Faculty of Engineering and Technology (FET)

Sri Sri University

Cuttack Odisha India Pin-754006

B.Tech in CSE - CSCD Project Report

Project Title: Manufacturing Plant Network

Group Number: 03

Department: FET

Guided by: Dr. Chinmaya Kumar Nayak & Ms. Neha Bagle

Submitted by:

- Amal Antony Alex (FET-BCD-2023-27-020)
- Swosti Sanhita Jena (FET-BCD-2023-27-022)
- Chidananda Sashank Bhuyan (FET-BCD-2023-27-025)
- Chiranjibi Dash (FET-BCD-2023-27-026)

Certificate of the Guide

This is to certify that the project titled "Manufacturing Plant Network" submitted by the following students:

- Amal Antony Alex (FET-BCD-2023-27-020)

- Swosti Sanhita Jena (FET-BCD-2023-27-022)

- Chidananda Sashank Bhuyan (FET-BCD-2023-27-025)

- Chiranjibi Dash (FET-BCD-2023-27-026)

of the **Faculty of Engineering and Technology** has been carried out under my guidance in partial fulfillment of the requirements for the award of the degree.

To the best of my knowledge, this work has not been submitted to any other university or institution for the award of any degree or diploma.

Guided by:

Dr. Chinmaya Kumar Nayak - Associate Professor

Ms. Neha Bagle - Cyber Security Engineer and Trainer

Institution: Sri Sri University

(Signature)

Student Declaration

We hereby declare that the project work entitled "Manufacturing Plant Network" submitted to Faculty of Engineering and Technology, Sri Sri University Cuttack Odisha, is a record of original work carried out by us under the guidance of Dr. Chinmaya Kumar Nayak & Ms. Neha Bagle.

This work has not been submitted anywhere else for any other degree or diploma.

- Amal Antony Alex (FET-BCD-2023-27-020)
- Swosti Sanhita Jena (FET-BCD-2023-27-022)
- Chidananda Sashank Bhuyan (FET-BCD-2023-27-025)
- Chiranjibi Dash (FET-BCD-2023-27-026)

Date: 12/04/2025
Place: Sri Sri University, Cuttack

Acknowledgement

We would like to express our sincere gratitude to our project guide Dr. Chinmaya Kumar Nayak & Ms. Neha Bagle for their valuable guidance, encouragement, and continuous support throughout the course of this project.

We are also thankful to the faculty and staff of the Faculty of Engineering and Technology Sri Sri University Cuttack for their assistance and for providing the necessary facilities to carry out our work.

Our heartfelt thanks to our families and friends for their moral support and motivation during the project development.

Finally, we thank each other as a team for the hard work and collaboration that made this project a success.

Students Signatures:

1.

2.

3.

4.

Table of Contents

1. Cover Page

2. Guide Certificate

3. Student Declaration

4. Acknowledgement

5. Abstract

6. Introduction

7. Objectives & Scope

8. Problem Statement

9. Motivation

10. Literature Review

11. Proposed Solution

12. System Design

13. Technical Details

14. Implementation

15. Testing & Results

16. Cost Analysis

17. Societal & Industry Impact

18. Conclusion & Future Scope

19. References

20. Appendix (if any)

21. Code (if any)

Abstract

This report presents a comprehensive design and implementation of a secure, scalable, and high-performance network infrastructure tailored for a modern manufacturing plant. Leveraging Cisco Packet Tracer, the project adopts a hierarchical model comprising Core, Distribution, and Access layers to ensure high availability, reliability, and streamlined management. The network is segmented into critical zones including Production, Engineering, Corporate, Storage, DMZ, and Guest, with each zone supported by dedicated VLANs and subnets to ensure traffic isolation and efficient resource utilization.

To strengthen network security and resilience, the infrastructure incorporates dual Internet Service Providers (ISPs) for redundancy, firewall systems, intrusion prevention mechanisms, Access Control Lists (ACLs), port security, and strict segmentation of IoT devices, SCADA systems, and enterprise IT resources. Routing is managed using the Open Shortest Path First (OSPF) protocol, while Dynamic Host Configuration Protocol (DHCP) servers and static IP addressing facilitate seamless device management. Additional features include Secure Shell (SSH) for secure remote access and Port Address Translation (PAT) for efficient outbound traffic handling.

This report emphasizes the importance of rigorous testing and validation processes throughout the implementation phase to ensure the delivery of a robust and forward-looking network infrastructure. The outcome is a resilient and secure system architecture capable of supporting current operational demands while also positioning the facility for future technological evolution and scalability.

Introduction

In the evolving landscape of modern industrial infrastructure, a robust and scalable network system is essential for ensuring seamless communication, operational efficiency, and secure data flow across various organizational units. This project, titled *"Manufacturing Plant Network"* focuses on developing a resilient and future-ready network infrastructure tailored specifically for a manufacturing environment, encompassing critical departments such as Assembly, Quality Control (QC), Logistics, and Administration. As manufacturing plants grow in complexity and scale, the need for a unified, secure, and efficient communication backbone becomes vital. The project highlights the strategic importance of efficient network routing and switching mechanisms. It leverages Cisco Packet Tracer to simulate a real-world scenario that supports both current operations and future expansions. This project employs a hierarchical network model (Core, Distribution, and Access Layers) to ensure modularity, scalability, and redundancy. Key features include VLAN segmentation for traffic management, secure communication protocols, and Operational Technology (OT) security mechanisms to safeguard industrial control systems from cyber threats. By integrating real-time monitoring capabilities and emphasizing secure interconnectivity between departments, the design addresses the core challenges of modern manufacturing facilities. Ultimately, this initiative aims to demonstrate how tailored network architectures, when implemented thoughtfully, can significantly enhance operational workflows, ensure business continuity, and lay a strong foundation for technological growth in an industrial setting.

Objectives & Scope

Objective:

The primary objective of the project titled "Manufacturing Plant Network" is:

- Design and simulate a secure, scalable network in Cisco Packet Tracer for departments like Assembly, QC, Logistics, and Admin.

- Implement a hierarchical architecture with redundancy for high availability and easy management.

- Use VLANs and subnetting to ensure secure, isolated communication between IoT, SCADA, and enterprise systems.

- Integrate real-time monitoring and cybersecurity features like ACLs, SSH, PAT, and firewalls to safeguard OT environments.

Scope:

The scope of this project encompasses the complete design and simulation of a manufacturing plant's internal network using Cisco Packet Tracer. It includes the creation of a three-tier hierarchical topology with clearly defined Core, Distribution, and Access layers, along with redundancy to prevent single points of failure. The project will implement VLANs to segment network traffic between different departments and critical systems like SCADA and IoT devices. IP addressing, routing protocols, and wireless configurations will be set up for optimized performance and secure access. The scope also includes integrating real-time monitoring capabilities to ensure the network's reliability and responsiveness, establishing multi-ISP connectivity to ensure uninterrupted internet access, and designing the system to be future-ready for anticipated technological growth and departmental expansions.

Problem Statement

In a modern manufacturing environment, reliable and secure network infrastructure is essential for efficient operations across departments like Assembly, Quality Control, Logistics, and Administration. This project aims to design a scalable and secure network for a manufacturing plant using Cisco Packet Tracer, focusing on performance, security, and real-time responsiveness.

To achieve this, the network design must address the following:

- **Integration of Plant Units:**
  Establish seamless communication across various departments such as Assembly, Quality Control, Logistics, and Administration, ensuring smooth coordination between production lines and inventory systems.
- **Secure VLAN Segmentation:**
  Implement VLAN-based segmentation to isolate and secure network traffic between IoT devices, SCADA systems, and enterprise-level networks, minimizing security risks and improving data flow control.
- **Real-Time Monitoring and Responsiveness:**
  Enable real-time network monitoring to detect, analyse, and respond to performance issues or faults without disrupting ongoing industrial operations.
- **High Availability and Cybersecurity:**
  Ensure continuous availability of network services and apply protective measures against industrial cyber threats, especially those targeting OT (Operational Technology) systems, with redundancy and security best practices.

Motivation

In the era of Industry 4.0, modern manufacturing plants are increasingly dependent on interconnected systems to enhance efficiency, productivity, and automation. These systems, however, are becoming prime targets for cybersecurity threats, particularly within operational technology (OT) environments. The growing complexity and interconnectivity of industrial networks demand the implementation of robust and scalable network solutions to ensure both security and future growth. This project is driven by the need to understand and address the unique challenges faced by manufacturing networks. It provides a valuable opportunity to design and simulate a real-world network architecture using Cisco Packet Tracer, enabling the practical application of theoretical networking concepts. Furthermore, the project emphasizes the importance of implementing effective network security measures to protect OT systems from cyber threats, ensuring the resilience and integrity of industrial operations. By engaging in this hands-on experience, we aim to bridge the gap between classroom learning and real-world application, equipping ourselves with the skills necessary to design secure, scalable, and efficient networks tailored to the dynamic needs of modern manufacturing environments.

