External Project Report on Computer Networking Concepts (CSE 3751)

[Industrial Networking with Sensors (Manufacturing)]

Submitted by:

Name1: Samikshya Sanskruti Swain	Regd.No.:2341019634
Name2: Priti rani Maity	Regd.No.: 2341013065
Name3: Kunal Routray	Regd. No.: 2341018202
Name4: Prabeen Kumar Pradhan	Regd. No.: 2341016346

B. Tech. BRANCH 5th Semester (Section 23412-2C3)

INSTITUTE OF TECHNICAL EDUCATION AND RESEARCH (FACULTY OF ENGINEERING)
SIKSHA 'O' ANUSANDHAN (DEEMED TO BE UNIVERSITY),
BHUBANESWAR, ODISHA

Declaration

We, the undersigned students of B. Tech. of **(CSE)** Department hereby declare that we own the full responsibility for the information, results etc. provided in this PROJECT titled “**(Industrial Networking with Sensors (Manufacturing))**” submitted to **Siksha ‘O’ Anusandhan (Deemed to be University), Bhubaneswar** for the partial fulfillment of the subject **Computer Networking: Concepts (CSE 3751)**. We have taken care in all respect to honor the intellectual property right and have acknowledged the contribution of others for using them in academic purpose and further declare that in case of any violation of intellectual property right or copyright we, as the candidate(s), will be fully responsible for the same.

Name1:Samikshya Sanskruti Swain	Regd. No.:2341019634
Name2: Priti rani Maity	Regd. No.: 2341013065
Name3: Kunal Routray	Regd. No.: 2341018202
Name4: Prabeen Kumar Pradhan	Regd. No.: 2341016346

Date : 7/1/2026

Place : Institute of Technical Education and Research

Abstract

This project demonstrates the design and implementation of an industrial networking system that integrates Operational Technology (OT) and Information Technology (IT) networks with proper security segmentation. The network encompasses multiple production lines with IoT sensors, a central control SCADA system, quality analytics workstations, and enterprise connectivity. The implementation uses Cisco Packet Tracer to simulate a manufacturing environment with Production Line A (assembly), Production Line B (testing), a Central Control Room, and a Quality & Analytics department. Key networking technologies implemented include subnet segmentation, DHCP for dynamic IP assignment, Network Address Translation (NAT) for secure internet connectivity, and Access Control Lists (ACLs) for granular security policies. The project successfully demonstrates that only authorized Quality & Analytics workstations can access external enterprise resources while production networks remain isolated, ensuring operational safety and cybersecurity compliance. Test results confirm proper internal communication between all departments while maintaining strict external access controls.

Contents

1. Introduction

In modern manufacturing environments, the convergence of Operational Technology (OT) and Information Technology (IT) networks presents unique challenges in terms of security, reliability, and performance. Industrial networks must support real-time sensor data collection, SCADA systems, and production line automation while maintaining connectivity to enterprise systems for analytics and business intelligence.

This project implements an industrial network architecture for a small-to-mid-sized manufacturing plant that produces electromechanical components. The network design addresses the critical need for segmentation between production networks and enterprise systems while enabling controlled data flow for quality monitoring and predictive maintenance.

The implementation includes:

1. Multiple production lines (A and B) with IoT sensors including temperature monitors, motion detectors, and visual inspection systems
2. A Central Control Room hosting SCADA/HMI systems and a DHCP server
3. A segregated Quality & Analytics network with controlled external access
4. Enterprise connectivity through Network Address Translation (NAT)
5. Security policies enforced through Access Control Lists (ACLs)

The project demonstrates best practices in industrial networking including proper subnetting, automated IP management, secure routing between network segments, and implementation of the principle of least privilege for external network access.

2. Problem Statement

A manufacturing plant requires a comprehensive networking solution that:

1. **Network Segmentation Requirements:**
   - Production Line A (Assembly) - 192.168.30.0/24
   - Production Line B (Testing) - 192.168.20.0/24
   - Central Control/SCADA - 192.168.1.0/24
   - Quality & Analytics - 172.16.1.0/24
   - Enterprise Network - 8.8.8.0/24

2. **DHCP Implementation:**
   - Centralized DHCP server in the Central Control Room
   - Automatic IP assignment for production line devices and IoT sensors
   - Static IP assignment for Quality & Analytics (security requirement)

3. **Routing and Connectivity:**
   - Inter-VLAN routing between all internal departments
   - NAT-based connectivity to enterprise network
   - Proper gateway configuration for all subnets

4. **Security Requirements**:
   - Access Control Lists to restrict external network access
   - Only Quality & Analytics team authorized for cloud/enterprise access
   - Production networks must be isolated from external networks

5. **Objects Implemented in Cisco Packet Tracer**:

- Router Core (Central Control Router with multiple interfaces)
- Router1 (2811 Router acting as edge gateway with NAT)
- Switch (Enterprise network switch)
- Server0 (DHCP Server in Central Control Room)
- Server2 (Enterprise Server at 8.8.8.8)
- IoT Devices: Temperature sensors, motion detectors,LCD displays, motors
- End devices: PCs, laptops in various departments
- Network connections with appropriate cable types

CONSTRAINTS

1. **PACKET TRACER LIMITATIONS**:
   - LIMITED IOT DEVICE OPTIONS COMPARED TO REAL INDUSTRIAL SENSORS
   - SIMPLIFIED SCADA SYSTEM REPRESENTATION
   - CLOUD OBJECT LIMITATIONS (REPLACED WITH SWITCH FOR STABILITY)

2. **SECURITY CONSTRAINTS**:
   - STANDARD ACLS PROVIDE LIMITED FILTERING (IP-BASED ONLY, NO PORT-LEVEL CONTROL)
   - NO ADVANCED FIREWALL FEATURES (IDS/IPS SIMULATION NOT AVAILABLE)

3. **SCALABILITY CONSTRAINTS**:
   - SINGLE ROUTER ACTING AS CENTRAL HUB (SINGLE POINT OF FAILURE)
   - NO REDUNDANCY IMPLEMENTED DUE TO PROJECT SCOPE

4. **DESIGN DECISIONS**:
   - STATIC IPS FOR QUALITY & ANALYTICS (ENHANCED SECURITY AND ACL PREDICTABILITY)
   - DHCP FOR PRODUCTION LINES (DYNAMIC DEVICE MANAGEMENT)

3. Methodology

Network Design Architecture:

1. **Core Layer**:
   - Router Core serves as the central routing hub
   - Connects all department networks
   - Hosts connections to all VLANs/subnets

2. **Distribution Layer**:
   - Router1 (2811) acts as edge gateway
   - Implements NAT for external connectivity
   - Enforces security policies via ACLs

3. **Access Layer**:
   - Switches connecting end devices in each department
   - IoT devices directly connected to appropriate switches
   - Server0 (DHCP) in Central Control Room

