

INFORMATION NETWORK DESIGN

Project

ABSTRACT

ในยุคปัจจุบัน การดำเนินงานขององค์กรจำเป็นต้องให้ความสำคัญกับ ความปลอดภัยของข้อมูล และ ความเสถียรของระบบ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับธุรกิจ การออกแบบระบบเครือข่ายที่มีประสิทธิภาพจึงเป็นปัจจัยสำคัญในการลดความเสี่ยงต่าง ๆ ไม่ว่าจะเป็นการโจรตีจากภายนอกหรือปัญหาภายในองค์กร

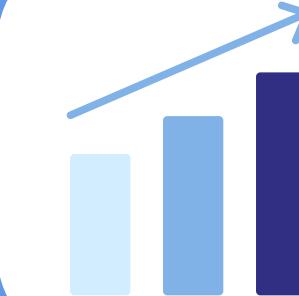


OBJECTIVE



COST EFFICIENCY

เพื่อออกราคาให้เหมาะสมตามงบประมาณ กับ
ขนาดเครือข่ายขององค์กร



PERFORMANCE

เพื่อให้เครือข่ายมีประสิทธิภาพสูงสุด
ลด Delay เพิ่ม Throughput



SECURITY

เพื่อป้องกันการเข้าถึงจากภายนอกที่ไม่ได้รับอนุญาต
ทำ Authen



IMPROVE SKILL

เพื่อฝึกฝนก้าวเข้าสู่การออกราคาเครือข่าย
อย่างถูกต้อง และ เหมาะสม

BUSINESS REQUIREMENT



BUSINESS REQUIREMENTS

HEADQUATER REQUIREMENTS

- Headquater มี 5 ชั้น 4 ห้อง 40 คนต่อชั้น รองรับการเติบโตของพนักงานในอีก 5 ปีที่ 15% รวมเป็น 46 คนต่อชั้น
- 3 application ทำงานที่ HQ (Inventory Management), (Human Resource Management), (VoIP)
- มีระบบ Access Control เพื่อทำ authentication

FACTORY REQUIREMENTS

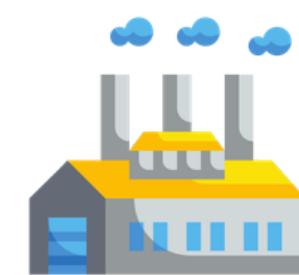
- Factory มี 2 ชั้น (ชั้น 1 มี 5 ห้อง) (ชั้น 2 มี 2 ห้อง) 29 คนต่อชั้นใน 15 ปี

Requirements ร่วมกันสองฝ่าย

- ออกแบบตามหลัก Information hiding, Modularity
- Low Latency, High Availability and Redundancy
- มี Next Gen Firewall ป้องกันการโจมตีจากภายนอก
- มีช่องทางออก Internet เพียง 1 ช่องทาง
- ระยะห่างระหว่าง HQ และ Factory คือ 1 km
- สามารถทำการติดต่อสื่อสารกันภายในและภายนอกองค์กรได้
- จำนวน user เพิ่มขึ้น 15 % ใน 5 ปี
- มี VPN ติดต่อกับ Partner ภายนอก