Literature Review

S. No.	Author(s)	Year	Title	Objective	Methodology	Key Findings	Gaps Identified
1	G. Mwansa	2024	Enhancing Practical Skills in Computer Networking: Evaluating the Unique Impact of Simulation Tools, Particularly in Cisco Packet Tracer.	This study examines the effectiveness of networking simulation tools, particularly Cisco Packet Tracer, in enhancing the learning experiences	The CIPP Evaluation Model	Simulation tools significantly improve students' practical skills understanding of theoretical concepts in computer networking	Longitudinal studies, mixed methods, and comparative studies
2	Das et al.	2023	Packet tracer for smart home networks and real-world monitoring	To demonstrate how to run IoT-based technologies using Cisco Packet Tracer, connecting IoT devices to a home portal gateway for smart home network control	Using Cisco Packet Tracer software to connect and control IoT devices in a smart home network, including solar panels and batteries	Monitor IoT devices in a smart home setting, allowing users to check device functionality	The study does not address the limitations of using a simulated environment versus real-world conditions and the scalability of such systems

Literature Review

S. No.	Author(s)	Year	Title	Objective	Methodology	Key Findings	Gaps Identified
3	Malanchini et al.	2023	Convergence of Manufacturing and Networking in Future Factories	To highlight the potential for intelligent networking and advanced ML -based solutions Industry's	The work presents a vision and framework by introducing network-aware and production-aware principles	Manufacturing-network integration enables adaptable machines and dynamic communication networks.	Challenges include addressing issues in private networks and exploring future 6G
4	Lindenschmitt et al	2023	6G Underlayer Network Concepts for Ultra Reliable and Low Latency Communication in Manufacturing	To propose underlayer network designs tailored for manufacturing environments, ensuring low latency, high reliability, and robust security.	The study introduces a network concept for underlayer networks and evaluates its application in closed-loop communication for machine tools.	Enhance flexibility and efficiency in manufacturing by integrating wireless technologies, addressing challenges like signal interference and latency.	Further research is needed to explore the practical implementation of underlayer networks in diverse manufacturing settings.

Literature Review

S. No.	Author(s)	Year	Title	Objective	Methodology	Key Findings	Gaps Identified
5	J. Allison	2022	Simulation-Based Learning via Cisco Packet Tracer to Enhance the Teaching of Computer Networks	To enhance the teaching of computer networks through simulation-based learning using Cisco Packet Tracer	Implementation of simulation-based learning in cisco packet tracer	Simulation-based learning with Cisco Packet Tracer improves the teaching of computer networks	Comparative studies are needed to evaluate the effectiveness against traditional lab methods and other simulation tools.
6	Cisco Networking Academy	2020	Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7)	To provide a comprehensive companion guide that aligns with the Cisco Networking Academy's CCNAv7 curriculum.	The book combines theory with hands-on exercises, case studies, and Packet Tracer activities.	Delivers foundational networking knowledge, including VLANs, STP, EtherChannel, IPv4 and IPv6 routing, & WLAN configurations	Lacks deeper exploration into emerging networking technologies like SDN (Software-Defined Networking).

Literature Review

S. No.	Author(s)	Year	Title	Objective	Methodology	Key Findings	Gaps Identified
7	J. F. Kurose & K. W. Ross	2020	Computer Networking: A Top-Down Approach (7th Edition)	Aims to provide a comprehensive understanding of computer networking, focusing on a top-down & lower-layer networking approach that starts with application-layer protocols	High-level networking concepts such as web applications, HTTP, and email protocols before introducing transport, network, and link-layer protocols.	A top-down approach enhances understanding by relating networking principles to real-world applications before diving into technical details.	Primarily focuses on traditional networking models and might not extensively cover the latest advancements in AI-driven networking and machine learning applications in networking.
8	D. D. Coleman & D. A. Westcott	2020	CWNA Certified Wireless Network Administrator Official Study Guide (5th Edition)	To provide a comprehensive guide for wireless networking professionals preparing for the CWNA certification.	Technical explanations of Wi-Fi standards, RF behavior, wireless security, and enterprise WLAN architecture are provided.	Proper WLAN design and security implementation with in-depth coverage of 802.11 standards and best practices.	Lacks coverage of emerging technologies like Wi-Fi 6E and 5G integration in wireless networks.

Proposed Solution

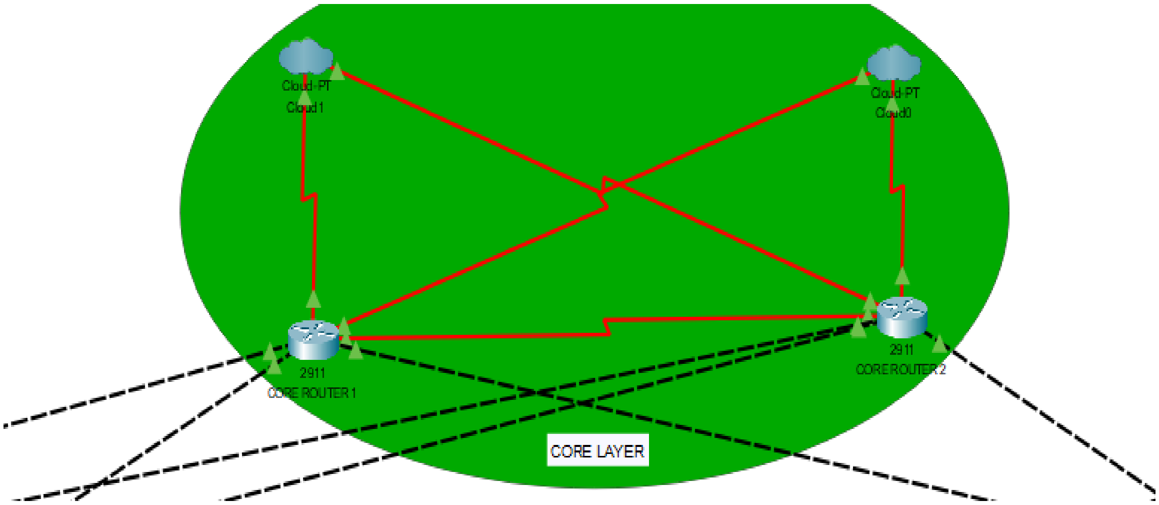
The proposed network architecture follows a robust hierarchical model, structured across three distinct layers to ensure scalability, performance, and efficient management:

- At the Core Layer, two high-performance core routers are deployed, providing redundant connectivity to external Internet Service Providers (ISPs) via the cloud.
- The Distribution Layer comprises three multilayer switches that serve as the backbone for inter-VLAN routing and policy enforcement.
- The Access Layer includes dedicated access switches and wireless access points (APs) to ensure seamless connectivity for end-user devices.
- The network is logically segmented into six functional zones: the Guest & Reception Area (2 VLANs), Production Zone (2 VLANs), Engineering Zone (2 VLANs), Corporate Zone (5 VLANs), Storage Zone (3 VLANs), and the Demilitarized Zone (DMZ) (3 VLANs).
- Each department is assigned a dedicated VLAN to enhance security and broadcast domain efficiency, with Dynamic Host Configuration Protocol (DHCP) facilitating dynamic IP assignment and static IPs reserved for critical infrastructure such as servers.
- To optimize routing and traffic flow, Open Shortest Path First (OSPF) is implemented as the dynamic routing protocol, complemented by Network Address Translation (NAT) Overload for efficient internet access using a single public IP.

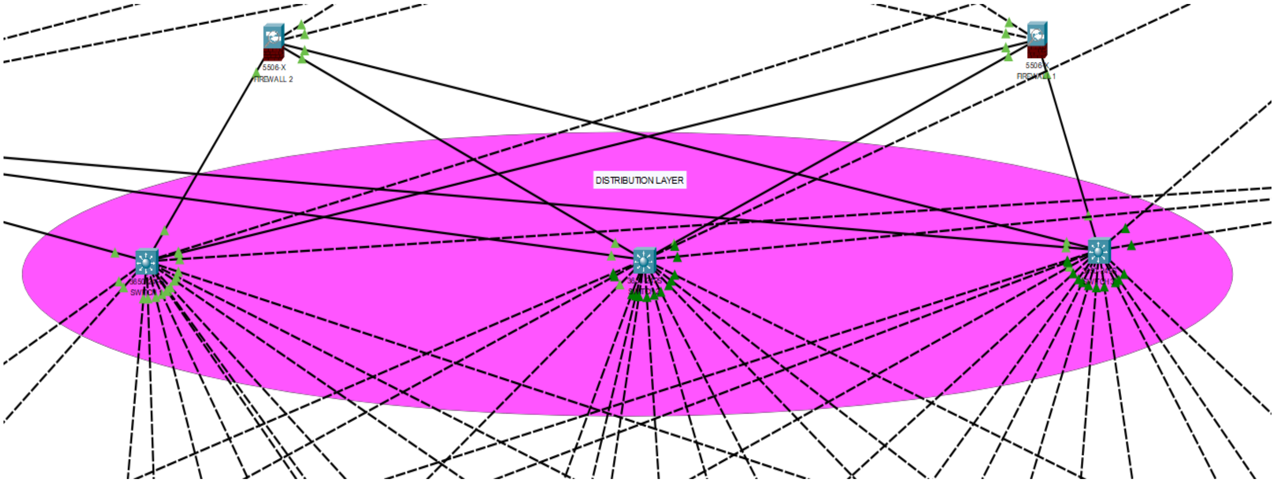
This design ensures high availability, secure segmentation, and scalable performance across the organization’s network infrastructure.