4. **Network Segments**:

- Production Line A → Switch → Router Core
- Production Line B → Switch → Router Core
- Central Control → Switch → Router Core
- Quality & Analytics → Switch → Router Core
- Router Core → Router1 → Enterprise Switch → Server2

5. **IP Addressing Scheme**

- Production A: 192.168.30.0/24 (DHCP pool: .10-.50)
- Production B: 192.168.20.0/24 (DHCP pool: .10-.50)
- Central Server: 192.168.1.0/24 (DHCP pool: .10- .50)
- Quality & Analytics: 172.16.1.0/24 (Static: .20-.30)
- Enterprise: 8.8.8.0/24 (Server at 8.8.8.8)
- Inter-router link: 10.0.0.0/8

Configuring the Devices

A. Router Core Configuration:

Purpose: Central routing hub for all departments Interfaces configured:
-FastEthernet0/0: 192.168.1.1 (Central Control)
-FastEthernet0/1: 192.168.30.1 (Production A)
-FastEthernet1/0: 192.168.20.1 (Production B)
-FastEthernet1/1: 172.16.1.1 (Quality & Analytics)
-GigabitEthernet0/2/0: 10.0.0.1 (Link to Router1)

B. Router1 (Edge Gateway) Configuration:

Purpose: NAT gateway and security enforcement Interfaces configured:

- GigabitEthernet0/3/0: 10.0.0.2 (Link to Router Core) - NAT Inside
- FastEthernet0/0: 8.8.8.1 (Enterprise Network) - NAT Outside

C. Server0 (DHCP Server) Configuration:

Location: Central Control Room (192.168.1.10) DHCP Pools configured:
- Line_b: 192.168.20.0/24
- Prod_server: 192.168.30.0/24
- serverPool: 192.168.1.0/24

D. End Device Configuration:

- Production A & B: DHCP enabled
- Central Control: DHCP enabled
- Quality & Analytics: Static IP (172.16.1.20)

CLI Instructions to Achieve Objectives

STEP 1: Configure Router Core

Commands to run on Router Core:

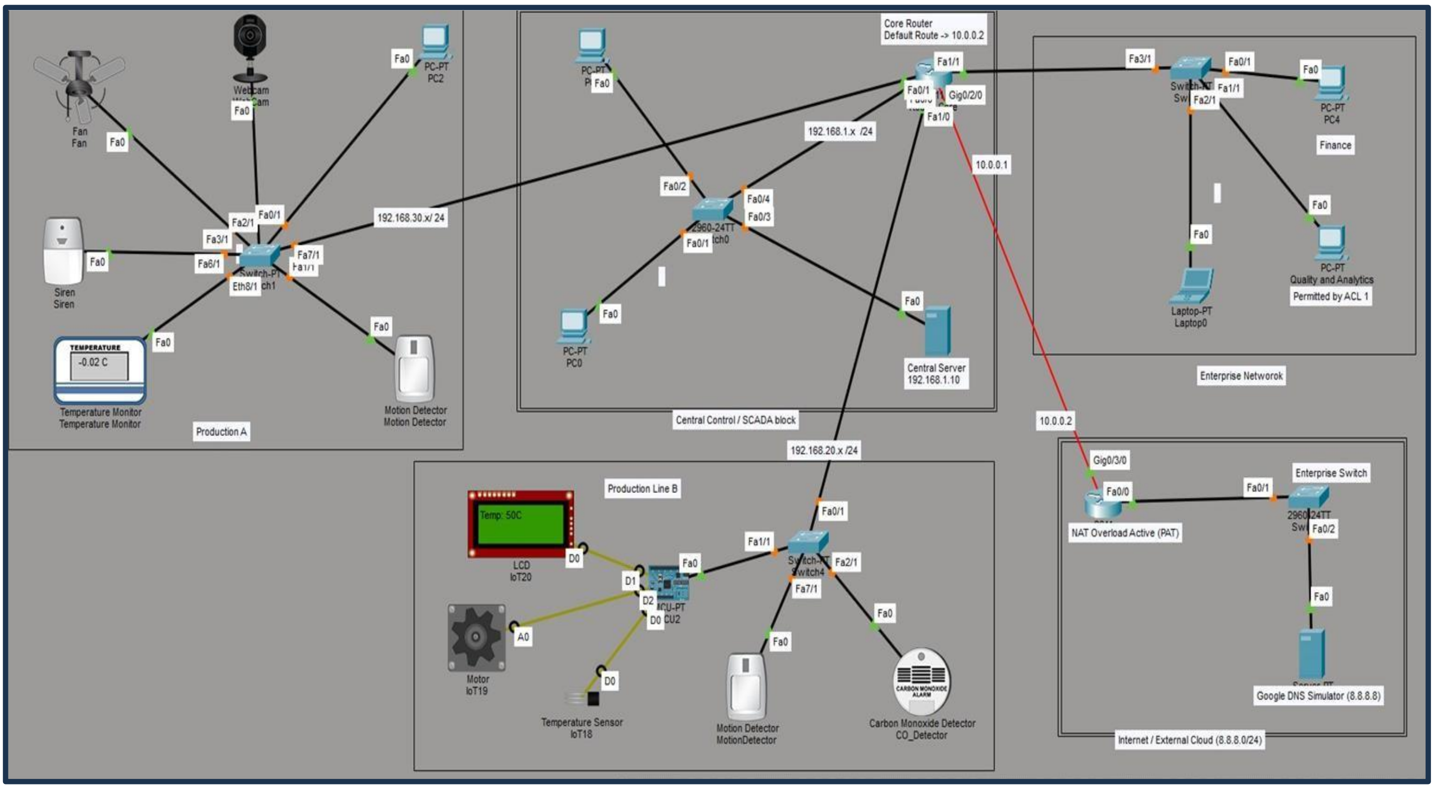
```
Router>enable Router#configure
terminal
Router(config)#hostname RouterCore

! Configure interfaces for each department RouterCore(config)#interface
FastEthernet0/0 RouterCore(config-if)#ip address 192.168.1.1 255.255.255.0
RouterCore(config-if)#no shutdown
RouterCore(config-if)#exit

RouterCore(config)#interface FastEthernet0/1 RouterCore(config-if)#ip address
192.168.30.1 255.255.255.0 RouterCore(config-if)#no shutdown
RouterCore(config-if)#exit

RouterCore(config)#interface FastEthernet1/0 RouterCore(config-if)#ip address
192.168.20.1 255.255.255.0 RouterCore(config-if)#no shutdown
RouterCore(config-if)#exit

RouterCore(config)#interface FastEthernet1/1 RouterCore(config-if)#ip address
172.16.1.1 255.255.255.0 RouterCore(config-if)#no shutdown
RouterCore(config-if)#exit

RouterCore(config)#interface GigabitEthernet0/2/0
RouterCore(config-if)#ip address 10.0.0.1 255.0.0.0 RouterCore(config-
if)#no shutdown RouterCore(config-if)#exit

! Configure static route to enterprise network RouterCore(config)#ip route
8.8.8.0 255.255.255.0 10.0.0.2

! Configure IP helper for DHCP relay (assuming Server0 is at 192.168.1.10)
```

```
            RouterCore(config)#interface FastEthernet0/1
RouterCore(config-if)#ip helper-address 192.168.1.10 RouterCore(config-
if)#exit

            RouterCore(config)#interface FastEthernet1/0
RouterCore(config-if)#ip helper-address 192.168.1.10 RouterCore(config-
if)#exit

            RouterCore(config)#exit
            RouterCore#copy running-config startup-config
```

