

CpwE Industrial Network Infrastructure with GNS3 Platform

AHMAD SYAFI NURROYAN

1. BACKGROUND

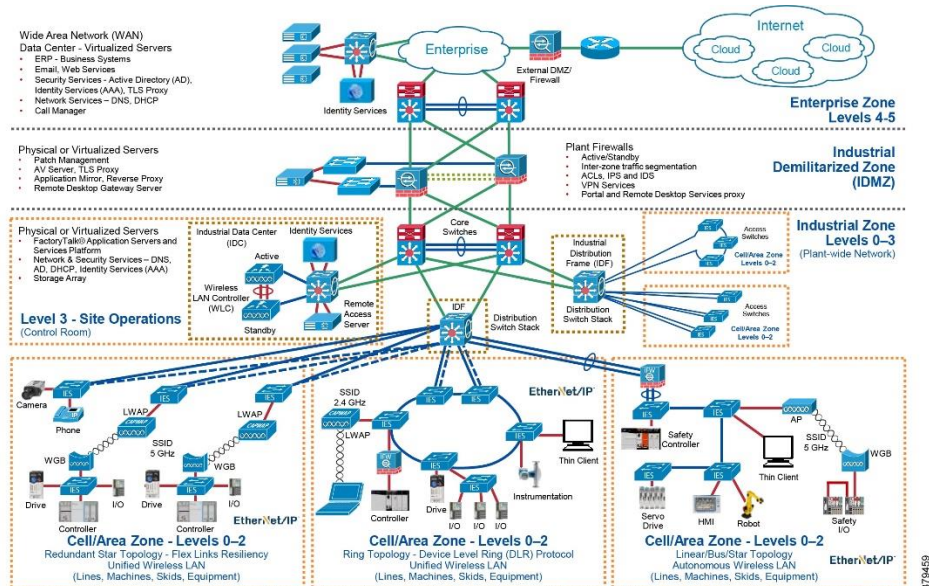
The Industrial Revolution 4.0 has changed the way modern factories operate. The concept of Smart Factory, which automatically connects all production systems, is now increasingly being implemented. The key lies in Industrial Internet of Things (IIoT) technology, which enables all machines and equipment in a factory to connect and share data directly. However, the success of this technology has given rise to a new problem: how to integrate IT (information technology) and OT (operational technology) systems in factories.

Until now, computer networks in offices (IT) and networks in production areas (OT) have operated separately. Offices place greater emphasis on data security and confidentiality, while factory floors require systems that run continuously with rapid response times. Many IIoT projects have failed because their network infrastructure cannot integrate these two different systems. A McKinsey report (2023) states that only 26% of factories have successfully implemented IIoT due to network infrastructure issues. IDC (2022) also notes that 42% of digital transformation failures in the manufacturing sector are caused by inadequate network design.

The problem is further complicated by the fact that most IT personnel do not understand factory systems, and vice versa. As a result, many factories still rely on manual methods to connect data from the office to production.

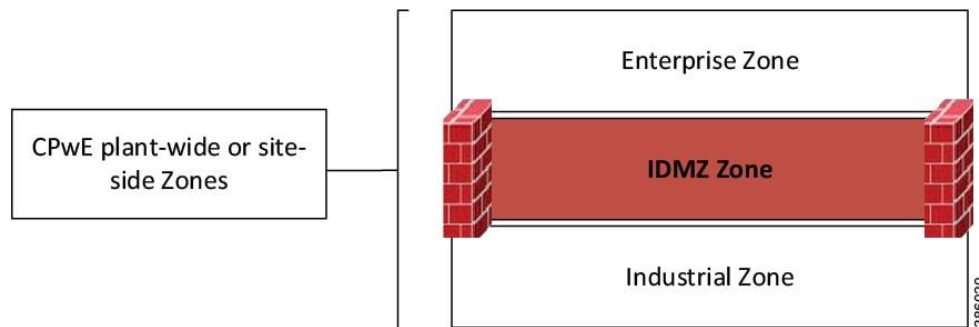
To address this issue, large companies such as Cisco and Rockwell Automation have created a standard called Converged Plantwide Ethernet (CPwE). This is not a finished product, but rather a tested and proven design guide for building reliable, secure, and scalable factory networks.