System Design

Part A: Core Layer: -

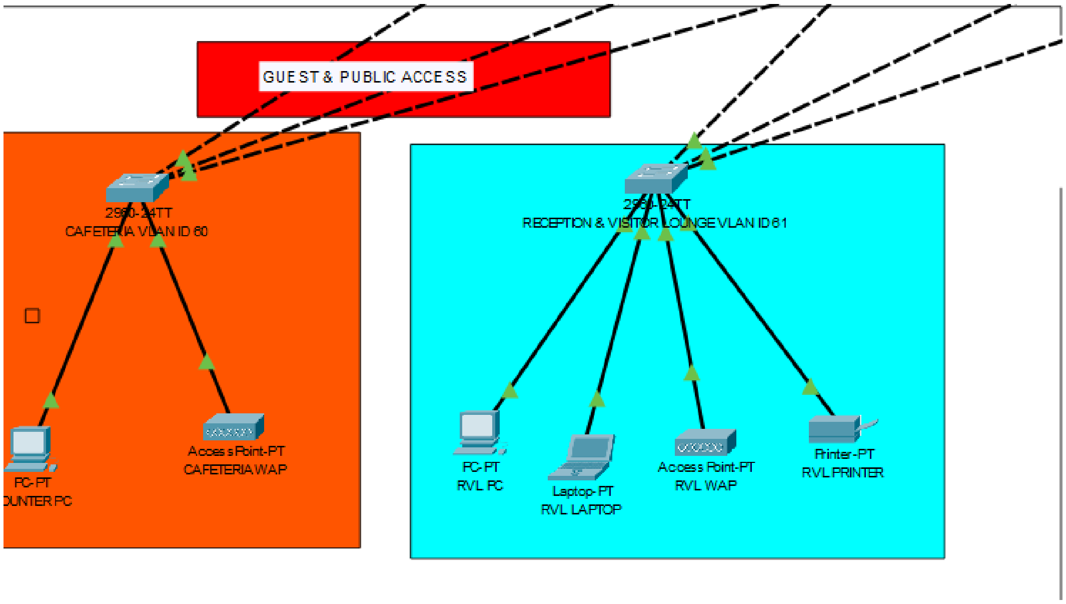


Part B: Distribution Layer: -

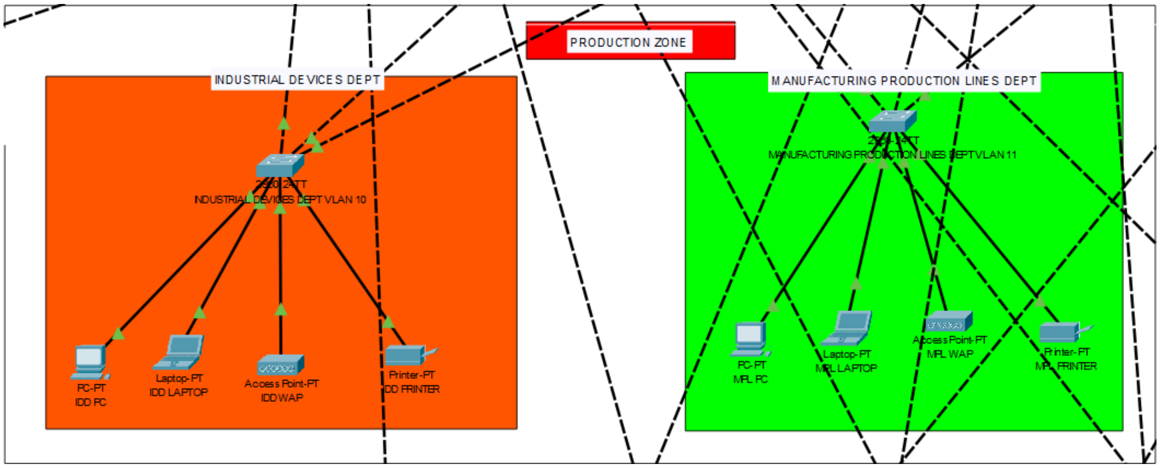


Part C: Access Layer: - The access layer is divided into 6 different zones:

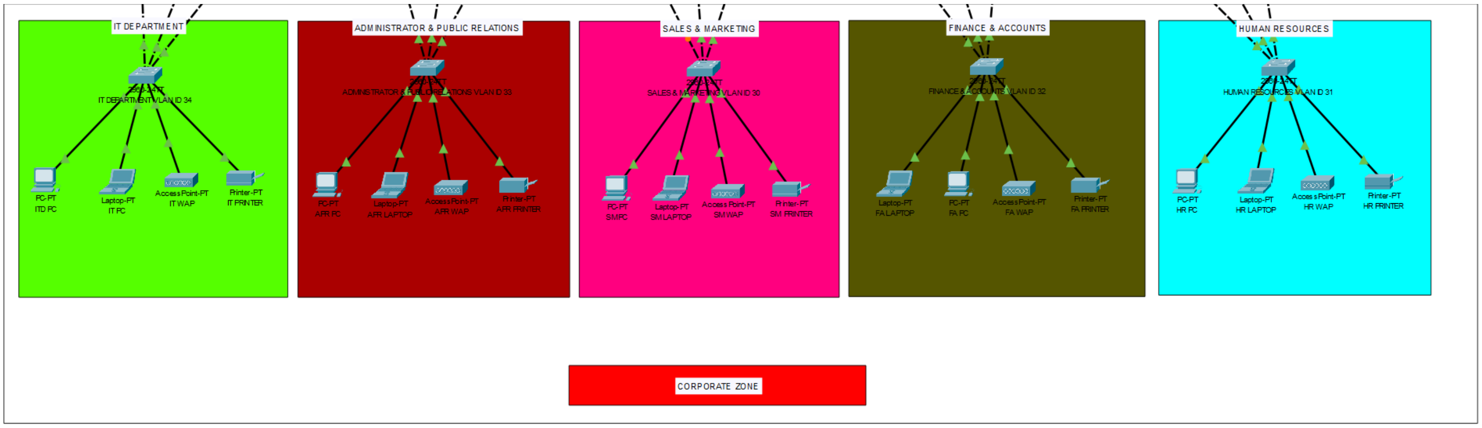
Zone 1: Guest & Public Zone:



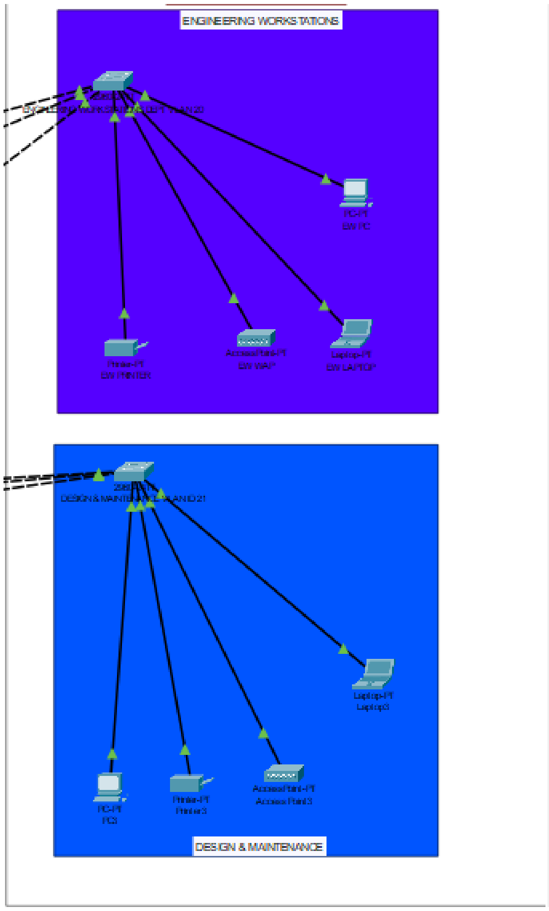
Zone 2: Production Zone:

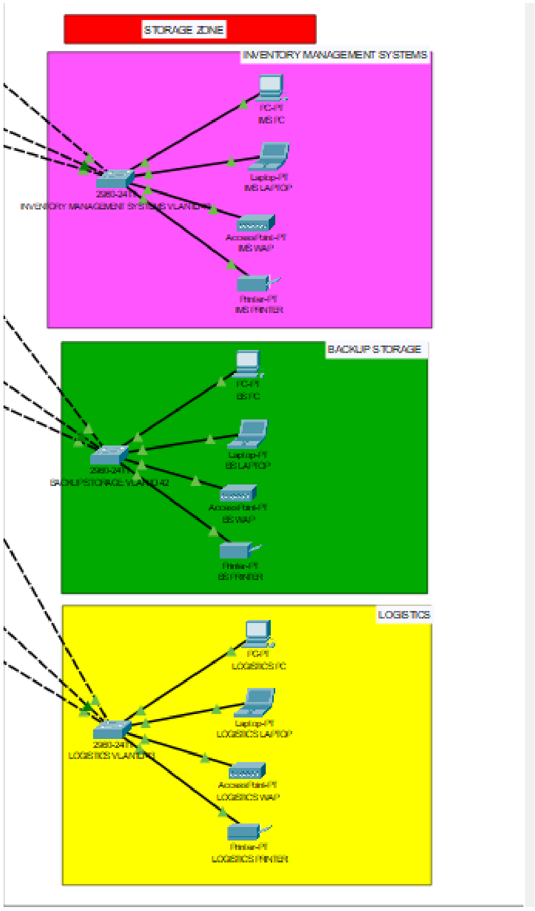


Zone 3: Corporate Zone:

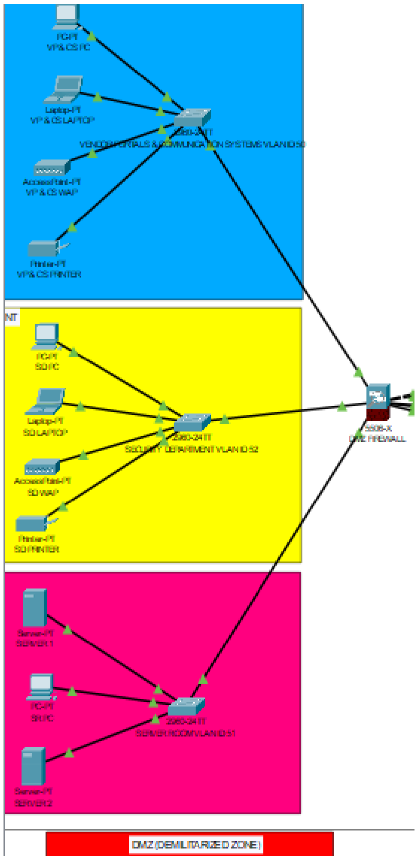


Zone 4 & 5: Engineering & Storage Zone:

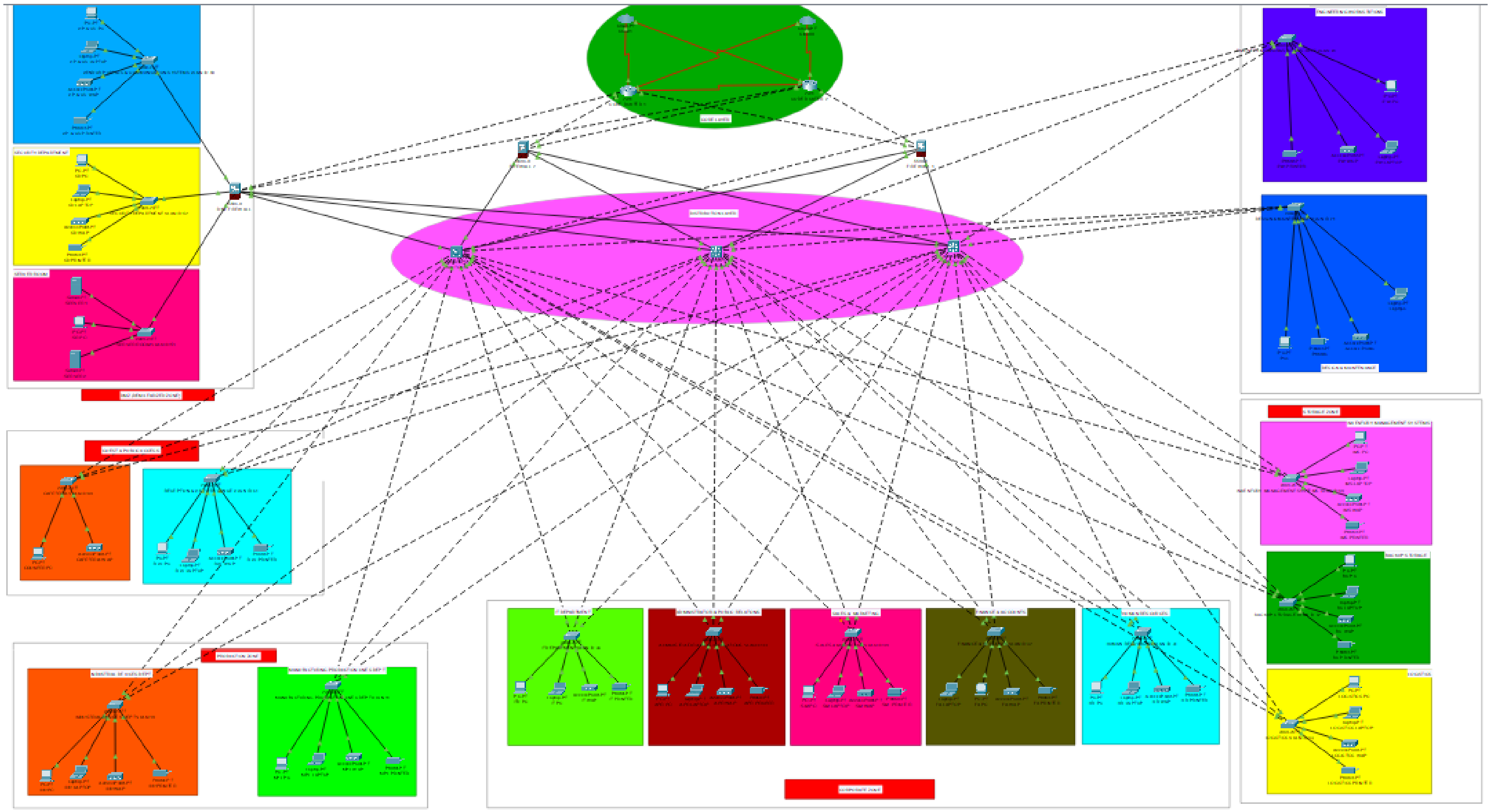




Zone 6: Demilitarized Zone (DMZ):



The Complete System Design:



Technical Details

Hardware Components Routers:

2 Cisco Series-2911 Routers – used for core routing, OSPF, and NAT configuration.

Switches: 3 Cisco Series-3650-24PS Multilayer & 17 Cisco Series-2960-IOS15 Access Switches – provide Layer 2 and Layer 3 switching and VLAN support.

Firewalls: 3 Cisco Series-5506-x – enforce security policies and inspect traffic across the network.

Servers: 2 Central Servers Series –Server-PT – configured for DHCP, monitoring, and future cloud-based healthcare services.

End Devices: PCs, printers, and IoT-enabled devices for various hospital departments.

Power Backup: Uninterruptible Power Supply (UPS) ensures 24/7 network reliability.

WAN: Ensures connectivity between zones via dedicated lines.

Software & Tools Cisco Packet Tracer:

Used for designing, simulating, and testing the network configuration.

DHCP Server: Automatically allocates dynamic IP addresses to client devices.

Routing Protocols:

OSPF (Open Shortest Path First): Used for dynamic routing between internal routers.

NAT Overload (PAT): Enables internal devices to access the internet with a single public IP.

IP Addressing Scheme Base Network:

172.168.0.0/16 – used as the private address space.

Allocated IP Range: 172.16.0.0 – 172.16.240.47 – assigned across departments and sites.

VLAN Configuration:

VLANs ranging from VLAN 10 to VLAN 60 are created for zone segmentation and separate VLAN IDs for better traffic management and security.