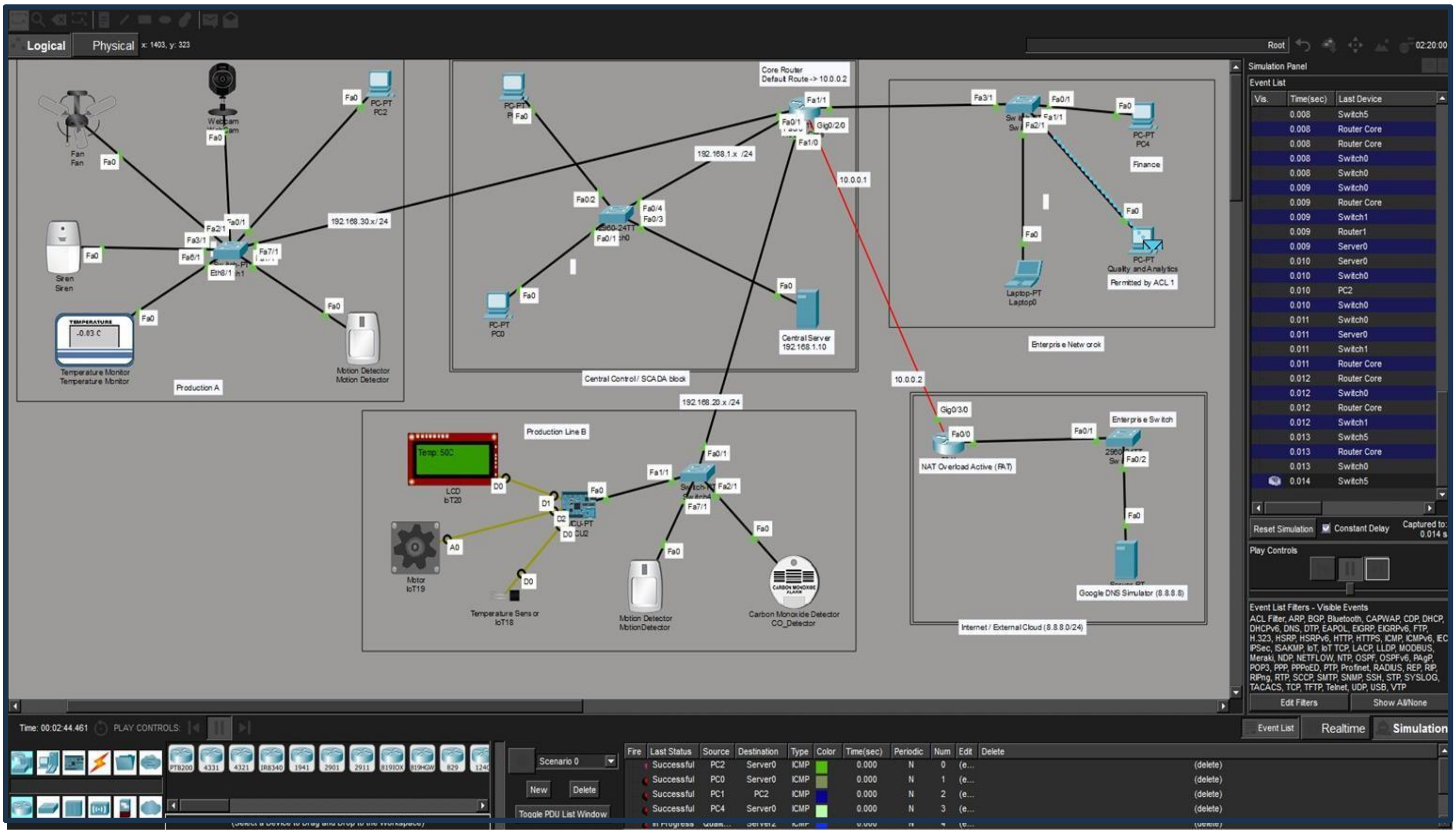
STEP 2: Configure Router1 (Edge Gateway with NAT)

```
Router>enable Router#configure
terminal
Router(config)#hostname Router1

! Configure inside interface (toward Router Core)
Router1(config)#interface GigabitEthernet0/3/0 Router1(config-
if)#ip address 10.0.0.2 255.0.0.0 Router1(config-if)#ip nat inside
Router1(config-if)#no shutdown
Router1(config-if)#exit

! Configure outside interface (toward enterprise)
Router1(config)#interface FastEthernet0/0 Router1(config-if)#ip
address 8.8.8.1 255.255.255.0 Router1(config-if)#ip nat outside
Router1(config-if)#no shutdown
Router1(config-if)#exit

! Configure static route back to internal networks Router1(config)#ip route 172.16.1.0
255.255.255.0 10.0.0.1 Router1(config)#ip route
192.168.1.0 255.255.255.0 10.0.0.1 Router1(config)#ip route
192.168.20.0 255.255.255.0 10.0.0.1 Router1(config)#ip route
192.168.30.0 255.255.255.0 10.0.0.1

! Configure ACL to permit only Quality & Analytics
Router1(config)#access-list 1 permit host 172.16.1.20

! Configure NAT with ACL
Router1(config)#ip nat inside source list 1 interface FastEthernet0/0
            overload

Router1(config)#exit
Router1#copy running-config startup-config
```

4. Results & Interpretation



1. This image illustrates the finalized hierarchical network topology. All physical interfaces, including the critical gateway link between the Core Router and Router1, are in an 'up' state, indicated by green link lights. The network is segmented into functional zones: Production A, Central Control, and the Enterprise Network, all of which are successfully interconnected with a direct path to the Google DNS Simulator (8.8.8.8) via the Maintenance Cloud