A complete CPwE architecture has 5 levels (Levels 0-4/5), ranging from sensors on the factory floor to servers in the company cloud.



Although this 5-level model is very detailed, the essence of CPwE actually lies in zone division (segmentation). The idea is simple: divide the network into three main zones, namely the

Enterprise Zone (office area), Industrial Zone (factory area), and a buffer zone in the middle called the Industrial Demilitarized Zone or IDMZ.



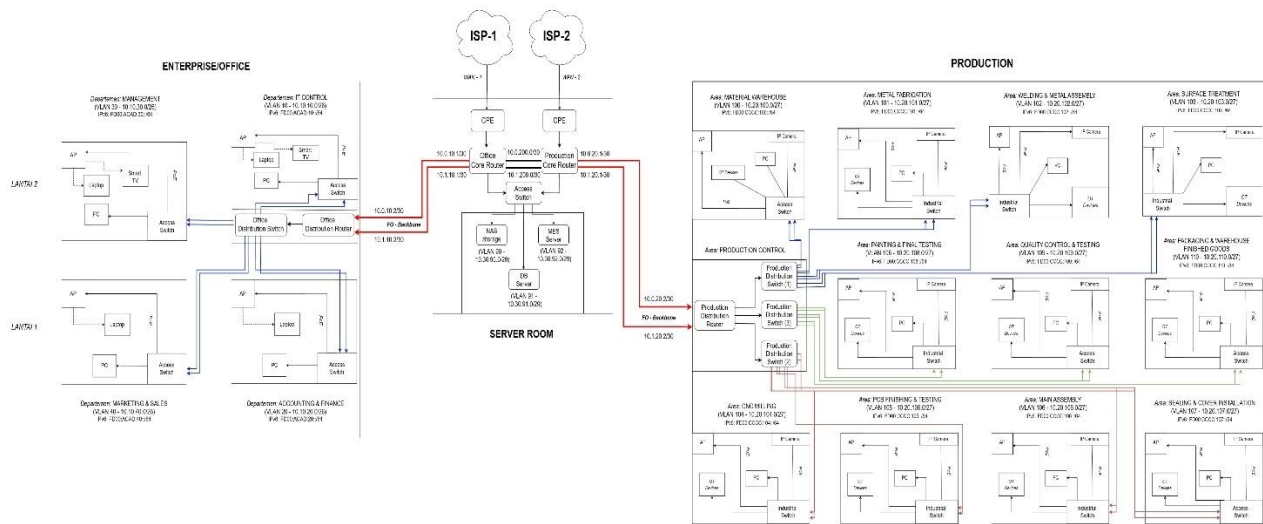
This zoning has proven to be effective. A study by Siemens (2021) shows that factories that implement VLAN segmentation and edge computing have seen their productivity increase by up to 28% and machine downtime reduced by 35%.

This project aims to design a network infrastructure for medium-sized factories using the 3-zone concept from CPwE. The design maps the Enterprise Zone for IT and Accounting, IDMZ as the server room, and the Industrial Zone for the production control area.

In line with the project's focus, this design only focuses on network infrastructure without covering the configuration or programming of specific Operation Technology (OT) devices such as PLC, HMI, or SCADA. In addition, the topology design is more focused on logical network architecture, so that physical aspects such as device resistance to the environment (M.I.C.E.), grounding, and UPS are indeed important in the real world, but are not discussed in the scope of this simulation.

2. TOPOLOGY DESIGN

2.1 Topology Design



In the designed topology, the Office section consists of 4 departments and Production consists of 11 areas. In each Office department and Production area, there is one managed switch or industrial switch that provides VLAN access to client devices such as PCs, Access Points, and other devices. This switch also performs trunking to interfaces connected to the distribution switch. To prevent Single Point of Failure (SPOF) issues, each managed switch is connected to the distribution switch using 2 links for redundancy.