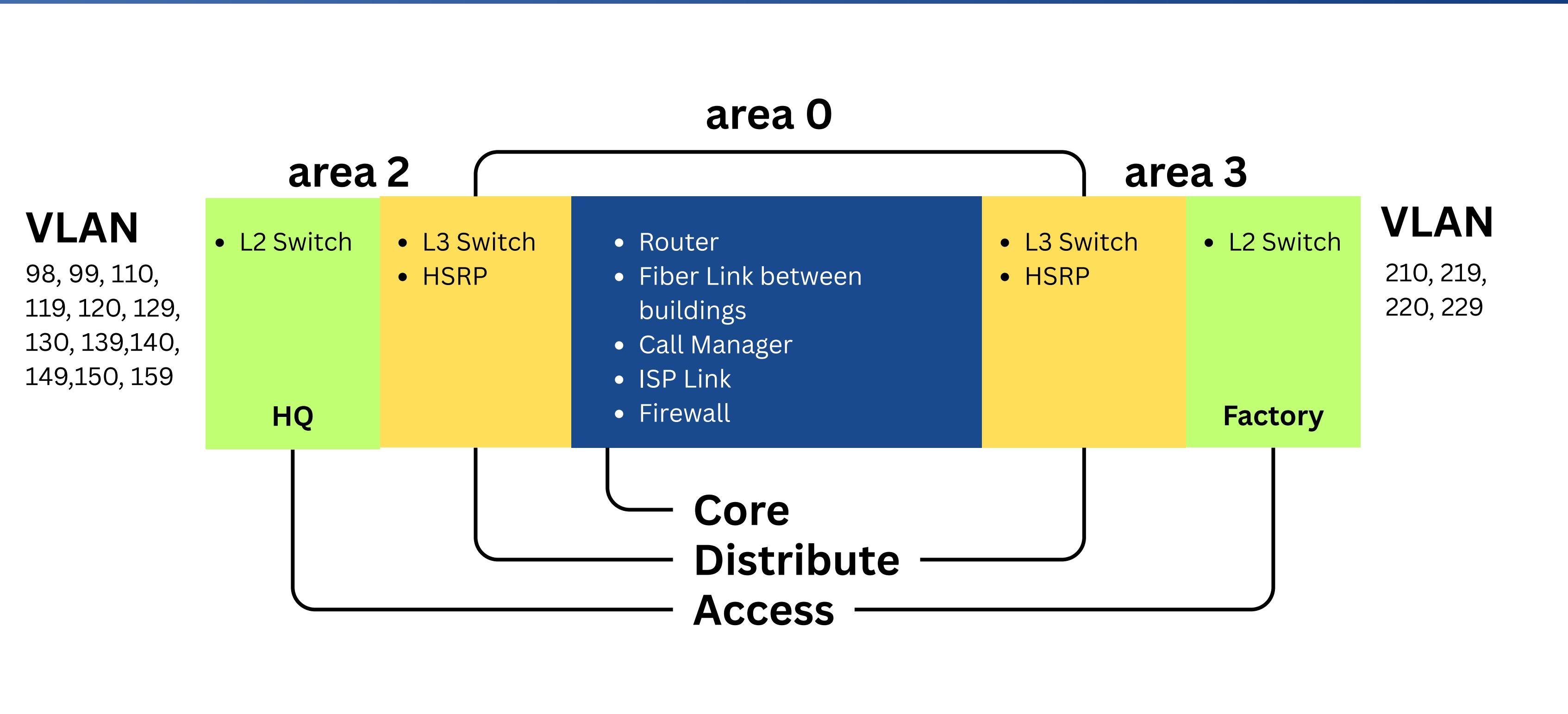
1 KM



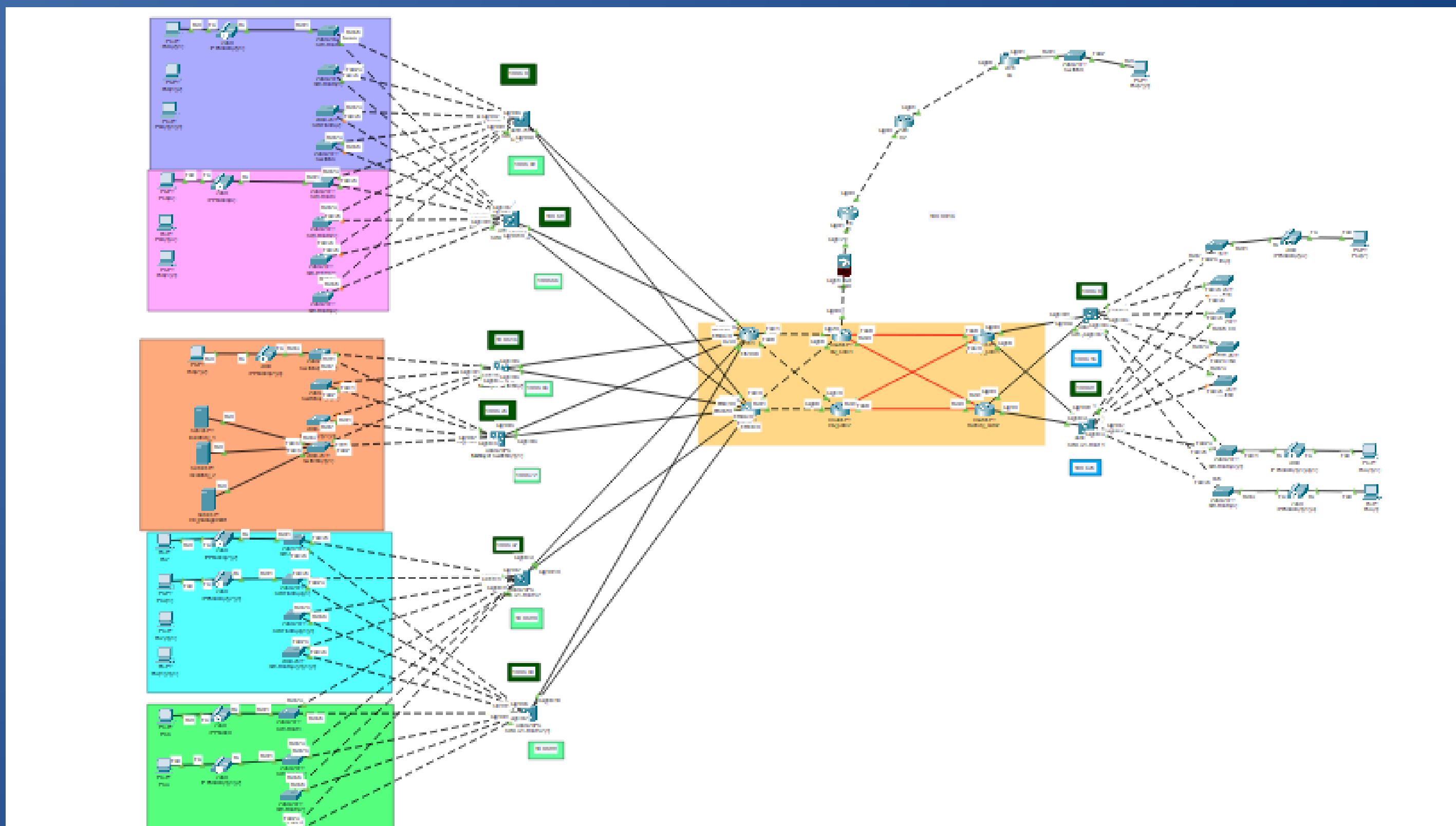
NETWORK DESIGN



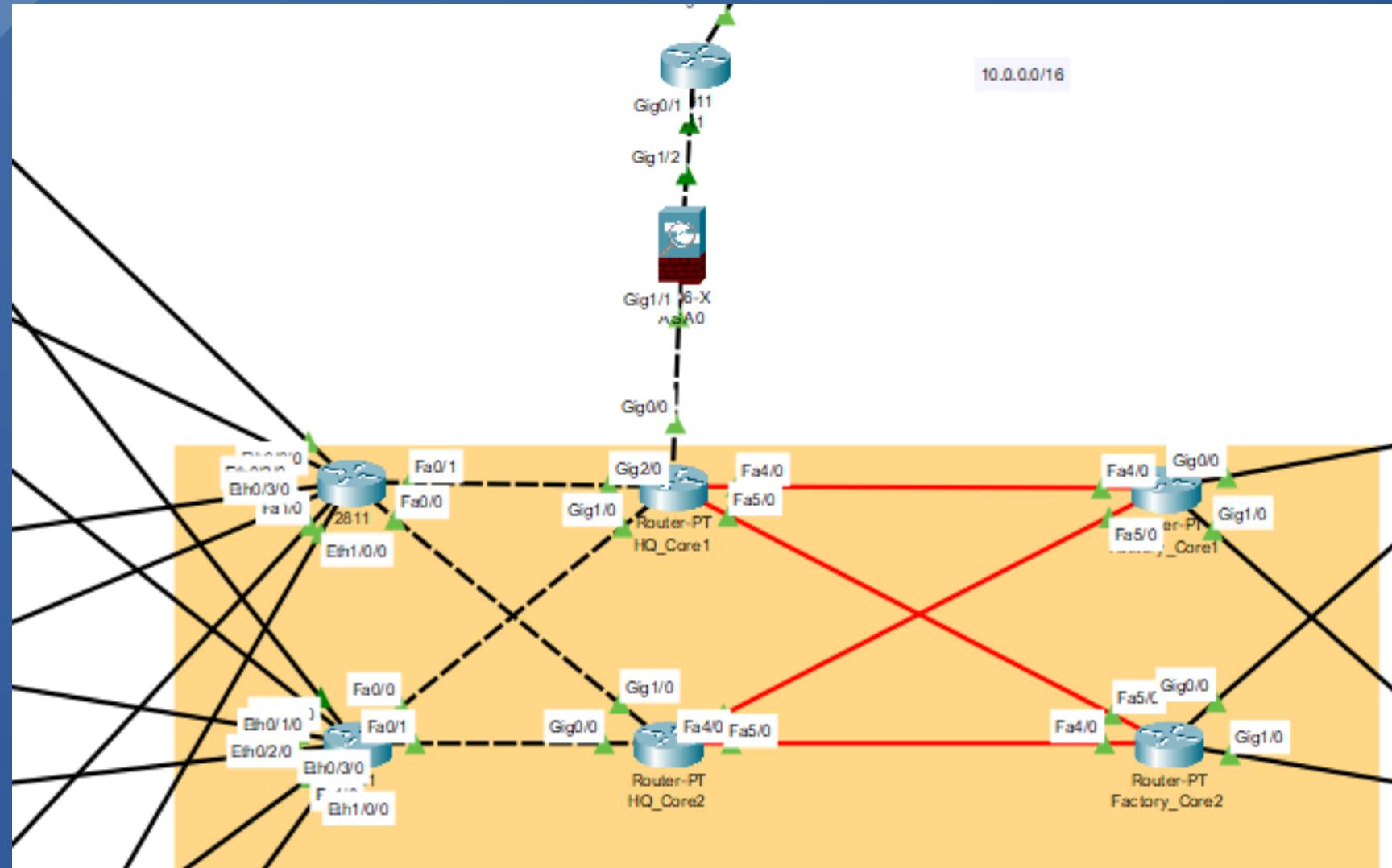
OVERVIEW DESIGN



LOGICAL DESIGN

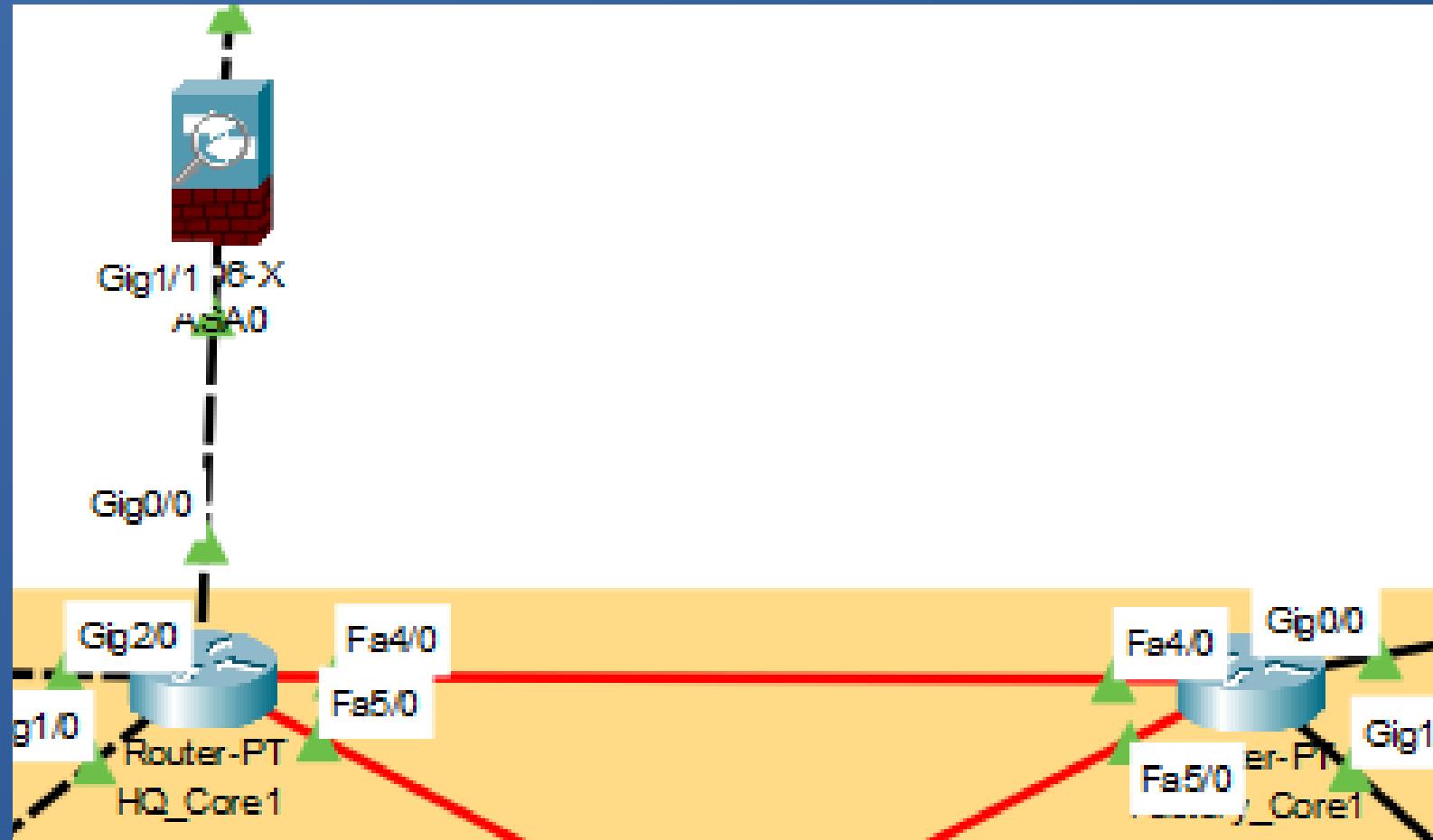


CORE NETWORK



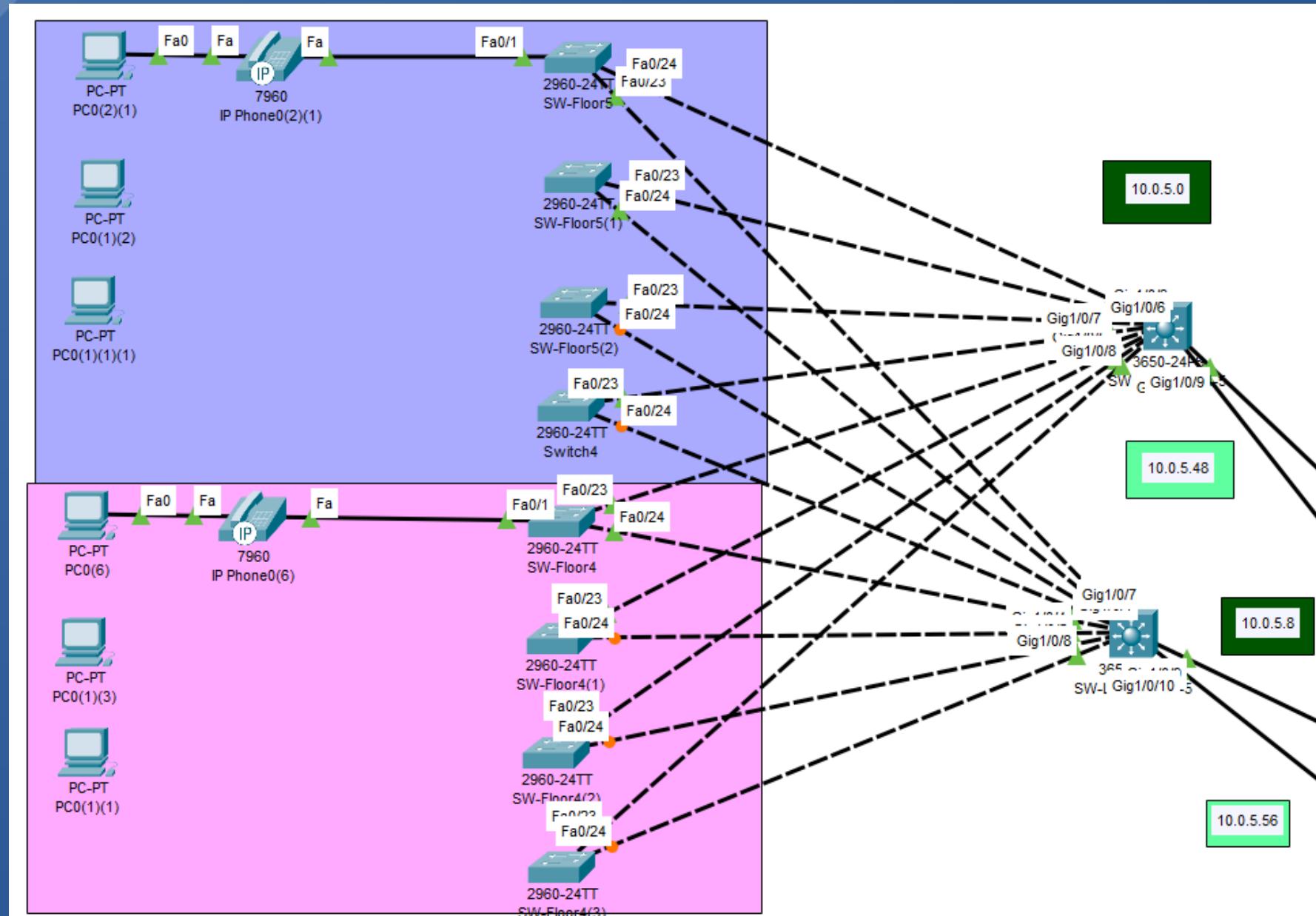
มีการติดตั้ง Router จำนวน 6 ตัวใน Core Layer
เพื่อสร้าง ระบบ Redundancy และ High Availability โดยใช้ OSPF เป็น Routing Protocol
เพื่อแบ่งเครือข่ายออกเป็น หลาย Area ซึ่งช่วยลด
ภาระในการประมวลผลเส้นทางและเพิ่มประสิทธิภาพ
ในการทำงานของเครือข่าย

CORE NETWORK



การออก Internet ในองค์กรเราออกผ่าน Core Layer โดยมีการเช่า link ออก Internet เพียงช่องเดียว และ มีการใช้ Firewall ไว้คุยควบคุมการเข้าถึงเครือข่ายระหว่างภายใน และภายนอก โดยออกผ่านทาง Headquarter

DISTRIBUTION LAYER



ที่ชั้น Distribution Layer มีการใช้ L3 switch 2 ตัว ต่อ 2 ชั้นใน Headquarters และ มีการกำ HSRP เพื่อป้องกันกรณีที่อุปกรณ์เกิดความเสียหาย จะยัง มีอุปกรณ์สำรองทำงานสำหรับ 2 ชั้นได้ดังเดิม