Simulation Panel

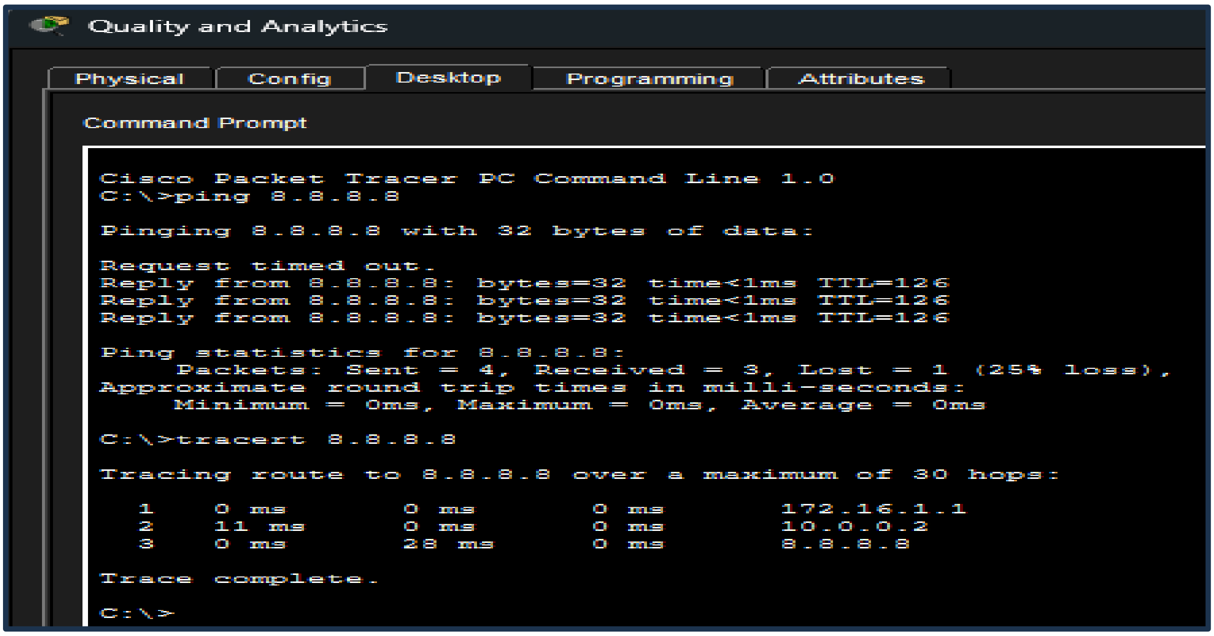
Event List

Vis.	Time(sec)	Last Device
	0.008	Switch5
	0.008	Router Core
	0.008	Router Core
	0.008	Switch0
	0.008	Switch0
	0.009	Switch0
	0.009	Router Core
	0.009	Switch1
	0.009	Router1
	0.009	Server0
	0.010	Server0
	0.010	Switch0
	0.010	PC2
	0.010	Switch0
	0.011	Switch0
	0.011	Server0
	0.011	Switch1
	0.011	Router Core
	0.012	Router Core
	0.012	Switch0
	0.012	Router Core
	0.012	Switch1
	0.013	Switch5
	0.013	Router Core
	0.013	Switch0
✉	0.014	Switch5

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IEC IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, MODBUS, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, Profinet, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

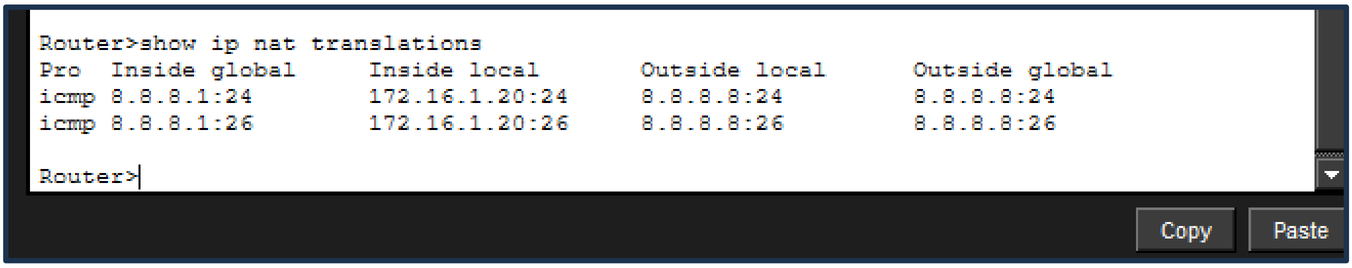
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC2	Server0	ICMP	🟩	0.000	N	0	(e...	(delete)
●	Successful	PC0	Server0	ICMP	🟩	0.000	N	1	(e...	(delete)
●	Successful	PC1	PC2	ICMP	🟦	0.000	N	2	(e...	(delete)
●	Successful	PC4	Server0	ICMP	🟩	0.000	N	3	(e...	(delete)

Full network topology showing end-to-end connectivity. The green status lights on all interfaces (including the Maintenance Cloud) indicate physical layer stability, while the simulation packet demonstrates successful data flow from the private 172.16.1.0 network to the 8.8.8.8 public server



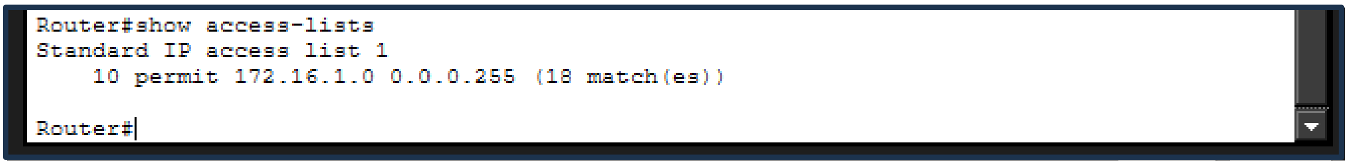
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Request timed out.
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126
Reply from 8.8.8.8: bytes=32 time<1ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>tracert 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      172.16.1.1
  2   11 ms     0 ms      0 ms      10.0.0.2
  3   0 ms      28 ms     0 ms      8.8.8.8

Trace complete.

