Includes routers, switches, endpoints, VLANs, routing, and security.

4. Test Environment

Cisco Packet Tracer or physical lab. Routers, switches, servers, printers, PCs.

5. Test Cases

Connectivity, redundancy, performance, security, application tests, and user acceptance.

6. Acceptance Criteria

100% authorized reachability, <30 sec failover, <100ms latency.

7. Deliverables

Test logs, defect report, final QA sign-off.

8. Risks

Routing loops, single-point-of-failure switches, ACL errors.

Automated Provisioning Plan

Enterprise Hub Network Infrastructure

Prepared by: Jerry Edose

Role: Automation Admin (Originally)

Swapped to Quality Assurance

Team: Alpha Team

Date: October 2025

> **Role Note:** Jerry Edose originally served as Automation Admin and created this Automated Provisioning Plan before swapping roles with Iguodala Christian to become Quality Assurance.

1. Executive Summary

This plan automates the provisioning of a secure, segmented cloud network reflecting the provided enterprise topology. Each department is mapped to a subnet with Transit Gateway hub-and-spoke routing, hybrid VPN connectivity, and guardrails.

2. Objectives

- Provision VPC and departmental subnets with Transit Gateway in <30 minutes.
- Ensure >95% idempotent Terraform applies.
- Enforce policy-as-code with tagging and encryption standards.
- Enable hybrid Site-to-Site VPN for printers and legacy servers.

3. Scope

In-Scope Components

In-scope components include AWS VPC, subnets, TGW, route tables, IAM roles, EC2 base images, monitoring, logging, and KMS encryption.

> **Key Infrastructure Elements:**
>
> - AWS VPC and departmental subnets
> - Transit Gateway (TGW) configuration
> - Route tables and routing policies
> - IAM roles and permissions
> - EC2 base images
> - Monitoring and logging systems
> - KMS encryption implementation

Out-of-Scope Items

Out-of-scope items include application deployment, data migration, and on-premises printer configuration.

4. Security & Compliance

Security is ensured through IAM least privilege, private subnets, NAT gateways, encryption at rest and in transit, and auditing via CloudTrail and Config. Compliance is enforced by mandatory tagging and OPA checks.

> **Security Measures:**
>
> - **IAM Least Privilege:** Minimal permissions assigned to roles and users
> - **Private Subnets:** Critical resources isolated from public internet
> - **NAT Gateways:** Secure outbound internet access for private resources
> - **Encryption:** Data protected at rest and in transit using KMS
> - **Auditing:** CloudTrail and Config monitoring all infrastructure changes
> - **Compliance:** Mandatory tagging and Open Policy Agent (OPA) checks

5. Change Management

All infrastructure changes follow GitOps workflows: feature branches → PR → plan review → approval → apply. Rollback strategy is forward-fix or controlled resource replacement, with logs and state backups retained.

> **GitOps Workflow:**
>
> 1. Create feature branch for infrastructure changes
> 2. Submit Pull Request (PR) for review
> 3. Review Terraform plan output
> 4. Obtain approval from authorized team members
> 5. Apply changes to infrastructure
>
> **Rollback Strategy:** Forward-fix or controlled resource replacement with comprehensive logs and state backups retained for audit and recovery purposes.

IP Addressing Plan

Created by: Marquis Buckley

Course: CS 351

Device	Router ID	Interfaces	IP Address	Subnet Mask	Wild card Mask
Corporate Router	1.1.1.1	Fa0/0	10.0.0.1	255.255.255.252	0.0.0.3
		Fa0/1	10.0.5.2	255.255.255.252	0.0.0.3
		Eth1/2	192.168.10.1	255.255.255.0	0.0.0.255
		Eth1/0	10.0.6.1	255.255.255.252	0.0.0.3
		Eth1/1	10.0.11.2	255.255.255.252	0.0.0.3
		Eth1/3	10.0.13.2	255.255.255.252	0.0.0.3
Corporate Laptop		Fa0/3	DHCP	255.255.255.0	n/a
Corporate PC		Fa0/4	DHCP	255.255.255.0	n/a
Server 1		Fa0/2	192.168.10.100	255.255.255.0	n/a
Supply Router	2.2.2.2	Fa0/1	10.0.0.2	255.255.255.252	0.0.0.3
		Fa0/0	10.0.1.1	255.255.255.252	0.0.0.3
		Eth1/2	192.168.20.1	255.255.255.0	0.0.0.255
		Eth1/1	10.0.6.2	255.255.255.252	0.0.0.3
		Eth1/0	10.0.8.1	255.255.255.252	0.0.0.3
SupplyLaptop 1		Fa0/2	DHCP	255.255.255.0	n/a
SupplyLaptop 2		Fa0/ 3	DHCP	255.255.255.0	n/a
Manufacture Router	3.3.3.3	Fa0/1	10.0.1.2	255.255.255.252	0.0.0.3
		Fa0/0	10.0.2.1	255.255.255.252	0.0.0.3
		Eth1/2	192.168.60.1	255.255.255.0	0.0.0.255
		Eth1/1	10.0.8.2	255.255.255.252	0.0.0.3
		Eth1/0	10.0.9.1	255.255.255.252	0.0.0.3
Manufacturing Laptop 1		Fa0/2	DHCP	255.255.255.0	n/a
Manufacturing Laptop 2		Fa0/ 3	DHCP	255.255.255.0	n/a