The distribution switch is then connected to the office router to receive all trunk traffic from the router. Each router in the office and production is connected to the fiber optic backbone path with 2 links that have different IPs for physical redundancy. Fiber optics are used for the backbone link because of their durability in outdoor environments and their ability to cover long distances without signal degradation. In addition, because they do not conduct electricity, fiber optics are much safer from interference that commonly occurs in high-voltage areas. Examples include electrical interference, ground loops, or lightning strikes that can damage network devices.

In the server room, there are two core routers responsible for receiving and distributing traffic to the office and production areas. These two core routers are also interconnected using two physical links as redundancy. Both core routers are connected to a switch that accommodates the company's internal servers, such as NAS Storage, DB Server, and MES Server. The connection to both core routers is made because these servers are shared resources used by the office and production. For the internet connection, 2 ISPs are used as a load balancing mechanism as well as failover.

2.2 System Limitations

In addition to the adjustments to the ISP topology above, there are several other limitations applied to the implementation of this simulation due to limitations in software features (software image) and hardware resources:

1. **Layer 2 redundancy via STP (not LACP):** Redundant connections between switches use the Spanning Tree protocol (Active/Standby mode). This is because the switch image used in GNS3 does not fully support the LACP/EtherChannel feature.
2. **EtherChannel Limitations on Routers:** The initial design planned to implement LACP on the link from the Office/Production Router to the Distributed Switch for redundancy. However, this could not be implemented because the image used was a pure router that did not support Layer 2 EtherChannel features like a Layer 3 Switch. Therefore, the connection still uses a dual link but without LACP aggregation.
3. **Internet Access in the Production Zone:** Referring to the CPwE standard, devices in the production zone (OT) should be isolated and not allowed to access the internet for data security reasons. However, in this simulation, internet access in the production zone is opened on a limited basis for testing purposes. This is done because wireless devices are simulated using the built-in GNS3 switch, which has limited features (cannot ping), so connectivity needs to be tested directly through internet access from the end-device.
4. **Absence of Dedicated Firewall Devices:** The ideal security design includes a dedicated firewall between the ISP and the Core Router. However, this component was omitted due to the lack of a license for an enterprise firewall image and the limited computing resources (RAM/CPU) of the laptop to run an open source image (such as VyOS). Instead, security and traffic filtering functions are implemented using ACL (Access Control List) on the router.
5. **Server Simulation:** Server devices (NAS, DB, MES) are implemented using lightweight virtual nodes (VPCS/Router) that only serve to verify IP connectivity and validate ACL rules, without running real application services (such as SQL or Web Server services).

2.3 IP Address Allocation

Location	Network Name (Department/Area)	VLAN ID	IPv4 Subnet	Ipv6 Subnet
Office	IT Control	10	10.10.10.0/26	FD00:ACAD:10::/64
Office	Accounting & Finance	20	10.10.20.0/26	FD00:ACAD:20::/64
Office	Management	30	10.10.30.0/26	FD00:ACAD:30::/64
Office	Marketing & Sales	40	10.10.40.0/26	FD00:ACAD:40::/64
Server	NAS Storage	90	10.30.90.0/29	-
Server	DB Server	91	10.30.91.0/29	-
Server	MES Server	92	10.30.92.0/29	-
Production	Material Warehouse	100	10.20.100.0/27	FD00:CCCC:100::/64
Production	Metal Fabrication	101	10.20.101.0/27	FD00:CCCC:101::/64
Production	Welding & Metal Assembly	102	10.20.102.0/27	FD00:CCCC:102::/64
Production	Surface Treatment	103	10.20.103.0/27	FD00:CCCC:103::/64
Production	CNC Milling	104	10.20.104.0/27	FD00:CCCC:104::/64
Production	PCB Finishing & Testing	105	10.20.105.0/27	FD00:CCCC:105::/64

Production	Main Assembly	106	10.20.106.0/27	FD00:CCCC:106::/64
Production	Sealing & Cover Installation	107	10.20.107.0/27	FD00:CCCC:107::/64
Production	Painting & Final Testing	108	10.20.108.0/27	FD00:CCCC:108::/64
Production	Quality Control & Testing	109	10.20.109.0/27	FD00:CCCC:109::/64
Production	Packaging & Warehouse Finished Goods	110	10.20.110.0/27	FD00:CCCC:110::/64