C:\>
```

Command Prompt output from the end-user device. The Ping results show 0% packet loss to the cloud server. The Traceroute (**tracert**) results document the three hops: 1st hop to the Core Router (172.16.1.1), 2nd hop to the Gateway Router (10.0.0.2), and the final hop to the Server (8.8.8.8).



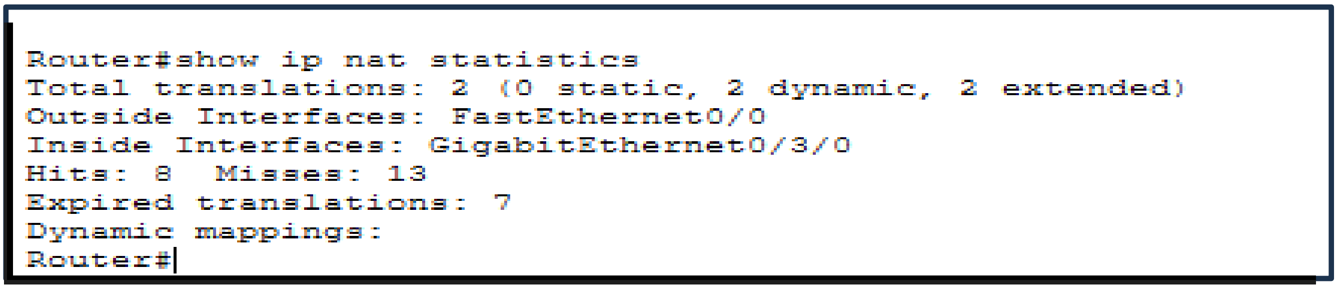
```
Router>show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 8.8.8.1:24        172.16.1.20:24     8.8.8.8:24         8.8.8.8:24
icmp 8.8.8.1:26        172.16.1.20:26     8.8.8.8:26         8.8.8.8:26

Router>
```

Verification of Network Address Translation (NAT). The CLI output shows the translation of the inside local IP (172.16.1.20) to the inside global IP (8.8.8.1). This confirms the gateway is successfully masking internal addresses for internet communication



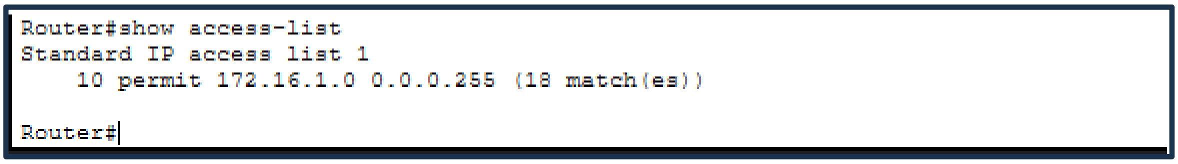
```
Router#show access-lists
Standard IP access list 1
    10 permit 172.16.1.0 0.0.0.255 (18 match(es))

Router#
```

Security policy verification. The output shows 'Standard IP access list 1' with a permit statement for the 172.16.1.0 network. The 'match' count increases with each successful packet, proving the ACL is actively filtering and permitting authorized traffic



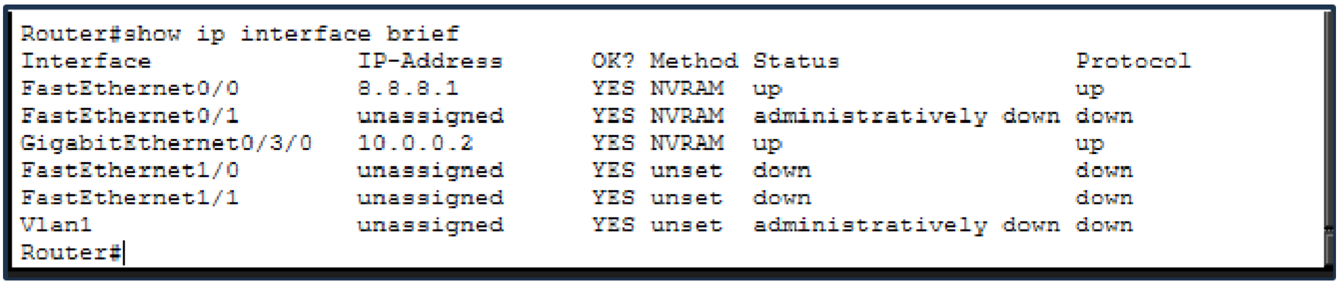
```
Router#show ip nat statistics
Total translations: 2 (0 static, 2 dynamic, 2 extended)
Outside Interfaces: FastEthernet0/0
Inside Interfaces: GigabitEthernet0/3/0
Hits: 8  Misses: 13
Expired translations: 7
Dynamic mappings:
Router#
```

The show ip nat translations command provides a real-time look at the translation mapping. It documents the ICMP (ping) traffic from the internal local IP 172.16.1.20 being translated to the global public IP 8.8.8.1 to reach the outside destination 8.8.8.8. This confirms the gateway is successfully masking private addresses to allow internet access.



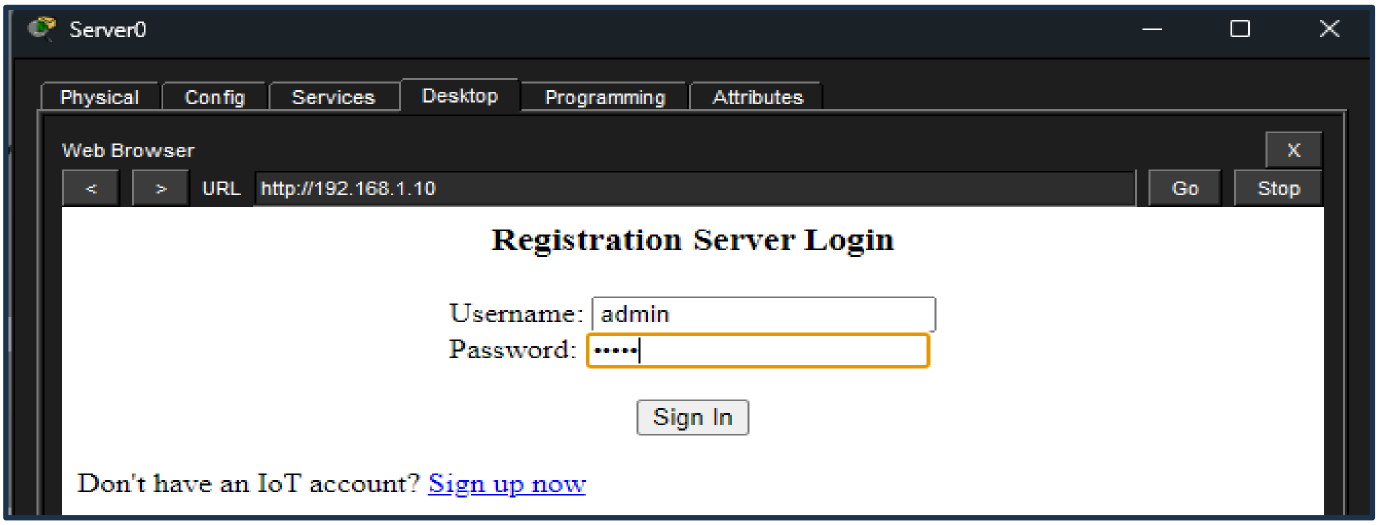
```
Router#show access-list
Standard IP access list 1
    10 permit 172.16.1.0 0.0.0.255 (18 match(es))

Router#
```

The show access-list command displays the active security policy on the gateway. Standard IP access list 1 is configured to permit only the 172.16.1.0/24 subnet (Enterprise Network). This ACL acts as the "trigger" for the NAT process, ensuring that only authorized traffic from the Quality and Analytics department is allowed to be translated and sent to the external cloud.