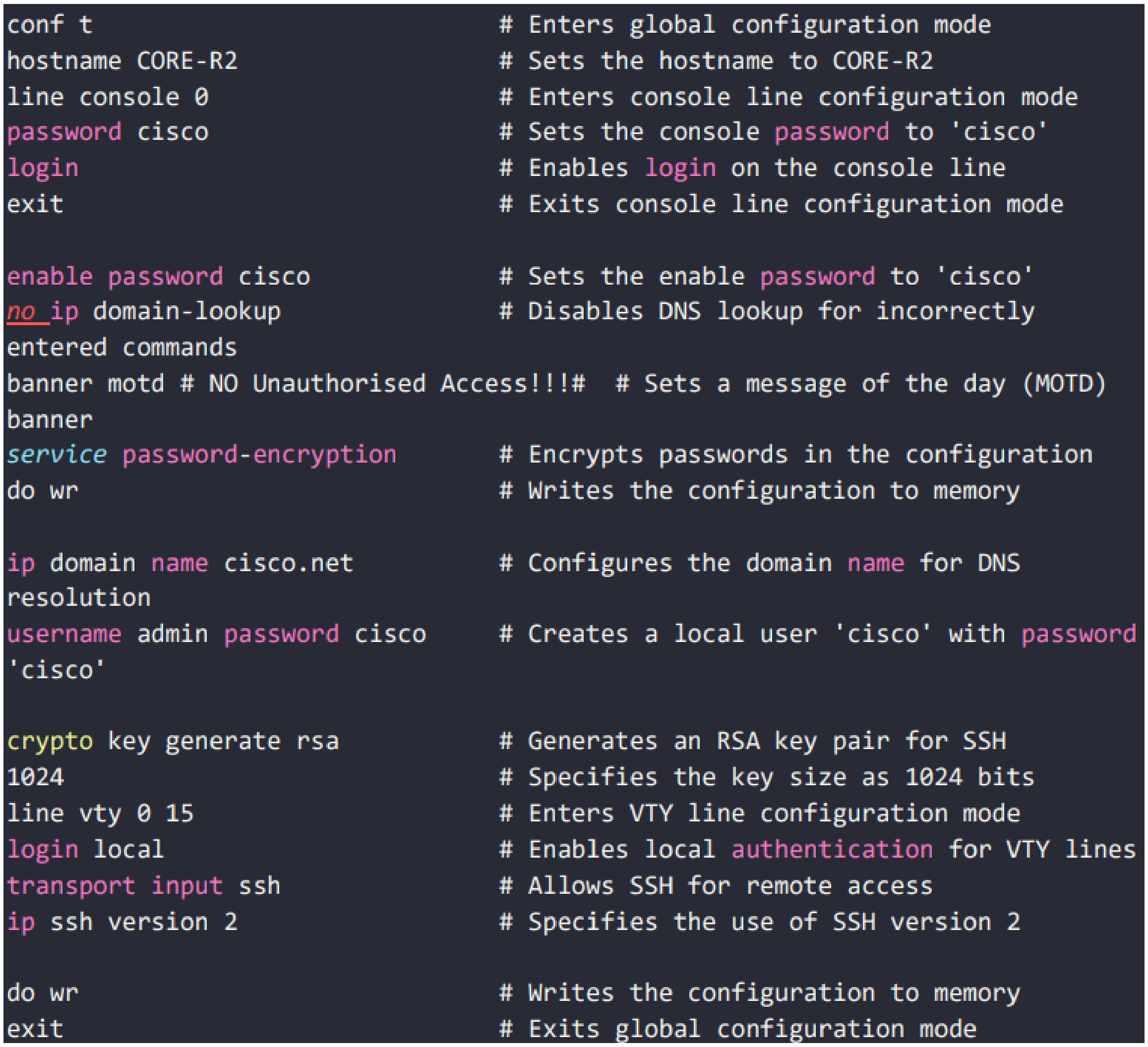
Implementation

To achieve a secure, scalable, and efficient manufacturing plant network, the following implementation were made:

Basic configuration and SSH configuration:

Basic configuration on Cisco devices involves setting the hostname, securing access with passwords, assigning IP addresses to interfaces, and saving the setup.

For secure remote access, SSH is configured by setting a domain name, creating a user, generating RSA keys, and enabling SSH on VTY lines. This ensures encrypted and secure management of the device over the network.

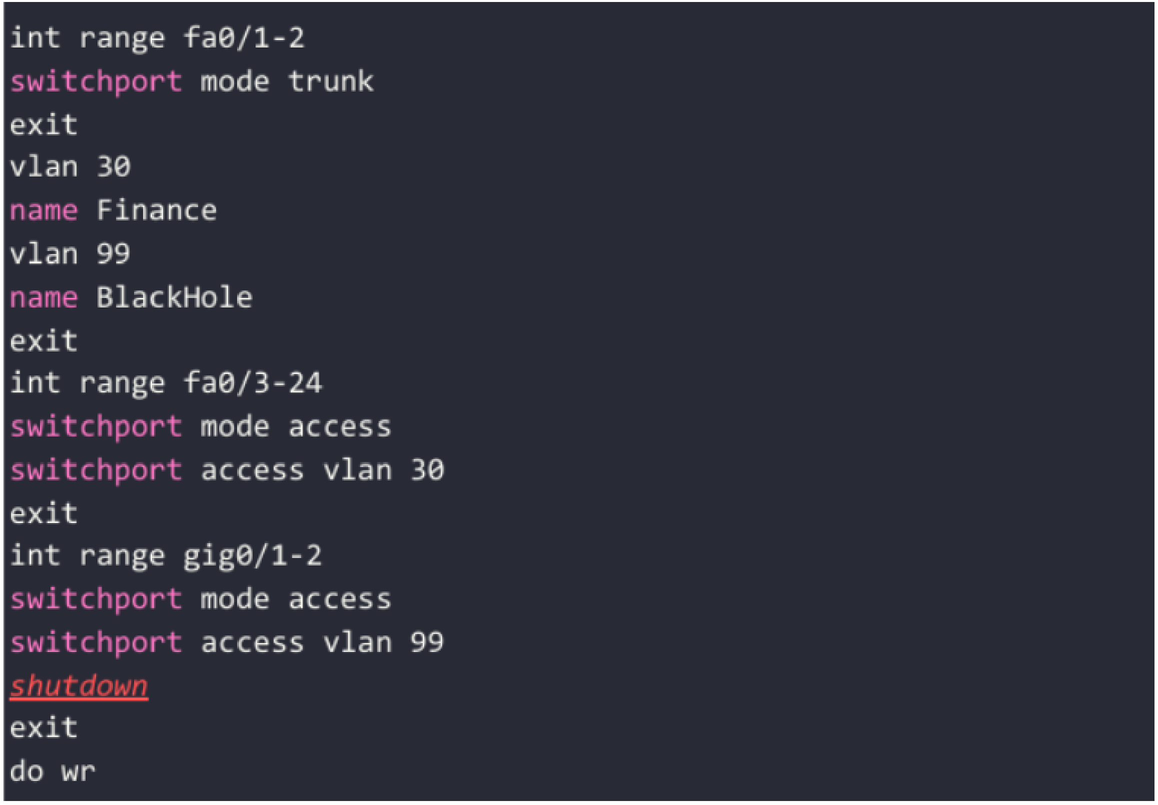


```
conf t                            # Enters global configuration mode
hostname CORE-R2                  # Sets the hostname to CORE-R2
line console 0                    # Enters console line configuration mode
password cisco                    # Sets the console password to 'cisco'
login                             # Enables login on the console line
exit                              # Exits console line configuration mode

enable password cisco             # Sets the enable password to 'cisco'
no ip domain-lookup               # Disables DNS lookup for incorrectly
entered commands
banner motd # NO Unauthorised Access!!!#  # Sets a message of the day (MOTD)
banner
service password-encryption       # Encrypts passwords in the configuration
do wr                             # Writes the configuration to memory

ip domain name cisco.net          # Configures the domain name for DNS
resolution
username admin password cisco     # Creates a local user 'cisco' with password
'cisco'

crypto key generate rsa           # Generates an RSA key pair for SSH
1024                              # Specifies the key size as 1024 bits
line vty 0 15                     # Enters VTY line configuration mode
login local                       # Enables local authentication for VTY lines
transport input ssh               # Allows SSH for remote access
ip ssh version 2                  # Specifies the use of SSH version 2

do wr                             # Writes the configuration to memory
exit                              # Exits global configuration mode
```

VLAN Segmentation and Trunking:

VLAN (Virtual Local Area Network) segmentation divides a network into multiple logical groups, improving performance, security, and traffic management. Devices in the same VLAN can communicate as if they are on the same physical network, even if they are connected to different switches.

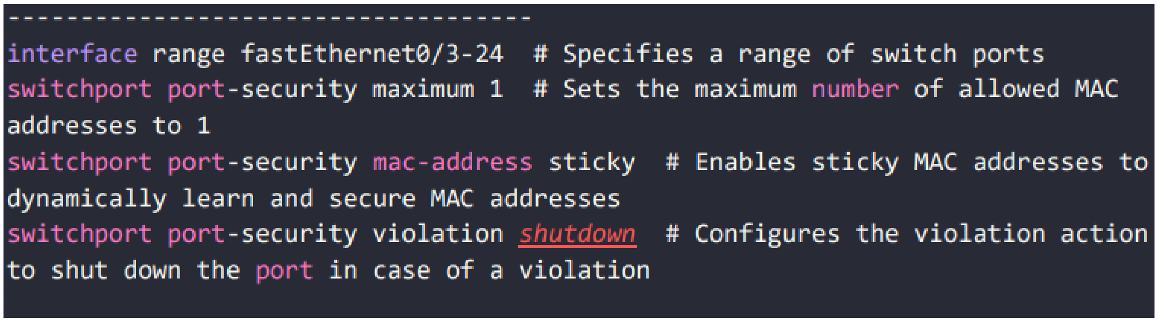
Trunking is used to carry traffic from multiple VLANs across a single link between switches. It allows VLAN information to travel between switches using tagging protocols like IEEE 802.1Q, ensuring proper delivery to the correct VLAN.



```
int range fa0/1-2
switchport mode trunk
exit
vlan 30
name Finance
vlan 99
name BlackHole
exit
int range fa0/3-24
switchport mode access
switchport access vlan 30
exit
int range gig0/1-2
switchport mode access
switchport access vlan 99
shutdown
exit
do wr
```

Port Security using sticky MAC method:

Port security is a feature on Cisco switches that restricts access to switch ports based on MAC addresses. Using the **sticky MAC** method, the switch dynamically learns the MAC address of a device connected to a port and automatically adds it to the running configuration. Once learned, the port only allows traffic from that MAC address. If another device tries to connect, the port can block it based on the configured violation mode (protect, restrict, or shutdown). This helps prevent unauthorized access and improves network security.