Connection From	Connection To	Link #	IPv4 Subnet	IP Address Side 1	IP Address Side 2
Office Core Router	Office Router	Link 1	10.0.10.0/30	10.0.10.1	10.0.10.2
Office Core Router	Office Router	Link 2	10.1.10.0/30	10.1.10.1	10.1.10.2
Production Core Router	Production Router	Link 1	10.0.20.0/30	10.0.20.1	10.0.20.2
Production Core Router	Production Router	Link 2	10.1.20.0/30	10.1.20.1	10.1.20.2
Office Core Router	Production Core Router	Link 1	10.0.200.0/30	10.0.200.1	10.0.200.2
Office Core Router	Production Core Router	Link 2	10.1.200.0/30	10.1.200.1	10.1.200.2

3. TESTING

3.1 DHCP Testing and IP Allocation

Testing was conducted on the client side to ensure that the DHCP Server was functioning correctly and able to provide IP addresses according to the specified configuration.

1. The first test was conducted on all clients in the Production area. The results showed that IP allocation was in accordance with the DHCP Pool configuration and the distribution of VLAN addresses in each area.

Metal Fabrication

```
PC5> ip dhcp -r
DDORA IP 10.20.101.2/27 GW 10.20.101.1
PC5>
```

Welding & Metal Assembly

```
PC12> ip dhcp -r
DDORA IP 10.20.102.2/27 GW 10.20.102.1
PC12>
```

Material Warehouse

```
PC6> ip dhcp -r
DDORA IP 10.20.100.2/27 GW 10.20.100.1
PC6>
```

2. The second test was conducted on all clients in the Office area. The results showed that the IP allocation was in accordance with the DHCP Pool configuration and the VLAN address distribution in each area.

IT Controll

```
PC1> ip dhcp -r
DORA IP 10.10.10.2/26 GW 10.10.10.1
PC1>
```

Accounting & Finance

```
PC3> ip dhcp -r
DORA IP 10.10.20.2/26 GW 10.10.20.1

PC3> █
```

3. Static IP address allocation on each server.

DB-Server

```
DB-SERVER> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
DB-SERV10.30.91.3/29 10.30.91.6 00:50:79:66:68:0b 20272 127.0.0.1:20273
fe80::250:79ff:fe66:680b/64

DB-SERVER> █
```

NAS-Storage

```
NAS-STORAGE> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
NAS-STO10.30.90.3/29 10.30.90.6 00:50:79:66:68:0a 20270 127.0.0.1:20271
fe80::250:79ff:fe66:680a/64

NAS-STORAGE> █
```

MES-Server

```
MES-SERVER> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
MES-SER10.30.92.3/29 10.30.92.6 00:50:79:66:68:0c 20274 127.0.0.1:20275
fe80::250:79ff:fe66:680c/64
fd00:acad:92::3/64

MES-SERVER> █
```

3.2 Division Ping Testing and Access List Implementation

Testing was conducted in every department or area in both divisions, Office and Production, to ensure that all connections between VLANs were functioning in accordance with the access list rules that had been implemented. The purpose of this testing was to verify that each area could only access resources that were permitted by the network policy.

1. The first test was conducted in the IT Control department in the Office division. The results showed that VLAN 10 (IT Control) could connect to the server and to all areas in Production in accordance with the applicable access list provisions.

Test ping to servers

```
PC1> sh

NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PORT
PC1       10.10.10.2/26  10.10.10.1   00:50:79:66:68:0d  20284  127.0.0.1:20285
          fe80::250:79ff:fe66:680d/64
          fd00::acad:10:0:2050:79ff:fe66:680d/64  eui-64

PC1> ping 10.30.90.3

64 bytes from 10.30.90.3 icmp_seq=1 ttl=62 time=33.641 ms
64 bytes from 10.30.90.3 icmp_seq=2 ttl=62 time=29.435 ms
64 bytes from 10.30.90.3 icmp_seq=3 ttl=62 time=20.717 ms
^C
PC1> ping 10.30.91.3

64 bytes from 10.30.91.3 icmp_seq=1 ttl=62 time=449.116 ms
64 bytes from 10.30.91.3 icmp_seq=2 ttl=62 time=86.570 ms
64 bytes from 10.30.91.3 icmp_seq=3 ttl=62 time=52.239 ms
^C
PC1> ping 10.30.92.3

64 bytes from 10.30.92.3 icmp_seq=1 ttl=62 time=834.734 ms
64 bytes from 10.30.92.3 icmp_seq=2 ttl=62 time=37.487 ms
64 bytes from 10.30.92.3 icmp_seq=3 ttl=62 time=38.192 ms
^C
```