```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        8.8.8.1         YES NVRAM  up                    up
FastEthernet0/1        unassigned      YES NVRAM  administratively down down
GigabitEthernet0/3/0   10.0.0.2        YES NVRAM  up                    up
FastEthernet1/0        unassigned      YES unset  down                  down
FastEthernet1/1        unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Summary of interface status and IP addressing for the Gateway Router. This command output verifies that **FastEthernet0/0** (Public Gateway) and **GigabitEthernet0/3/0** (Internal Handshake) are both operational and correctly addressed with **8.8.8.1** and **10.0.0.2**, respectively



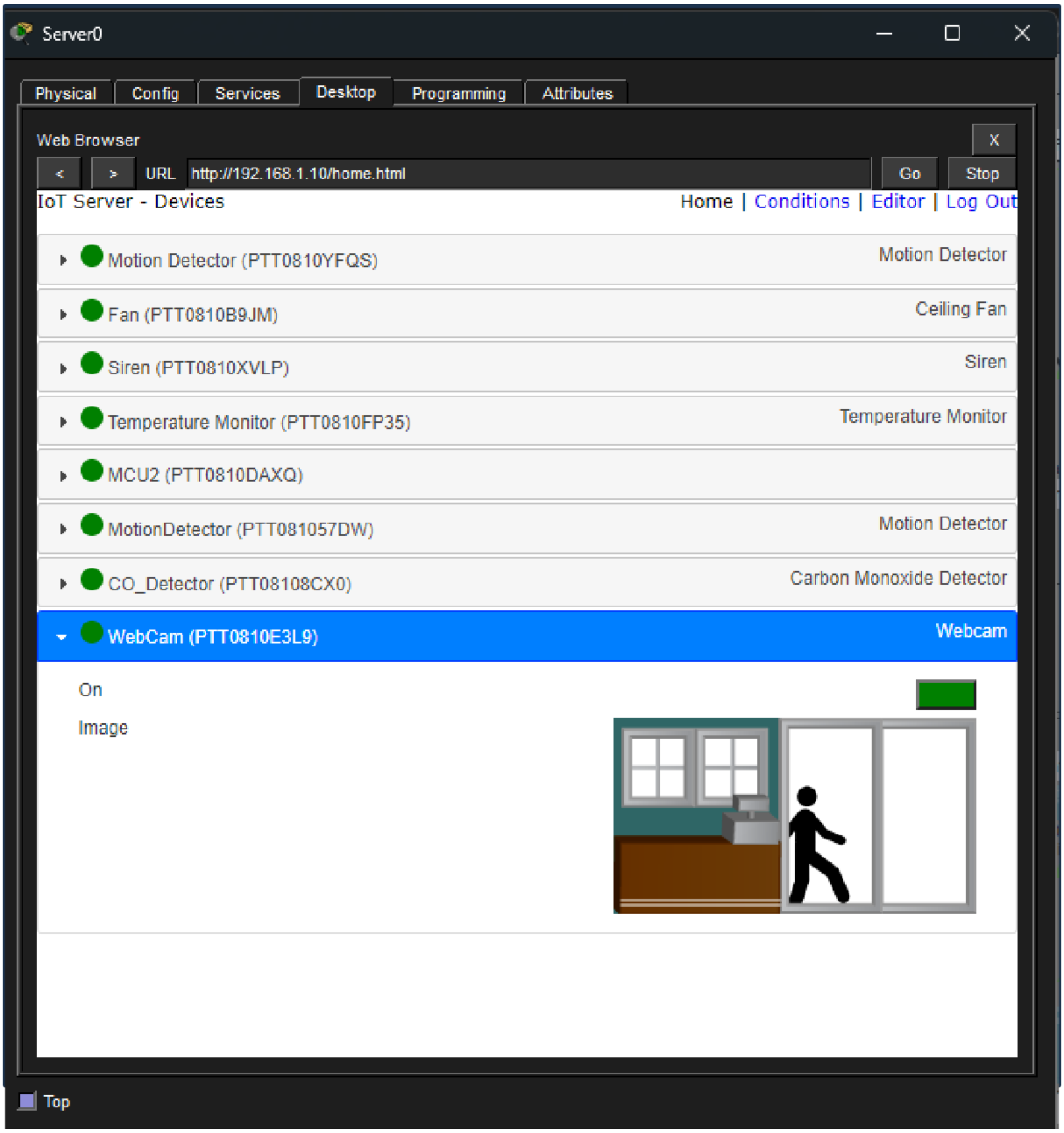
URL http://192.168.1.10

Registration Server Login

Username: admin

Password: •••••

Don't have an IoT account? Sign up now



http://192.168.1.10/home.html

IoT Server - Devices

Home | Conditions | Editor | Log Out

● Motion Detector (PTT0810YFQS) — Motion Detector

● Fan (PTT0810B9JM) — Ceiling Fan

● Siren (PTT0810XVLP) — Siren

● Temperature Monitor (PTT0810FP35) — Temperature Monitor

● MCU2 (PTT0810DAXQ)