DISTRIBUTION LAYER

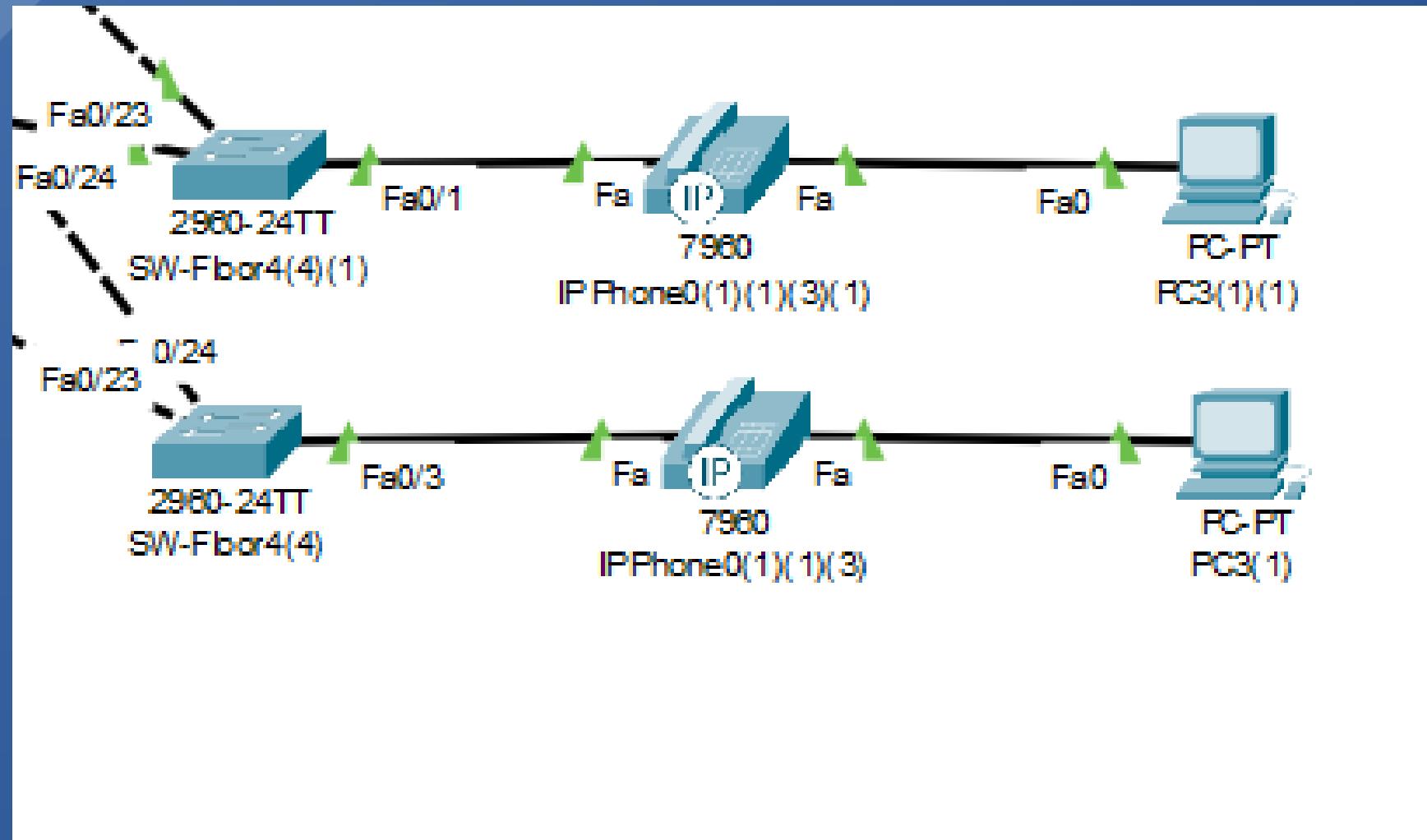
```
ip dhcp excluded-address 10.0.150.1 10.0.150.3
ip dhcp excluded-address 10.0.159.1 10.0.159.3
ip dhcp excluded-address 10.0.140.1 10.0.140.3
ip dhcp excluded-address 10.0.149.1 10.0.149.3
!
ip dhcp pool DATA4
 network 10.0.140.0 255.255.255.0
 default-router 10.0.140.1
ip dhcp pool VOICE4
 network 10.0.149.0 255.255.255.0
 default-router 10.0.149.1
 option 150 ip 10.0.5.81
ip dhcp pool DATA5
 network 10.0.150.0 255.255.255.0
 default-router 10.0.150.1
ip dhcp pool VOICES
ip dhcp pool VOIECS
 network 10.0.159.0 255.255.255.0
 default-router 10.0.159.1
 option 150 ip 10.0.5.81
```

มีการแบ่ง VLAN ระหว่างชั้นท็อปฟ์ (Headquarters (110, 120, 130, 140, 150) และ Factory (210, 220)

นอกจากนี้ยังมีการแบ่ง VLAN สำหรับ VoIP เป็น (119, 129, 139, 149, 159, 219, 229) และมีการทำ HSRP ที่ Interface VLAN ทุก VLAN

โดยที่ L3 switch จะทำการ DHCP และ分配 IP โดยให้แต่ละ VLAN มี IP pool เป็นของตัวเอง

ACCESS LAYER



มีการแบ่ง switch สำหรับห้องในชั้นต่างๆ โดย user จะมี PC และ IPhone อย่างละตัว โดยจะได้รับ Ip address จาก L3 switch โดยจะได้รับ 2 ip สำหรับ VoIP และ ip address สำหรับติดต่อสื่อสารกันในองค์กร

OSPF ROUTING

```
router ospf 1
log adjacency changes
network 10.0.3.8 0.0.0.7 area 0
network 10.0.2.24 0.0.0.7 area 0
network 10.0.2.16 0.0.0.7 area 0
```

ข้อดีของ OSPF และเหตุผลที่ควรเลือกใช้

เพราะว่า OSPF มีการใช้ Dijkstra's Algorithm ในการคำนวณเส้นทางที่สั้นที่สุด เมื่อพับการเปลี่ยนแปลงบนเครือข่าย เช่น Router มีปัญหาให้ใช้งานไม่ได้ ก็จะทำการคำนวณเส้นทางใหม่ได้อย่างรวดเร็วและยังป้องกันการปลอมแปลงเส้นทางได้อีกด้วย ก็ยังสามารถรองรับ IPv6 ได้ด้วย OSPFv3 เพื่อรองรับกับอนาคตที่จะเปลี่ยนไปใช้ IPv6