Test ping to production

```
PC1> ping 10.20.100.2

64 bytes from 10.20.100.2 icmp_seq=1 ttl=60 time=308.135 ms
64 bytes from 10.20.100.2 icmp_seq=2 ttl=60 time=85.765 ms
^C
PC1> ping 10.20.101.2

64 bytes from 10.20.101.2 icmp_seq=1 ttl=60 time=213.151 ms
64 bytes from 10.20.101.2 icmp_seq=2 ttl=60 time=140.426 ms
^C[[A
PC1> ping 10.20.102.2

64 bytes from 10.20.102.2 icmp_seq=1 ttl=60 time=353.167 ms
64 bytes from 10.20.102.2 icmp_seq=2 ttl=60 time=148.857 ms
64 bytes from 10.20.102.2 icmp_seq=3 ttl=60 time=112.963 ms
^C
```

2. The second test was conducted in the Accounting and Finance department in the Office division. The results showed that VLAN 20 (Accounting) could only connect to the DB server.

Test ping to servers

```
PC3> ping 10.30.90.3

*10.10.20.1 icmp_seq=1 ttl=255 time=50.459 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.20.1 icmp_seq=2 ttl=255 time=332.868 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.20.1 icmp_seq=3 ttl=255 time=53.969 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC3> ping 10.30.91.3

64 bytes from 10.30.91.3 icmp_seq=1 ttl=62 time=892.224 ms
64 bytes from 10.30.91.3 icmp_seq=2 ttl=62 time=15.645 ms
64 bytes from 10.30.91.3 icmp_seq=3 ttl=62 time=48.057 ms
^C
PC3> ping 10.30.92.3

*10.10.20.1 icmp_seq=1 ttl=255 time=137.194 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.20.1 icmp_seq=2 ttl=255 time=267.900 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.20.1 icmp_seq=3 ttl=255 time=621.988 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC3> []
```

Test ping to production

```
PC3>
PC3> ping 10.20.100.2

*10.10.20.1 icmp_seq=1 ttl=255 time=299.516 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.20.1 icmp_seq=2 ttl=255 time=230.178 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC3> ping 10.20.101.2

*10.10.20.1 icmp_seq=1 ttl=255 time=75.529 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.20.1 icmp_seq=2 ttl=255 time=152.723 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC3> ping 10.20.102.2

*10.10.20.1 icmp_seq=1 ttl=255 time=93.320 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.10.20.1 icmp_seq=2 ttl=255 time=62.628 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC3> []
```

3. The third test was conducted on all areas in the Production division because the access list rules were the same. The results showed that all areas could only connect to the DB server and MES Server.

Test ping Area 1 to servers

```
PC6> ping 10.30.90.3
*10.20.100.1 icmp_seq=1 ttl=255 time=35.843 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.100.1 icmp_seq=2 ttl=255 time=4.807 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC6> ping 10.30.91.3
84 bytes from 10.30.91.3 icmp_seq=1 ttl=61 time=480.171 ms
84 bytes from 10.30.91.3 icmp_seq=2 ttl=61 time=282.309 ms
^C
PC6> ping 10.30.92.3
84 bytes from 10.30.92.3 icmp_seq=1 ttl=61 time=611.350 ms
84 bytes from 10.30.92.3 icmp_seq=2 ttl=61 time=47.619 ms
^C
PC6> █
```