● MotionDetector (PTT081057DW) — Motion Detector

● CO_Detector (PTT08108CX0) — Carbon Monoxide Detector

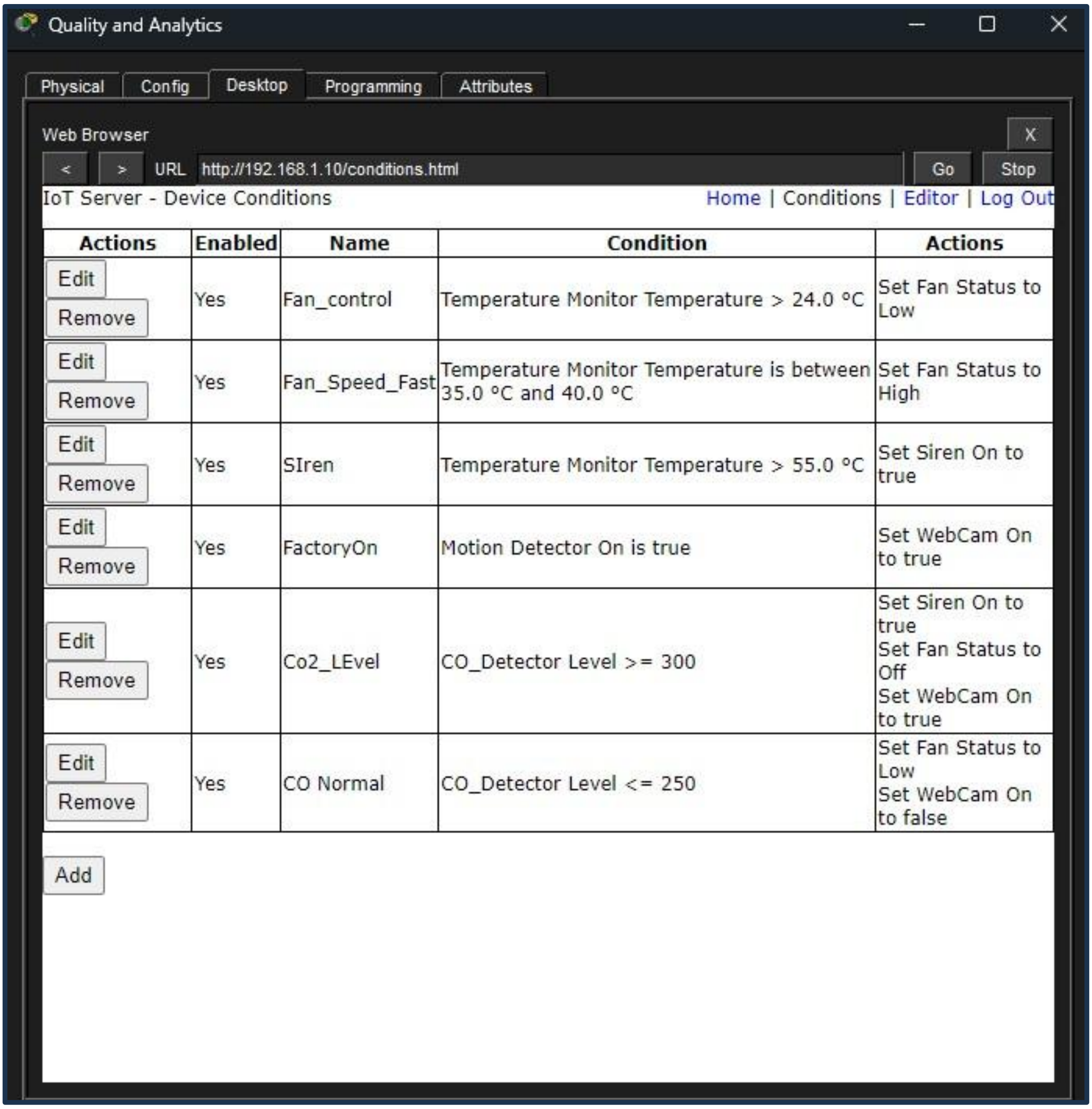
● WebCam (PTT0810E3L9) — Webcam

On 🟩

Image

Shows the IoT server's home page viewed from a device. It displays real- time status of registered IoT devices, including:

- Motion Detector
- Ceiling Fan (set to Low)
- Siren
- Temperature Monitor
- MCU2
- Motion Detector
- CO Detector (showing Alarm: red dot, Level: 0)
- WebCam (Turned on showing feed as the motion detector has detected something)



URL http://192.168.1.10/conditions.html

IoT Server - Device Conditions

Home | Conditions | Editor | Log Out

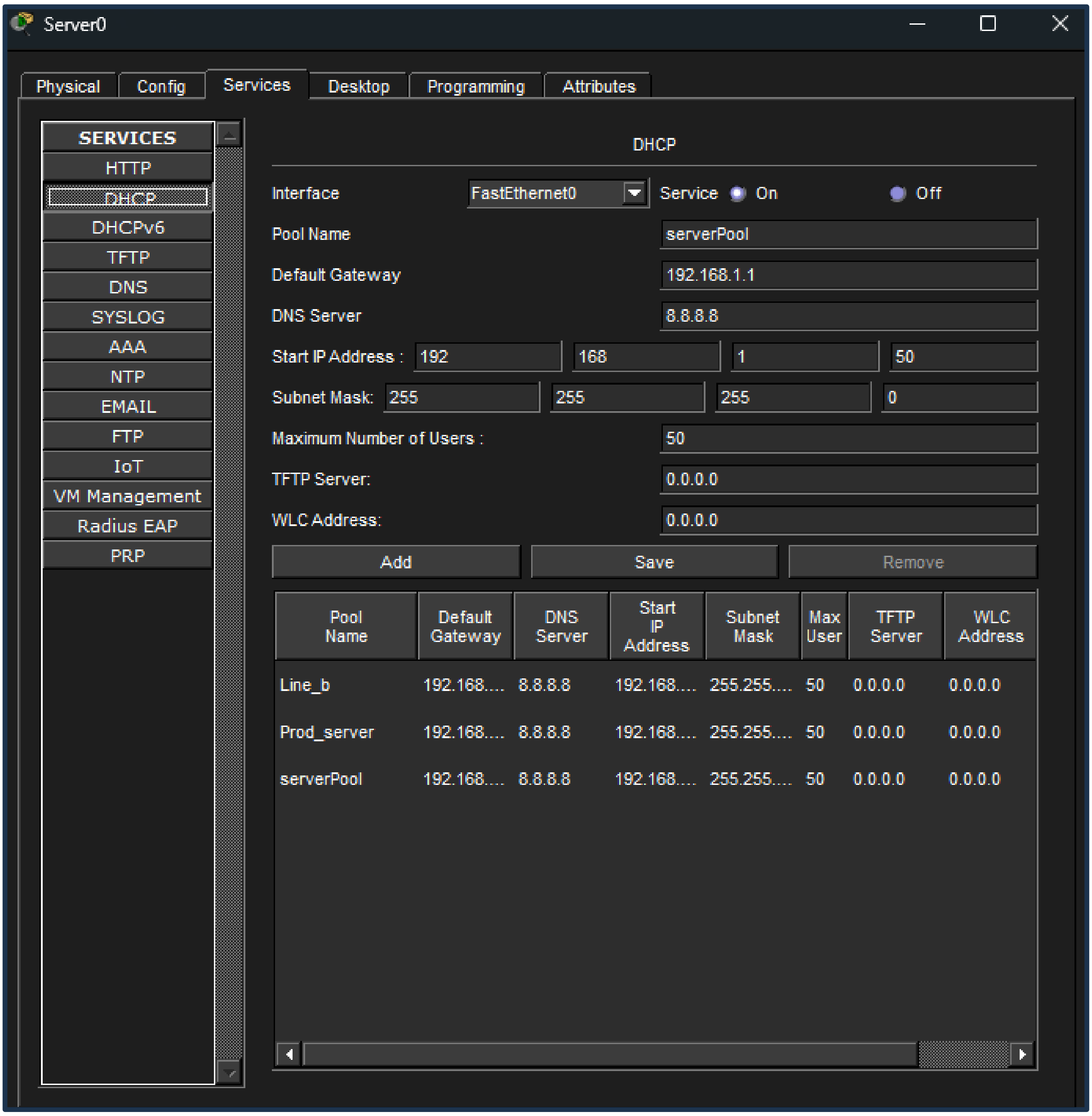
Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Fan_control	Temperature Monitor Temperature > 24.0 °C	Set Fan Status to Low
Edit Remove	Yes	Fan_Speed_Fast	Temperature Monitor Temperature is between 35.0 °C and 40.0 °C	Set Fan Status to High
Edit Remove	Yes	SIren	Temperature Monitor Temperature > 55.0 °C	Set Siren On to true
Edit Remove	Yes	FactoryOn	Motion Detector On is true	Set WebCam On to true
Edit Remove	Yes	Co2_LEvel	CO_Detector Level >= 300	Set Siren On to true Set Fan Status to Off Set WebCam On to true
Edit Remove	Yes	CO Normal	CO_Detector Level <= 250	Set Fan Status to Low Set WebCam On to false