VOIP

```
telephony-service
max-ephones 30
max-dn 30
ip source-address 10.0.5.81 port 2000
auto assign 1 to 9
!
ephone-dn 1
number 1010
!
ephone-dn 2
number 1020
!
ephone-dn 3
number 1030
!
ephone-dn 4
number 1040
!
ephone-dn 5
number 1050
!
ephone-dn 6
number 1060
!
ephone-dn 7
number 1070
!
ephone-dn 8
number 2010
!
ephone-dn 9
number 2020
```



```
ip dhcp pool VOICE4
network 10.0.149.0 255.255.255.0
default-router 10.0.149.1
option 150 ip 10.0.5.81
```



ใช้ L3 Switch ในการแจก IP ให้ IP Phone ด้วยการ DHCP โดยมีการตั้ง option 150 เพื่อให้รับ configuration จาก call manager ซึ่งคือ router โดย router ที่กำหน้าที่เป็น call manager ต้องให้บริการกับ telephony-service ในการแจกจ่ายหมายเลขของแต่ละเครื่อง เราสามารถต่อ PC ถัดจาก IP phone เพื่อประชัยด interface ของ L2 Switch



IP ADDRESSING SCHEME

Data Vlan

- 10.0.[98,99,110,120,130,140,150,210,220].0/24

Voice Vlan

- 10.0.[119,129,139,149,159,219,229].0/24

Core

- 10.0.[2,3,5,6,7].0/24

Public

- 9.9.9.[1 - 10]/24

Private

- 10.0.0.0/16

VLAN EXAMPLE

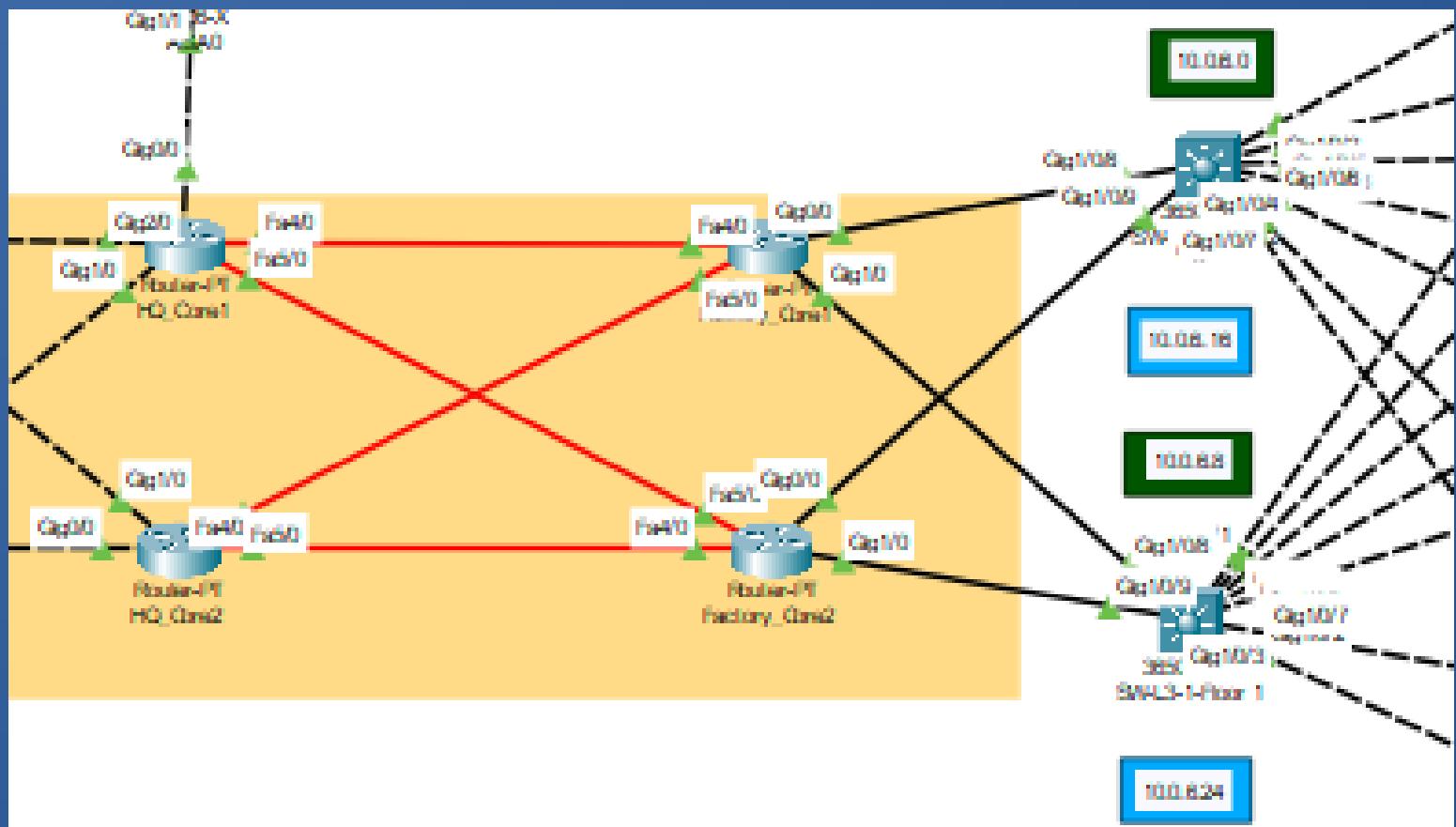
VLAN 110

- Virtual Gateway IP
 - 10.0.110. 1 /24
- Multilayer Switch SVI addresses
 - 10.0.110. [2,3] /24
- Host addresses
 - 10.0.110. [4-254] /24

A blue-tinted photograph of a modern skyscraper. The building features a curved glass facade with a grid pattern of windows. The sky is overcast with grey clouds.