Test ping Area 1 to office

```
^C
PC6> ping 10.10.10.2
*10.20.100.1 icmp_seq=1 ttl=255 time=52.579 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.100.1 icmp_seq=2 ttl=255 time=16.161 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC6> ping 10.10.20.2
*10.20.100.1 icmp_seq=1 ttl=255 time=14.307 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.100.1 icmp_seq=2 ttl=255 time=18.552 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC6> █
```

Test ping Area 2 to servers

```
PC5> ping 10.30.90.3
*10.20.101.1 icmp_seq=1 ttl=255 time=55.244 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.101.1 icmp_seq=2 ttl=255 time=54.495 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC5> ping 10.30.91.3
84 bytes from 10.30.91.3 icmp_seq=1 ttl=61 time=26.530 ms
84 bytes from 10.30.91.3 icmp_seq=2 ttl=61 time=91.066 ms
^C
PC5> ping 10.30.92.3
84 bytes from 10.30.92.3 icmp_seq=1 ttl=61 time=36.262 ms
84 bytes from 10.30.92.3 icmp_seq=2 ttl=61 time=93.055 ms
^C
PC5> █
```

Test ping Area 2 to office

```
^C
PC5> ping 10.10.10.2
*10.20.101.1 icmp_seq=1 ttl=255 time=48.897 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.101.1 icmp_seq=2 ttl=255 time=15.924 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC5> ping 10.10.20.2
*10.20.101.1 icmp_seq=1 ttl=255 time=16.078 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.101.1 icmp_seq=2 ttl=255 time=32.999 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC5> █
```

Test ping Area 3 to servers

```
PC12> ping 10.30.90.3
*10.20.102.1 icmp_seq=1 ttl=255 time=30.462 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.102.1 icmp_seq=2 ttl=255 time=2.971 ms (ICMP type:3, code:13, Communication administratively prohibited)
^C
PC12> ping 10.30.91.3
84 bytes from 10.30.91.3 icmp_seq=1 ttl=61 time=115.458 ms
84 bytes from 10.30.91.3 icmp_seq=2 ttl=61 time=64.721 ms
^C
PC12> ping 10.30.92.3
84 bytes from 10.30.92.3 icmp_seq=1 ttl=61 time=132.245 ms
84 bytes from 10.30.92.3 icmp_seq=2 ttl=61 time=53.632 ms
^C
PC12> █
```

Test ping Area 3 to office

```
PC12> ping 10.10.10.2
*10.20.102.1 icmp_seq=1 ttl=255 time=51.438 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.102.1 icmp_seq=2 ttl=255 time=31.743 ms (ICMP type:3, code:13, Communication administratively prohibited)
PC12> ping 10.10.20.2
*10.20.102.1 icmp_seq=1 ttl=255 time=47.165 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.20.102.1 icmp_seq=2 ttl=255 time=38.203 ms (ICMP type:3, code:13, Communication administratively prohibited)
PC12>
```

3.3 Testing SLACC IPv6

Testing was conducted in every department or area in both divisions, Office and Production.

1. The first test was conducted in the Office division. The results showed that VLAN 10 (IT Control) and VLAN 20 (Accounting) obtained IPv6 automatically.

IT Control

```
PC1> ip auto
GLOBAL SCOPE      : fd00:acad:10:0:2050:79ff:fe66:680d/64
ROUTER LINK-LAYER : 0c:77:c7:a3:00:02
```

Accounting

```
PC3> ip auto
GLOBAL SCOPE      : fd00:acad:20:0:2050:79ff:fe66:6802/64
ROUTER LINK-LAYER : 0c:77:c7:a3:00:02
```

2. The second test was conducted in the Production division. The results showed that VLAN 100 (Material Warehouse), VLAN 101 (Metal Fabrication), and VLAN 102 (Welding & Metal Assembly) obtained IPv6 automatically.