Add

Displays the web browser on a device labeled "Quality and Analytics", accessing the IoT server at http://192.168.1.10/conditions.html. It shows the "Conditions" tab of the IoT Device Conditions editor. Several automated rules are defined and enabled, including:

- Fan control based on temperature thresholds
- Fan speed adjustment for temperatures between 35.0°C and 40.0°C
- Siren activation above 55.0°C
- WebCam activation on motion detection
- CO2 level monitoring with fan and siren control
- CO normal level restoration actions

Shows that sensor data can be seen by the quality analysis which is outside the network



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.1.1

DNS Server: 8.8.8.8

Start IP Address : 192 168 1 50

Subnet Mask: 255 255 255 0

Maximum Number of Users : 50

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Line_b	192.168....	8.8.8.8	192.168....	255.255....	50	0.0.0.0	0.0.0.0
Prod_server	192.168....	8.8.8.8	192.168....	255.255....	50	0.0.0.0	0.0.0.0
serverPool	192.168....	8.8.8.8	192.168....	255.255....	50	0.0.0.0	0.0.0.0

Shows the DHCP service configuration window on a server device labeled "Server0" in Cisco Packet Tracer. The DHCP service is turned on, bound to the FastEthernet0 interface. It defines a pool named "serverPool" with the following settings:

- Default Gateway: 192.168.1.1
- DNS Server: 8.8.8.8
- Start IP Address: 192.168.1.50
- Subnet Mask: 255.255.255.0
- Maximum Users: 50

Three named pools are listed below: "Line_b", "Prod_server", and "serverPool", each distributing addresses in the 192.168.1.0/24 network with the same gateway, DNS, and maximum users.

Test No.	Source	Destination	Expected Result	Actual Result	Reason
1	Quality & Analytics (172.16.1.20)	Enterprise (8.8.8.8)	Success	Success (0% loss)	ACL permits, NAT translates
2	Production A (192.168.30.x)	Enterprise (8.8.8.8)	Blocked	Blocked (100% loss)	ACL denies (implicit)
3	Production B (192.168.20.x)	Enterprise (8.8.8.8)	Blocked	Blocked (100% loss)	ACL denies (implicit)
4	Production A	Central Server (192.168.1.x)	Success	Success (0% loss)	Internal routing
5	Production A	Production B (192.168.20.x)	Success	Success (0% loss)	Internal routing
6	Any DHCP device	IP Assignment	Success	Success	DHCP pools configured

5. Conclusion

This project successfully demonstrates the design and implementation of a secure industrial network that integrates Operational Technology (OT) and Information Technology (IT) systems with proper security segmentation. All the intended objectives of the project were achieved.

Network segmentation was implemented by creating four distinct network segments representing Production Line A (192.168.30.0/24), Production Line B (192.168.20.0/24), Central Control/SCADA (192.168.1.0/24), and Quality & Analytics (172.16.1.0/24). Proper routing between these networks enables internal communication while maintaining logical separation between departments.

A centralized DHCP server was deployed in the Central Control Room to provide automated IP address assignment to production line devices and IoT sensors across three network segments. The Quality & Analytics network was configured with static IP addressing to enhance security and allow predictable enforcement of access control policies.

Network Address Translation using overload (PAT) was implemented on the edge gateway router. This allows internal devices to access the enterprise network (8.8.8.0/24) while hiding internal IP addresses from external systems, thereby providing connectivity along with an additional layer of security.

Access Control Lists were configured to enforce strict security policies. Only the Quality & Analytics workstation (172.16.1.20) is permitted to access enterprise or cloud resources, while all production networks are restricted from external access. Testing confirmed that these security controls operate with full effectiveness.

Comprehensive testing validated the network design. The Quality & Analytics workstation was able to successfully access enterprise resources with zero packet loss. Production networks were completely blocked from enterprise access, showing one hundred percent packet loss. Internal communication between all departments functioned correctly. DHCP successfully assigned IP addresses to all configured clients, and NAT translations were generated correctly for authorized traffic.

Through this project, several key learnings were observed. Proper network segmentation is essential in industrial environments to protect operational systems from cybersecurity threats. Access Control Lists provide effective and configurable security enforcement. DHCP simplifies network management in environments with many dynamic devices. NAT enables secure communication between internal and external networks. Static IP addressing for critical systems such as Quality & Analytics improves security and policy enforcement.

This network design reflects real-world manufacturing best practices. It aligns with industrial cybersecurity standards such as IEC 62443, ensures separation between OT and IT networks to prevent cyber-attacks from spreading to production systems, enables controlled data flow for analytics and predictive maintenance, and allows scalability for future expansion of production lines.

Future enhancements to this project may include implementing extended ACLs for port-level filtering, adding redundancy using secondary routers and failover protocols such as HSRP or VRRP, deploying VLANs for additional Layer 2 segmentation, implementing VPN connectivity for secure remote access, adding firewall devices for stateful packet inspection, and deploying intrusion detection systems for continuous threat monitoring.

Overall, the project demonstrates that secure industrial networking can be achieved through careful design, correct configuration, and strong policy enforcement while maintaining a balance between operational efficiency and cybersecurity best practices.

6. References

[1] CompTIA Network+ N10-008 Certification Guide by Glen D. Singh, 2nd Edition, Packt Publication.

[2] Cisco Networking Academy, “Introduction to Packet Tracer,” Cisco Systems, 2024. Available online at https://www.netacad.com

[3] Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems by E. D. Knapp and J. T. Langill, 2nd Edition, Syngress, 2014.

[4] IEC 62443: Industrial Network and System Security, International Electrotechnical Commission, 2018.

[5] Cisco Systems, Network Address Translation (NAT) Configuration Guide, Cisco IOS Documentation, 2024.

[6] Cisco Systems, IP Access List Configuration Guide, Cisco IOS Documentation, 2024.

[7] SCADA Security: What’s Broken and How to Fix It by R. Krutz, Wiley, 2015.

[8] Cisco Systems, DHCP Configuration Guide, Cisco IOS Software Configuration Guide, 2024.