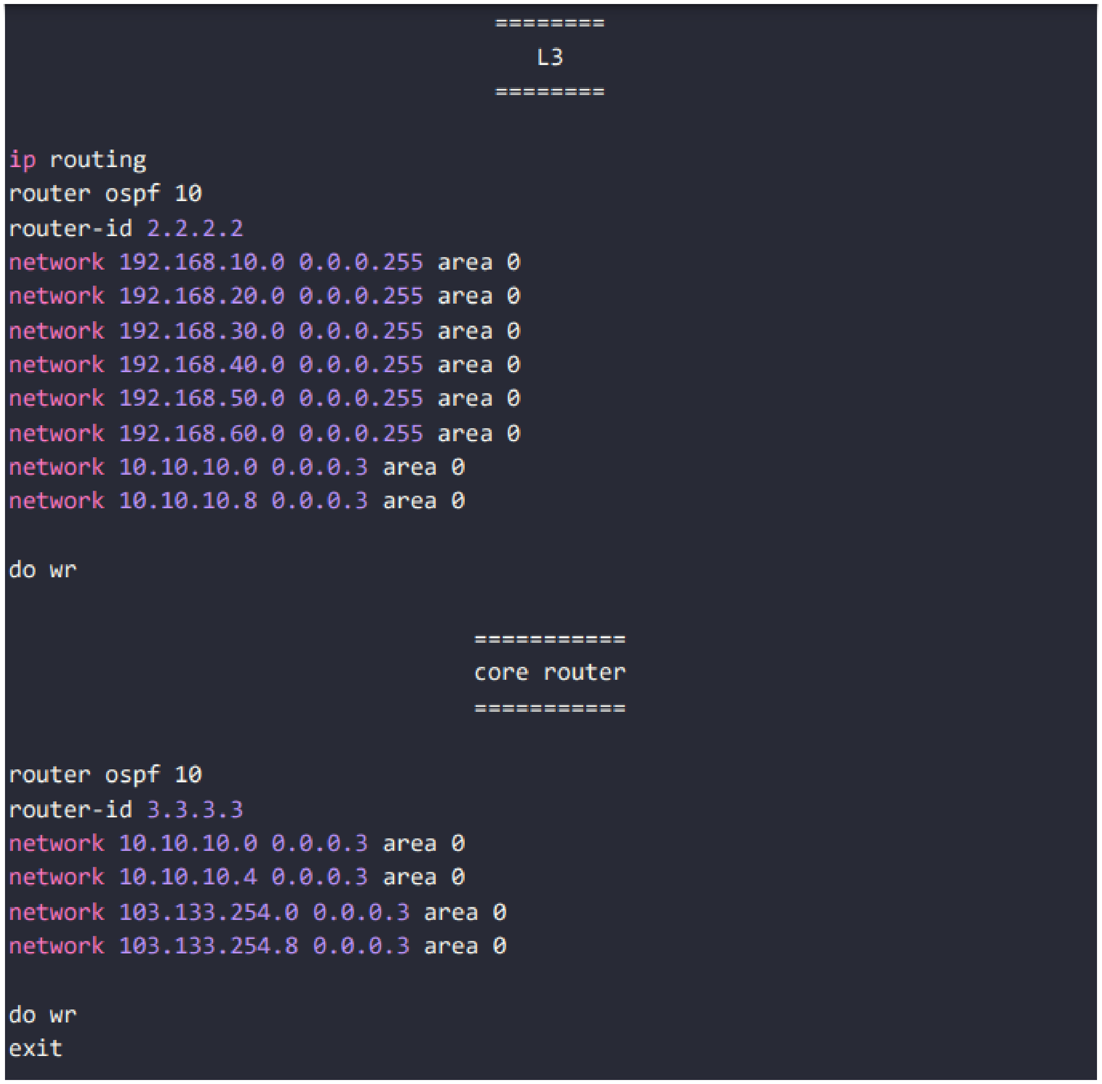


```
-----------------------------------
interface range fastEthernet0/3-24  # Specifies a range of switch ports
switchport port-security maximum 1  # Sets the maximum number of allowed MAC
addresses to 1
switchport port-security mac-address sticky  # Enables sticky MAC addresses to
dynamically learn and secure MAC addresses
switchport port-security violation shutdown  # Configures the violation action
to shut down the port in case of a violation
```

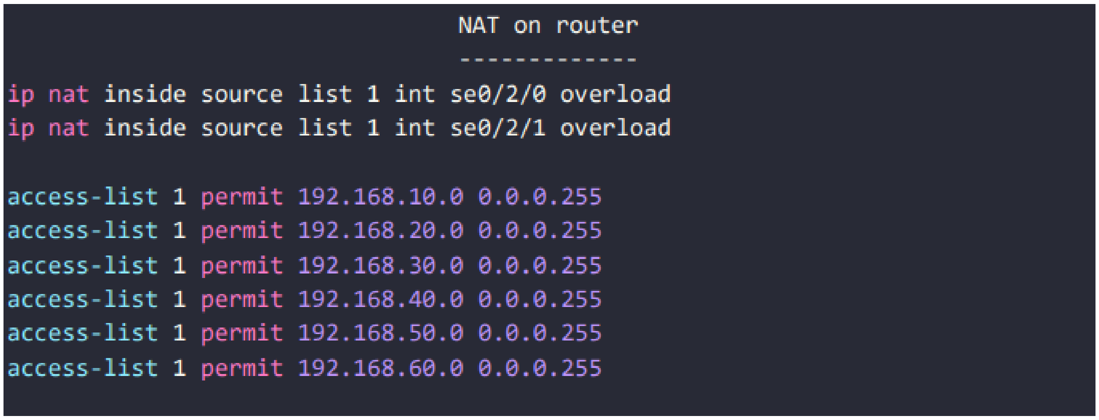
Routing Configuration:

Routing allows data to move between different networks. In Cisco devices, routing can be configured using static routes or dynamic routing protocols like OSPF & NAT.

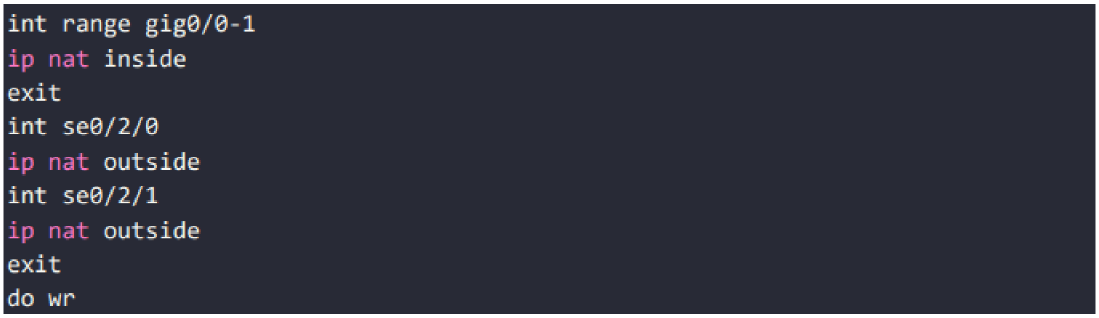
Static routing involves manually defining the path to reach other networks, while dynamic routing enables routers to learn routes automatically and adjust to network changes.



```
                                  ========
                                     L3
                                  ========

ip routing
router ospf 10
router-id 2.2.2.2
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 192.168.40.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.60.0 0.0.0.255 area 0
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.8 0.0.0.3 area 0

do wr

                                 ===========
                                 core router
                                 ===========

router ospf 10
router-id 3.3.3.3
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.4 0.0.0.3 area 0
network 103.133.254.0 0.0.0.3 area 0
network 103.133.254.8 0.0.0.3 area 0

do wr
exit
```



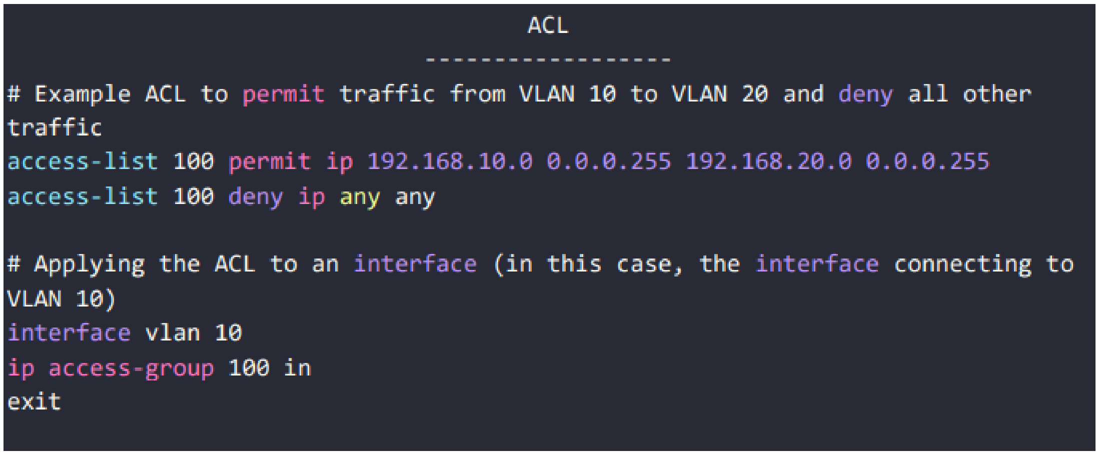
```
                              NAT on router
                              -------------
ip nat inside source list 1 int se0/2/0 overload
ip nat inside source list 1 int se0/2/1 overload

access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
access-list 1 permit 192.168.50.0 0.0.0.255
access-list 1 permit 192.168.60.0 0.0.0.255
```



```
int range gig0/0-1
ip nat inside
exit
int se0/2/0
ip nat outside
int se0/2/1
ip nat outside
exit
do wr
```

Access control List (ACL) Configuration:

Access Control Lists (ACLs) are used on Cisco devices to control the flow of traffic based on rules. They filter network traffic by allowing or denying packets based on criteria like IP addresses, protocols, or port numbers. ACLs can be standard (filter by source IP only) or extended (filter by source, destination, and protocol). They are applied to interfaces in either the inbound or outbound direction to enforce security and traffic policies. Proper ACL configuration helps secure the network and control access to resources.