**HOW THE DESIGN FULFILLS
THE REQUIREMENTS**

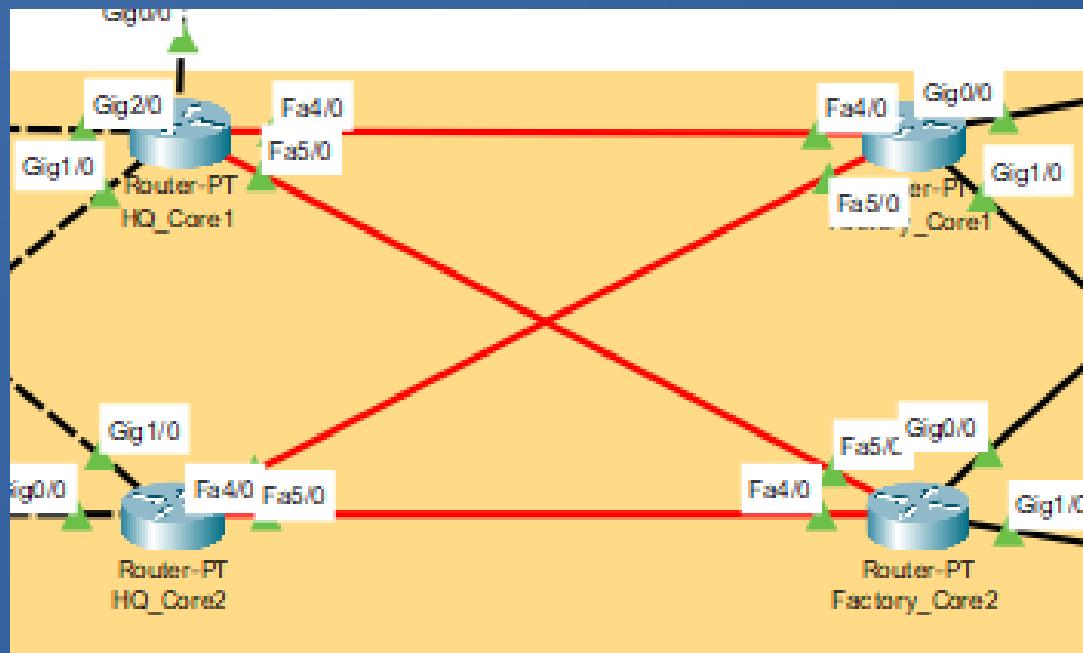
HIGH AVAILABILITY AND REDUNDANCY



มีการติดตั้งอุปกรณ์เครือข่ายสำรอง เช่น

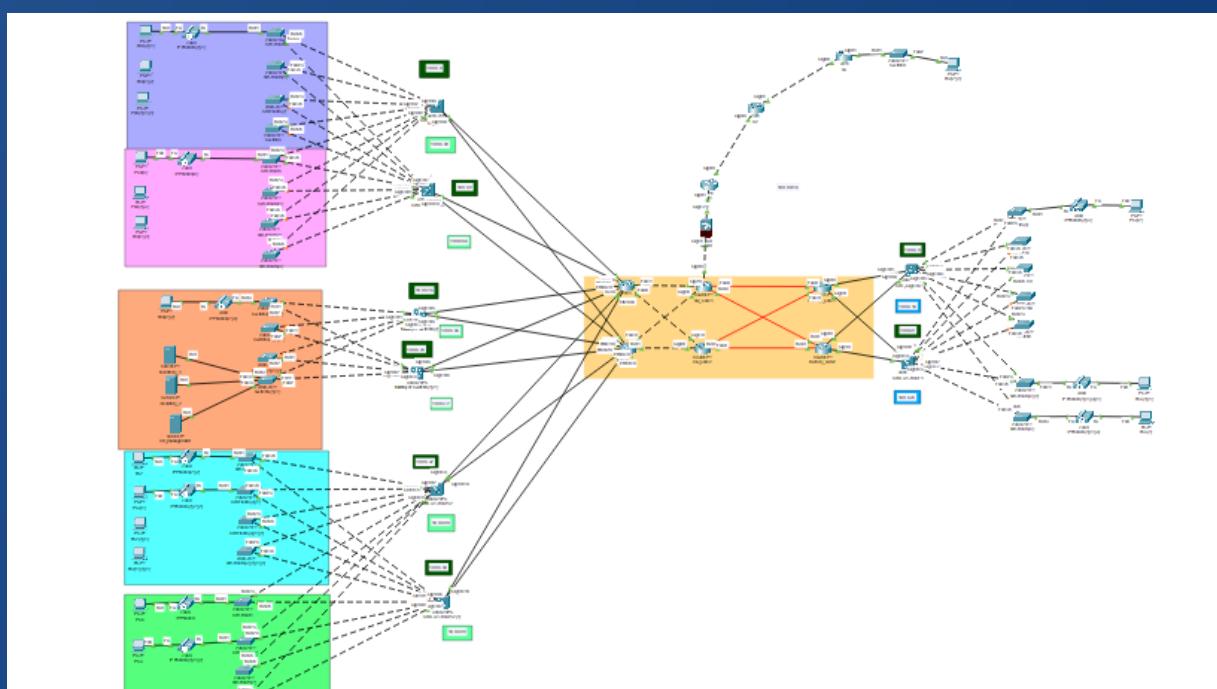
- router ใน core layer มี router หลักเส้นทางเพื่อป้องกันการเกิด single point of failure
- L3 switch ทำ HSRP เพื่อให้เกิดความพร้อมใช้งานในสถานการณ์ต่างๆ

LOW LATENCY



การเลือกใช้สาย Fiber กีมีความเร็วมากกว่าสาย Serial หรือ Coaxial กีมีระยะห่างกัน 1 Km ระหว่าง Headquarters และ Factory ช่วยลดการล่าช้าของการส่งข้อมูล ระหว่างอาคารที่ตั้งอยู่ห่างกัน

