Alpha Team Consulting

Course: WAN Tech - CS 351
Instructor: Prof. Roby
Document Date: Sept. 23, 2025
Project Client: Machina
Team Members: Aaron Foster, Iguodala Christian, Jerry Edose, Marquis Buckley, Treymon Dentman
Version Number: v.1
Prepared By: Aaron Foster
Document Status: Draft

Project Title

Designing a Secure and Scalable Network for a Clothing Company Specializing in Hiking Gear and Military Contracts for Combat Gear.

Project Overview

Machina is a performance apparel company serving outdoor consumers and government clients. This project designs a secure, scalable enterprise WAN (Wide Area Network) connecting HQ, a manufacturing/warehouse site, and retail/e-commerce locations. Deliverables include logical and physical network topology, IP plan, routing, security, QoS, and DR/BCP aligned with WAN best practices.

Project Goals

1. **Establish Reliable Connectivity: We shall provide a secure and stable WAN that interconnects headquarters, manufacturing facilities, warehouses, and retail locations, ensuring real-time and accurate information flow across all sites.**
2. **Operational Continuity: Our goal is to support critical business operations by enabling seamless access to design resources, Enterprise Resource Planning (ERP) systems, point-of-sale (POS) terminals, and supply chain applications without interruption.**
3. **Data Protection: We will safeguard sensitive government contracts and customer information through robust encryption, network segmentation, firewalls, and strict access control policies.**
4. **Scalable Architecture: We plan to implement an IP addressing scheme and network design that can easily scale to accommodate additional retail stores, warehouses, or remote offices as the company expands.**
5. **Improve Performance: We will use QoS to prioritize critical traffic such as POS transactions, VoIP, and ERP data over guest or best-effort traffic.**

6. **Resilient Infrastructure: We shall build redundancy into WAN links, routing paths, and network devices to minimize downtime and maintain business continuity during hardware failures, link outages, or other disruptions.**
7. **Centralized Management: We plan to enable centralized monitoring and configuration management with logging, flow analysis, and standardized router/switch provisioning to improve operational efficiency.**
8. **Disaster Recovery & Continuity: We will develop a disaster recovery framework to ensure the company can maintain operations or quickly restore services in the event of network outages, cyberattacks, or natural disasters.**

Company Structure (6 cores)

- **Design & Product Development**
- **Production / Manufacturing**
- **Supply Chain & Logistics**
- **Sales & Retail (E-commerce + Stores)**
- **Marketing & PR**
- **Corporate (Executive, Finance, HR, IT)**

Sites & Roles (Scope)

Headquarters / Data Center – Austin, TX

- **Centralized hub for corporate router and design router**
- **Hosts core servers (database, DNS, DHCP, backup)**

Manufacturing Facility – Fort Worth, TX

- **Primary production site for outdoor and military gear.**
- **Houses production systems, quality control, and secure R&D operations.**

Warehouse / Logistics Center – Dallas, TX

- **Manages inventory, distribution, and supply chain systems.**
- **Coordinates shipping to both retail stores and government contracts.**

Retail Store 1 – Houston, TX

- **Customer-facing retail location with POS systems and customer Wi-Fi.**
- **Reports sales and inventory back to HQ in real time.**

Retail Store 2 – Denver, CO

- **High-traffic outdoor gear market near the Rockies and other Mountain Terrain**
- **Provides POS services, connects securely to HQ for sales/inventory sync.**

Marketing & PR Department – Los Angeles, CA

- **Focused on digital campaigns, branding, and influencer partnerships.**
- **Requires high-speed access to HQ servers and cloud platforms.**

Deliverables Mapping

- **Project Overview – Defines company scope, goals, and WAN objectives.**
- **Network Topology – Logical and physical Packet Tracer designs showing site interconnections.**
- **IP & Security Plan – Subnetting scheme, VLAN segmentation, and access policies.**
- **Testing & Automation – Connectivity validation and router provisioning scripts/configs.**
- **Disaster Recovery Plan – Step-by-step recovery for outages and data continuity.**

Machina WAN Disaster Recovery Plan (DRP)

1. Purpose

The Disaster Recovery Plan at Machina exists to enable quick recovery of essential network services which will support ongoing business operations during system failures and cyberattacks and natural disasters and site outages. The plan establishes full network connectivity through WAN connections which maintains accurate data and continuous operations between all sites.