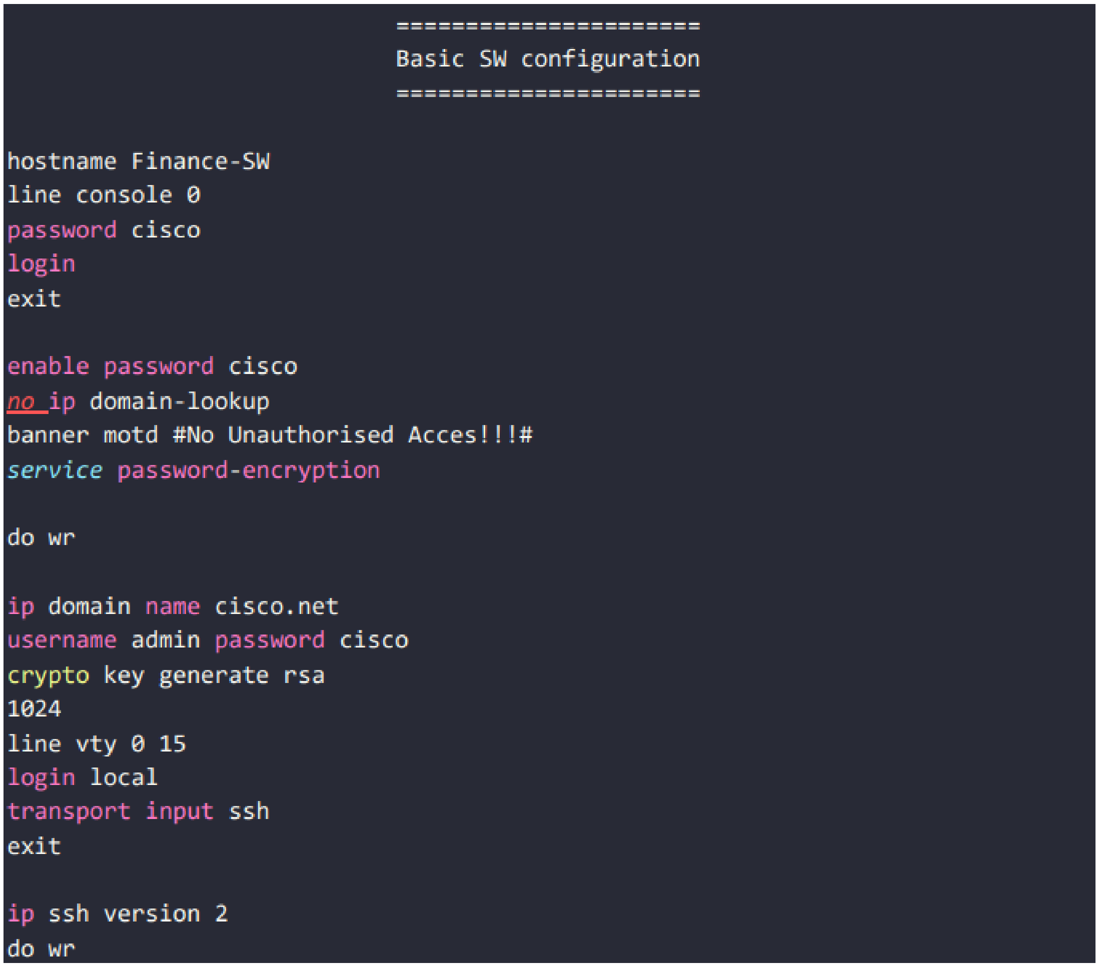


```
                                   ACL
                            ------------------
# Example ACL to permit traffic from VLAN 10 to VLAN 20 and deny all other
traffic
access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 100 deny ip any any

# Applying the ACL to an interface (in this case, the interface connecting to
VLAN 10)
interface vlan 10
ip access-group 100 in
exit
```

Switching Configuration (Excluding DMZ Switch):

Switching configuration on all internal switches involves setting up VLANs, assigning access ports to VLANs, enabling trunk links between switches, and configuring port security where needed. These switches are used for internal communication and segmentation to improve performance and security.

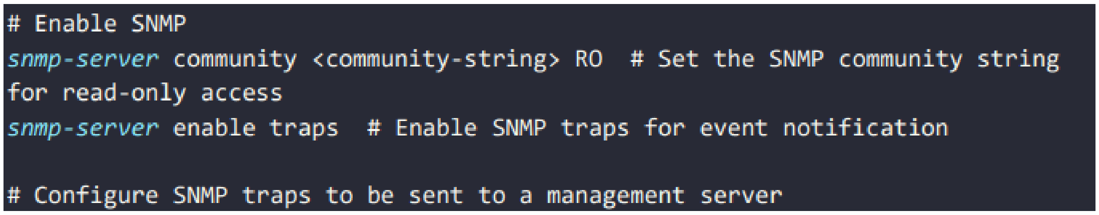
The DMZ switch is excluded from this configuration as it handles external-facing services and requires a separate, more secure setup. Internal switches focus on efficient and secure data flow within the organization



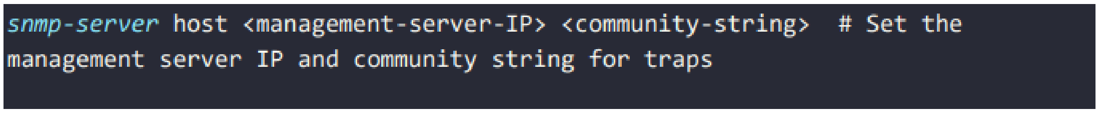
```
                              ======================
                              Basic SW configuration
                              ======================

hostname Finance-SW
line console 0
password cisco
login
exit

enable password cisco
no ip domain-lookup
banner motd #No Unauthorised Acces!!!#
service password-encryption

do wr

ip domain name cisco.net
username admin password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit

ip ssh version 2
do wr
```

SNMP Configuration:

SNMP (Simple Network Management Protocol) is used to monitor and manage network devices like routers and switches. Configuring SNMP on a Cisco device allows network management systems (NMS) to collect data and receive alerts about device performance and issues. Basic SNMP setup includes enabling the protocol and setting a community string (like a password) for read-only or read-write access. This helps administrators track network health and respond quickly to problems. SNMP enhances visibility, control, and automation in network management.



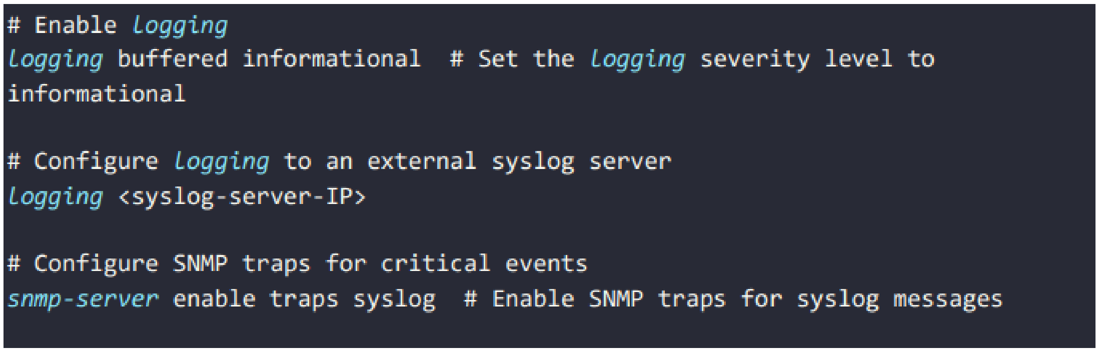
```
# Enable SNMP
snmp-server community <community-string> RO  # Set the SNMP community string
for read-only access
snmp-server enable traps  # Enable SNMP traps for event notification

# Configure SNMP traps to be sent to a management server
```



```
snmp-server host <management-server-IP> <community-string>  # Set the
management server IP and community string for traps
```

Logging and Alerts:

Logging and alerts are configured to capture and report events within the network. The configuration can include setting up logging destinations and severity levels for various events. Here is a sample configuration for logging on a Cisco device:



```
# Enable logging
logging buffered informational  # Set the logging severity level to
informational

# Configure logging to an external syslog server
logging <syslog-server-IP>

# Configure SNMP traps for critical events
snmp-server enable traps syslog  # Enable SNMP traps for syslog messages
```

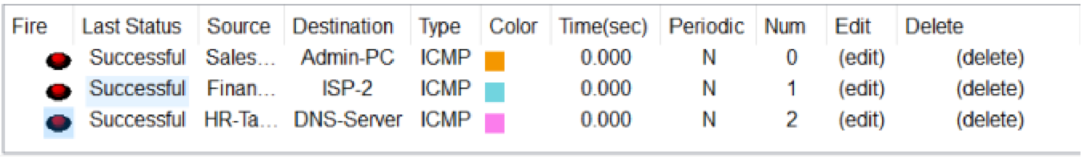
Testing & Results

Cisco Packet Tracer was employed to model and validate the proposed network setup. As a robust network simulation platform, Packet Tracer enables users to design, configure, and test networking scenarios within a virtual environment.

Designing the Network Topology: Based on the project's specifications, a detailed topology was created using Packet Tracer. This included integrating various network components such as routers, switches, end-user devices (PCs), servers, and other relevant hardware.