Network I.D	DNS	Default Gateway	Emails	Passworrd
10.0.0.0/30	n/a	n/a	corporate1@gmail.com	0.0.0.0
10.0.5.0/30	n/a	n/a	corporate2@gmail.com	0.0.0.0
10.0.5.0/30	n/a	n/a		
10.0.6.0/30				
10.0.11.0/30				
10.0.13.0/30				
n/a	DHCP	192.168.10.1		
n/a	DHCP	192.168.10.1		
n/a	192.168.10.100	192.168.10.1		
10.0.0.0/30	n/a	n/a	Supply1@gmail.com	0.0.0.0
10.0.1.0/30	n/a	n/a	Supply2@gmail.com	0.0.0.0
192.168.20.0/24	n/a	n/a		
10.0.6.0/30				
10.0.8.0/30				
n/a	DHCP	192.168.20.1		
n/a	DHCP	192.168.20.1		
10.0.1.0/30	n/a	n/a	Manufacture1@gmail.com	0.0.0.0
10.0.2.0/30	n/a	n/a	Manufacture2@gmail.com	0.0.0.0
192.168.60.0/24	n/a	n/a		
10.0.8.0/30				
10.0.9.0/30				
n/a	DHCP	192.168.60.1		
n/a	DHCP	192.168.60.1		

Test Website					
http://web.local/about.html					
http://web.local/index.html					

Design Router	4.4.4.4	Fa0/1	10.0.2.2	255.255.255.252	0.0.0.3
		Fa0/0	10.0.3.1	255.255.255.252	0.0.0.3
		Eth1/2	192.168.40.1	255.255.255.0	0.0.0.255
		Eth1/1	10.0.9.2	255.255.255.252	0.0.0.3
		Eth1/0	10.0.10.1	255.255.255.252	0.0.0.3
Design PC		Fa0/ 2	DHCP	255.255.255.0	n/a
Design Laptop 1		Fa0/ 3	DHCP	255.255.255.0	n/a
Sales Router	5.5.5.5	Fa0/1	10.0.3.2	255.255.255.252	0.0.0.3
		Fa0/0	10.0.4.1	255.255.255.252	0.0.0.3
		Eth1/2	192.168.50.1	255.255.255.0	0.0.0.255
		Eth1/1	10.0.10.2	255.255.255.252	0.0.0.3
		Eth1/0	10.0.7.1	255.255.255.252	0.0.0.3
Sales PC 1		Fa0/2	DHCP	255.255.255.0	n/a
Sales PC 2		Fa0/3	DHCP	255.255.255.0	n/a
Marketing router	6.6.6.6	Fa0/0	10.0.4.2	255.255.255.252	0.0.0.3
		Fa0/1	10.0.5.1	255.255.255.252	0.0.0.3
		Eth1/2	192.168.30.1	255.255.255.0	0.0.0.255
		Eth1/1	10.0.7.2	255.255.255.252	0.0.0.3
		Eth1/0	10.0.11.1	255.255.255.252	0.0.0.3
Marketing PC 1		Fa0/2	DHCP	255.255.255.0	n/a
Marketing PC 2		Fa0/3	DHCP	255.255.255.0	n/a
Internal Router		Fa0/0	10.0.13.1	255.255.255.252	0.0.0.3

10.0.2.0/30	n/a	n/a	Design1@gmail.com	0.0.0.0
10.0.3.0/30	n/a	n/a	Design2@gmail.com	0.0.0.0
192.168.40.0/24	n/a	n/a		
10.0.9.0/30				
10.0.10.0/30				
n/a	DHCP	192.168.40.1		
n/a	DHCP	192.168.40.1		
10.0.3.0/30	n/a	n/a	Sales1@gmail.com	0.0.0.0
10.0.4.0/30	n/a	n/a	Sales2@gmail.com	0.0.0.0
192.168.50.0/24	n/a	n/a		
10.0.10.0/30				
10.0.7.0/30				
n/a	DHCP	192.168.50.1		
n/a	DHCP	192.168.50.1		
10.0.4.0/30	n/a	n/a	Marketing 1@gmail.com	0.0.0.0
10.0.5.0/30	n/a	n/a	Marketing 2@gmail.com	0.0.0.0
192.168.30.0/24	n/a	n/a		
10.0.7.0/30				
10.0.11.0/30				
n/a	DHCP	192.168.30.1		
n/a	DHCP	192.168.30.1		
10.0.13.0/30				

		Fa0/1	10.0.14.1	255.255.255.252	0.0.0.3
External Router		Fa0/0	10.0.13.2	255.255.255.252	0.0.0.3
		Fa0/1	10.0.20.1	255.255.255.252	0.0.0.3
Firewall		Gig1/1	10.0.13.1	255.255.255.252	0.0.0.3
		Gig1/2	10.0.13.2	255.255.255.252	0.0.0.3

10.0.14.0/30				
10.0.13.0/30				
10.0.20.0/30				
10.0.13.0/30				
10.0.13.0/30				