Material Warehouse

```
PC6> ip auto
GLOBAL SCOPE      : fd00:cccc:100:0:2050:79ff:fe66:6805/64
ROUTER LINK-LAYER : 0c:92:4e:3c:00:01
```

```
PC6>
```

Metal Fabrication

```
PC5> ip auto
GLOBAL SCOPE      : fd00:cccc:101:0:2050:79ff:fe66:6806/64
ROUTER LINK-LAYER : 0c:92:4e:3c:00:04
```

```
PC5>
```

Welding & Metal Assembly

```
PC12> ip auto
GLOBAL SCOPE      : fd00:cccc:102:0:2050:79ff:fe66:6808/64
ROUTER LINK-LAYER : 0c:92:4e:3c:00:06

PC12> █
```

3.4 Testing Tunnel GRE

This test was conducted on the Host on both the Office and Production sides. The purpose was to verify whether the configured GRE Tunnel was actually functioning to route IPv6 traffic between the two locations.

1. The first test was conducted from the Office side. The result was successful, where VLAN 10 (IT Control) and VLAN 20 (Accounting) were proven to be able to connect to all areas in Production using the IPv6 network.

IT Control

```
PC1> trace fd00:cccc:100:0:2050:79ff:fe66:6805

trace to fd00:cccc:100:0:2050:79ff:fe66:6805, 64 hops max
 1 fd00:acad:10::1  123.625 ms  31.487 ms  27.249 ms
 2 fd00:1111:1::2  175.590 ms  704.939 ms  559.857 ms
 3 fd00:cccc:100:0:2050:79ff:fe66:6805  168.912 ms  127.287 ms  68.300 ms

PC1> trace fd00:cccc:101:0:2050:79ff:fe66:6806

trace to fd00:cccc:101:0:2050:79ff:fe66:6806, 64 hops max
 1 fd00:acad:10::1  91.844 ms  28.023 ms  13.502 ms
 2 fd00:1111:1::2  299.667 ms  146.087 ms  843.025 ms
 3 * * 316.144 ms

PC1> trace fd00:cccc:101:0:2050:79ff:fe66:6806

trace to fd00:cccc:101:0:2050:79ff:fe66:6806, 64 hops max
 1 fd00:acad:10::1  77.038 ms  19.106 ms  17.741 ms
 2 fd00:1111:1::2  423.878 ms  570.427 ms  99.698 ms
 3 fd00:cccc:101:0:2050:79ff:fe66:6806  102.235 ms  111.069 ms  78.977 ms

PC1> trace fd00:cccc:102:0:2050:79ff:fe66:6808

trace to fd00:cccc:102:0:2050:79ff:fe66:6808, 64 hops max
 1 fd00:acad:10::1  202.997 ms  31.094 ms  30.919 ms
 2 fd00:1111:1::2  444.747 ms  230.547 ms  967.103 ms
 3 fd00:cccc:102:0:2050:79ff:fe66:6808  263.684 ms  98.998 ms  95.190 ms

PC1> █
```

Accounting

```
PC3> trace fd00:cccc:100:0:2050:79ff:fe66:6805

trace to fd00:cccc:100:0:2050:79ff:fe66:6805, 64 hops max
 1 fd00:acad:20::1 281.000 ms 25.821 ms 18.837 ms
 2 fd00:1111:1::2 215.931 ms 450.185 ms 464.492 ms
 3 fd00:cccc:100:0:2050:79ff:fe66:6805 551.579 ms 109.313 ms 103.794 ms

PC3> trace fd00:cccc:101:0:2050:79ff:fe66:6806

trace to fd00:cccc:101:0:2050:79ff:fe66:6806, 64 hops max
 1 fd00:acad:20::1 282.180 ms 32.614 ms 12.128 ms
 2 fd00:1111:1::2 299.712 ms 660.493 ms 514.042 ms
 3 fd00:cccc:101:0:2050:79ff:fe66:6806 170.844 ms 79.787 ms 84.398 ms

PC3> trace fd00:cccc:102:0:2050:79ff:fe66:6808

trace to fd00:cccc:102:0:2050:79ff:fe66:6808, 64 hops max
 1 fd00:acad:20::1 321.859 ms 16.085 ms 13.647 ms
 2 fd00:1111:1::2 428.844 ms 537.506 ms 525.029 ms
 3 fd00:cccc:102:0:2050:79ff:fe66:6808 90.930 ms 100.704 ms 110.829 ms

PC3> █
```

2. The second test was conducted from the Production side. The results were successful, proving that VLAN 100 (Material Warehouse), VLAN 101 (Metal Fabrication), and VLAN 102 (Welding & Metal Assembly) could connect to all areas in the Office using the IPv6 network.