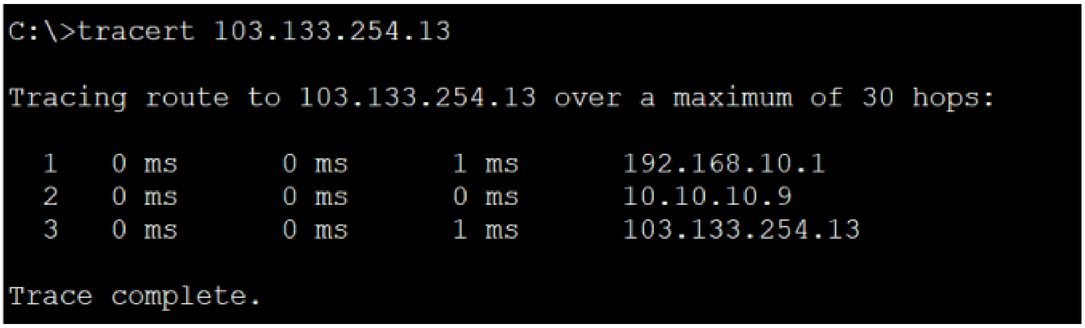
Device Configuration: Once the topology was established, configurations were applied to all necessary network devices. The intuitive interface of Packet Tracer, which closely resembles that of real Cisco hardware, allowed for the realistic simulation of router and switch configurations.

Traffic Flow Testing: Network communication and data transfer between devices were simulated to assess overall connectivity and performance. Packet Tracer's tools were utilized to generate and monitor traffic, ensuring proper data flow throughout the network.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Sales...	Admin-PC	ICMP	🟧	0.000	N	0	(edit)	(delete)
●	Successful	Finan...	ISP-2	ICMP	🟦	0.000	N	1	(edit)	(delete)
●	Successful	HR-Ta...	DNS-Server	ICMP	🟪	0.000	N	2	(edit)	(delete)

Redundancy and Failover Testing: The hierarchical network structure was designed with redundancy at each level, incorporating multiple routers, multilayer switches, and dual ISP links. These elements were rigorously tested to confirm the reliability of failover protocols and overall network stability.



```
C:\>tracert 103.133.254.13

Tracing route to 103.133.254.13 over a maximum of 30 hops:

  1   0 ms      0 ms      1 ms      192.168.10.1
  2   0 ms      0 ms      0 ms      10.10.10.9
  3   0 ms      0 ms      1 ms      103.133.254.13

Trace complete.
```

DHCP and IP Management: The network's dynamic IP address assignment via DHCP was verified to ensure devices obtained appropriate addresses. Simultaneously, static IP configurations were validated for critical devices, such as those located in the server room.

Cost Analysis

Equipment	No. of units	Cost Per Unit	Recurring Cost (INR/Year)	Maintenance Cost (INR/Year)
Core Router	2	Rs.50,000	Rs.10,000	Rs.12,000
Multilayer Switches	3	Rs.1,00,000	Rs.8,000	Rs.20,000
Access Switches	17	Rs.80,000	Rs.4,000	Rs.6,000
Servers	2	Rs.1,50,000	Rs.20,000	Rs.30,000
Wireless Access Points	16	Rs.20,000	Rs.2,000	Rs.3,000
Firewall	3	Rs.1,00,000	Rs.6,000	Rs.8,000
ISP Cost	-	Rs.60,000	Rs.3,50,000	-
UPS	10	Rs.10,000	Rs.5,000	Rs.5,000
Server Rack	1	Rs.1,00,000	Rs.2,000	Rs.2,000
Compliance Cost	-	-	Rs.50,000	-
Inventory Management	-	Rs.20,000/- Year	-	-
End Point Devices (PCs, etc)	-	Rs.65,000	Rs.20,000	Rs.15,000
Caballing & Miscellaneous	-	Rs.1,00,000	-	Rs.20,000
Total	-	Rs.8,55,000	Rs.4,77,000	Rs.1,21,000
Total Budget (Including all cost per unit, recurring cost, maintenance cost) – Rs.24,99,000				

Societal & Industry Impact

Societal Impact:

On the societal front, the project has the potential to create positive ripple effects beyond the plant itself. The implementation and ongoing maintenance of the advanced network will generate new job opportunities and promote skill development in areas such as IT, cybersecurity, and industrial automation. It will also contribute to safer working environments through improved monitoring, real-time alerts, and proactive risk management. The ability to optimize energy usage and reduce waste using real-time data analytics supports environmental sustainability efforts. Furthermore, this initiative could serve as a model for other industries in the region, encouraging broader adoption of smart manufacturing practices and fostering a culture of innovation. By contributing to economic development, technological literacy, and environmental responsibility, the project aligns with broader societal goals and demonstrates the transformative potential of digital infrastructure in modern industry.

Industry Impact:

The successful implementation of the proposed network infrastructure in the manufacturing plant is set to bring substantial benefits to the industry. By integrating advanced systems such as SCADA, IoT, and enterprise IT within a scalable and secure architecture, the plant will achieve greater operational efficiency through real-time monitoring, predictive maintenance, and faster decision-making. Enhanced cybersecurity measures—including VLAN segmentation, Zero Trust Architecture, and intrusion detection systems—will safeguard sensitive data and ensure business continuity. The network's design also allows for future scalability, supporting long-term technological growth and adaptability. Improved interdepartmental data flow will streamline operations, enhance productivity, and foster collaboration across various functions. Collectively, these advancements position the company for a strong competitive advantage in the evolving landscape of Industry 4.0, characterized by automation, smart technologies, and global digital integration.

Conclusion & Future Scope

Conclusion:

This project offers a comprehensive and practical approach to designing a secure and scalable network tailored for a manufacturing plant. By integrating Virtual Local Area Networks (VLANs), advanced routing protocols, and robust security measures, the design enhances network performance while safeguarding critical systems against potential threats. Real-time monitoring capabilities further bolster operational reliability by enabling proactive issue resolution, thereby minimizing downtime and ensuring seamless production processes. The network architecture is strategically future-proofed to accommodate growth and emerging technological advancements, aligning with Industry 4.0 standards and supporting innovations such as Industrial Internet of Things (IIoT). Ultimately, this implementation contributes to a resilient, efficient, and sustainable manufacturing environment, ensuring long-term operational excellence and adaptability in an evolving industrial landscape.

Future Scope:

The future scope of the manufacturing plant network involves several key enhancements. It includes implementing AI-driven analytics to predict failures and optimize network performance, deploying 5G-enabled IoT devices for real-time data transfer, and transitioning to IPv6 to ensure scalability. Additionally, blockchain-based authentication will secure vendor interactions, while biometric authentication will strengthen network access control. The network will also leverage cloud-native management with SD-WAN and a digital twin for simulation. These advancements will create a highly secure, intelligent, and future-proof industrial network, aligning with Industry 4.0 principles to enhance operational efficiency and resilience.

References

1. Mwansa, G., Ngandu, M. R., & Dasi, Z. S. (2024). Enhancing Practical Skills in Computer Networking: Evaluating the Unique Impact of Simulation Tools, Particularly Cisco Packet Tracer, in Resource-Constrained Higher Education Settings. Education Sciences, 14(10), 1099.
2. Das, B. J., Chidambaram, V., & Palanidoss, S. (2023, November). Packet tracer for smart home networks and real-world monitoring. In AIP Conference Proceedings (Vol. 2946, No. 1). AIP Publishing.
3. Malanchini, I., Michailow, N., Agostini, P., Ali-Tolppa, J., Hock, D., Kasparick, M., ... & Zhou, Q. (2023). Convergence of Manufacturing and Networking in Future Factories. arXiv preprint arXiv:2312.08708.
4. Lindenschmitt, D., Mertes, J., Schellenberger, C., Schmitz, M., Han, B., Aurich, J. C., & Schotten, H. D. (2023, October). 6G Underlayer Network Concepts for Ultra Reliable and Low Latency Communication in Manufacturing. In European Wireless 2023; 28th European Wireless Conference (pp. 26-30). VDE.
5. Allison, J. (2022, July). Simulation-based learning via cisco packet tracer to enhance the teaching of computer networks. In Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1 (pp. 68-74).
6. Cisco Networking Cisco Networking Academy. (2020). Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7). Pearson Education, Limited.
7. Kurose, J. F., & Ross, K. W. (2007). Computer networking: A top-down approach edition. Addision Wesley.
8. Coleman, D. D., & Westcott, D. A. (2014). CWNA: Certified wireless network administrator official study guide: Exam CWNA-106. John Wiley & Sons.

Appendix

Abbreviations:

ACL - Access Control List

CIPP Evaluation - Context, Input, Process, and Product

DHCP - Dynamic Host Configuration Protocol

DMZ - Demilitarized Zone

IoT – Internet of Things

IP - Internet Protocol

ISPs - Internet Service Providers

MAC Address - Media Access Control Address

NAT - Network Address Translation

OSPF - Open Shortest Path First

OT - Operational Technology

PAT - Port Address Translation

RSA - Rivest, Shamir, Adleman

SCADA - Supervisory Control and Data Acquisition

SDN – Software Defined Networking

SSH - Secure Shell

STP - Spanning Tree Protocol

UPS – Uninterrupted Power Supply

WAP – Wireless Access Points

VLAN - Virtual Local Area Network