2. Disaster Recovery Site

- **Primary DR Site: Dallas, TX (Warehouse & Logistics Center)**
- **Function: Serves as the company's disaster recovery hub and secondary data center.**
- **Resources Hosted: Backup servers, replicated databases, DHCP/DNS redundancy, and failover routing for WAN connections.**
- **Additional Backup: Essential configurations and router files and ERP data will be stored in encrypted cloud storage.**

3. Recovery Objectives

System / Function	RTO (Max Downtime)	RPO (Max Data Loss)	Priority
ERP / Supply Chain System	4 hours	1 hour	High
Point-of-Sale (POS) Systems	2 hours	30 minutes	High
Email & Collaboration	8 hours	2 hours	Medium
DNS / DHCP / Authentication	1 hour	15 minutes	Critical
Web & E-Commerce Services	6 hours	2 hours	High
Design File Storage	6 hours	2 hours	Medium

4. Recovery Strategy

- **Data Replication: The system maintains continuous synchronization of ERP and POS and authentication data between the Austin HQ location and the Dallas DR site.**

- **Backup Rotation: The system performs nightly local backups at HQ while it runs weekly full replication to Dallas and monthly encrypted offsite/cloud backup.**

- **Network Failover: SD-WAN tunnels will redirect all traffic to the DR site when HQ experiences a failure. The network creates new paths through static routes and OSPF adjacencies which become active within a few minutes.**

- **Power & Hardware Redundancy: The DR site maintains critical devices in hot standby mode through its backup systems which include UPS and generator power supply.**

5. Failover Procedure

1. **Incident Detection: NOC alerts the IT Manager of a service outage or breach.**
2. **Disaster Declaration: The IT Manager and Executive Team confirm severity and initiate DR procedures.**
3. **Network Rerouting:**
    - **WAN traffic is redirected from HQ to the Dallas DR site.**
    - **Redundant DNS and DHCP servers assume control.**
4. **Data Recovery:**
    - **Replicated ERP and database services activated at the DR site.**
    - **Authentication and VPN services reinitialized for remote access.**
5. **Validation: Network engineers verify routing, connectivity, and service integrity.**
6. **Communication: Executive leadership informs employees, partners, and government clients.**

6. Restoration & Return to Normal Operations

- **Once HQ systems are stable, data and configurations from the DR site are synchronized back to HQ.**
- **Network routes revert to normal traffic paths through Austin.**
- **Validation checks are performed for data consistency, user access, and application uptime.**
- **Final incident report is documented for process improvement.**

7. Roles & Responsibilities

Role	Responsibility
IT Manager	Declare disaster, oversee recovery, communicate with executives.
Network Engineers	Restore WAN connectivity and routing.
Server Administrators	Activate and sync DR systems (ERP, DNS, authentication).
Security Officer	Ensure data integrity and enforce access policies.
Executive Leadership	Approve DR actions and manage external communications.

8. Testing & Maintenance

- **Conduct quarterly failover tests to ensure readiness.**
- **Perform annual full-scale DR simulation involving all departments.**
- **Review and update the plan after:**
  - **Major network changes.**
  - **Addition of new sites or systems.**
  - **Lessons learned from real incidents or drills.**

9. Success Criteria

- **Critical services restored within RTO/RPO targets.**
- **WAN connectivity maintained for all remote sites.**
- **No data corruption or security breaches post-recovery.**
- **Clear communication and documentation of all recovery steps.**