Material Warehouse

```
PC6> trace fd00:acad:10:0:2050:79ff:fe66:680d

trace to fd00:acad:10:0:2050:79ff:fe66:680d, 64 hops max
 1 fd00:cccc:100::1 167.226 ms 29.082 ms 39.618 ms
 2 fd00:1111:1::1 250.223 ms 194.593 ms 457.265 ms
 3 fd00:acad:10:0:2050:79ff:fe66:680d 543.730 ms 264.052 ms 147.900 ms

PC6> trace fd00:acad:20:0:2050:79ff:fe66:6802

trace to fd00:acad:20:0:2050:79ff:fe66:6802, 64 hops max
 1 fd00:cccc:100::1 402.942 ms 26.453 ms 52.234 ms
 2 fd00:1111:1::1 554.340 ms 718.709 ms 562.421 ms
 3 fd00:acad:20:0:2050:79ff:fe66:6802 77.709 ms 144.201 ms 70.246 ms

PC6> █
```

Metal Fabrication

```
PC5> trace fd00:acad:10:0:2050:79ff:fe66:680d

trace to fd00:acad:10:0:2050:79ff:fe66:680d, 64 hops max
 1 fd00:cccc:101::1 530.948 ms 42.702 ms 82.532 ms
 2 fd00:1111:1::1 306.371 ms 536.333 ms 685.844 ms
 3 fd00:acad:10:0:2050:79ff:fe66:680d 108.834 ms 114.713 ms 219.247 ms

PC5> trace fd00:acad:20:0:2050:79ff:fe66:6802

trace to fd00:acad:20:0:2050:79ff:fe66:6802, 64 hops max
 1 fd00:cccc:101::1 332.673 ms 25.574 ms 18.348 ms
 2 fd00:1111:1::1 356.462 ms 527.131 ms 531.704 ms
 3 fd00:acad:20:0:2050:79ff:fe66:6802 571.530 ms 116.873 ms 208.757 ms

PC5> █
```

Welding & Metal Assembly

```
PC12> trace fd00:acad:10:0:2050:79ff:fe66:680d

trace to fd00:acad:10:0:2050:79ff:fe66:680d, 64 hops max
 1 fd00:cccc:102::1  259.788 ms  30.824 ms  37.007 ms
 2 fd00:1111:1::1   146.767 ms  683.114 ms  112.416 ms
 3 fd00:acad:10:0:2050:79ff:fe66:680d  154.326 ms  152.562 ms  95.699 ms

PC12> trace fd00:acad:20:0:2050:79ff:fe66:6802

trace to fd00:acad:20:0:2050:79ff:fe66:6802, 64 hops max
 1 fd00:cccc:102::1  205.146 ms  20.768 ms  31.851 ms
 2 fd00:1111:1::1   561.998 ms  826.045 ms  660.345 ms
 3 fd00:acad:20:0:2050:79ff:fe66:6802  258.433 ms  69.273 ms  178.888 ms

PC12> █
```

4. BIBLIOGRAPHY

Cisco, Panduit, & Rockwell Automation. (2023). *Physical Infrastructure for the Converged Plantwide Ethernet Architecture* (Publikasi No. ENET-TD020B-EN-P).

Pickard, J., Linn, J. B., Awojana, T. B., & Lunsford II, P. J. (2018). *Designing a Converged Plant-wide Ethernet/IP Lab for Hands-on Distance Learning: An Interdisciplinary Graduate Project*. 2018 ASEE Annual Conference & Exposition, Salt Lake City, UT, United States.

Santoso, I., Nursiaga, R., Firmansyah, H., Rantina, M., Asbari, M., & Santoso, G. (2025). Desain Sistem Jaringan Untuk Smart Factory Berbasis Industrial Internet of Things (iiot). *JAREKOM: Jurnal Jaringan dan Rekayasa Komputer*, 01(1), 74–80.