การลดจำนวน Hop ที่ไม่จำเป็น เพื่อลดการหน่วงจากการประมวลผลและการส่งต่อ (Forwarding Delay) เมื่อผ่าน network device ต่างๆ



SECURITY

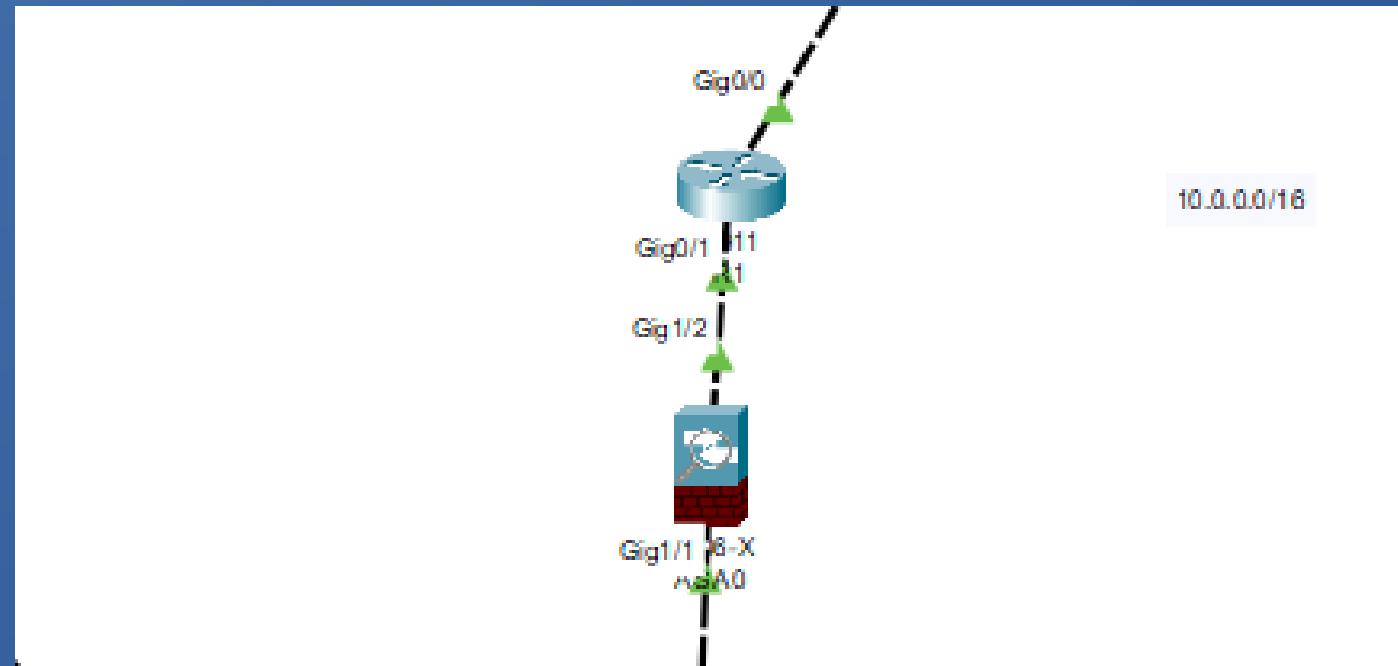
Access Control List

กำหนดสิทธิ์การเข้าถึง Server หรือเครือข่าย โดยระบุว่า Server ใน Topology นี้จะไม่สามารถออกไประยง ISP ได้

Firewall ASA เปิดใช้งานฟีเจอร์ป้องกันภัยคุกคาม IPS เพื่อตรวจจับและป้องกันการโจมตีที่อาจเกิดขึ้น และรองรับ VPN สำหรับการเชื่อมต่อ เพื่อให้การสื่อสารมีความปลอดภัยมากขึ้น

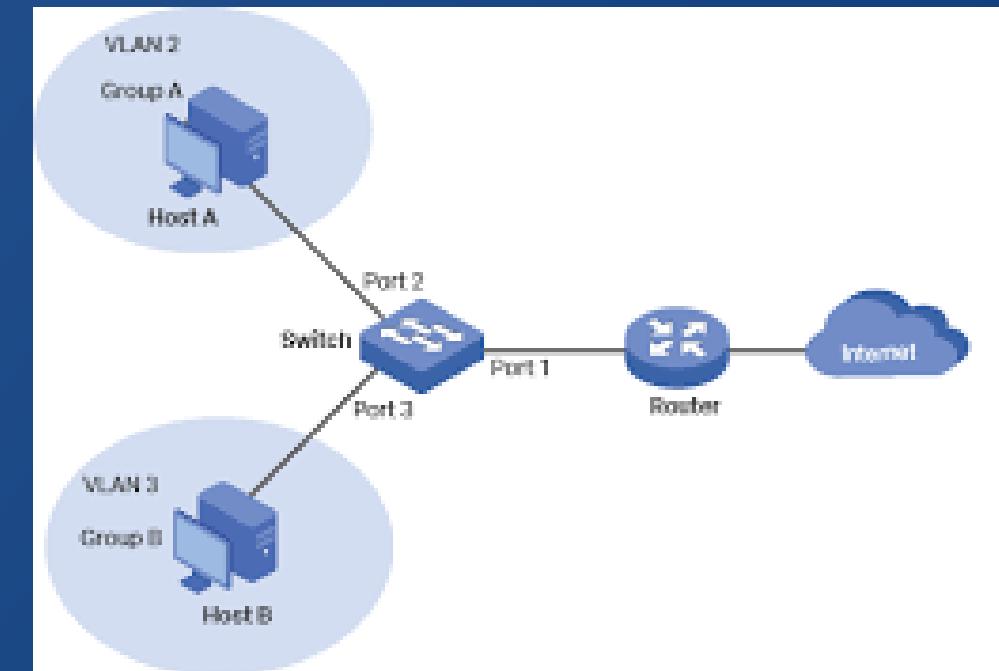


INFORMATION HIDING

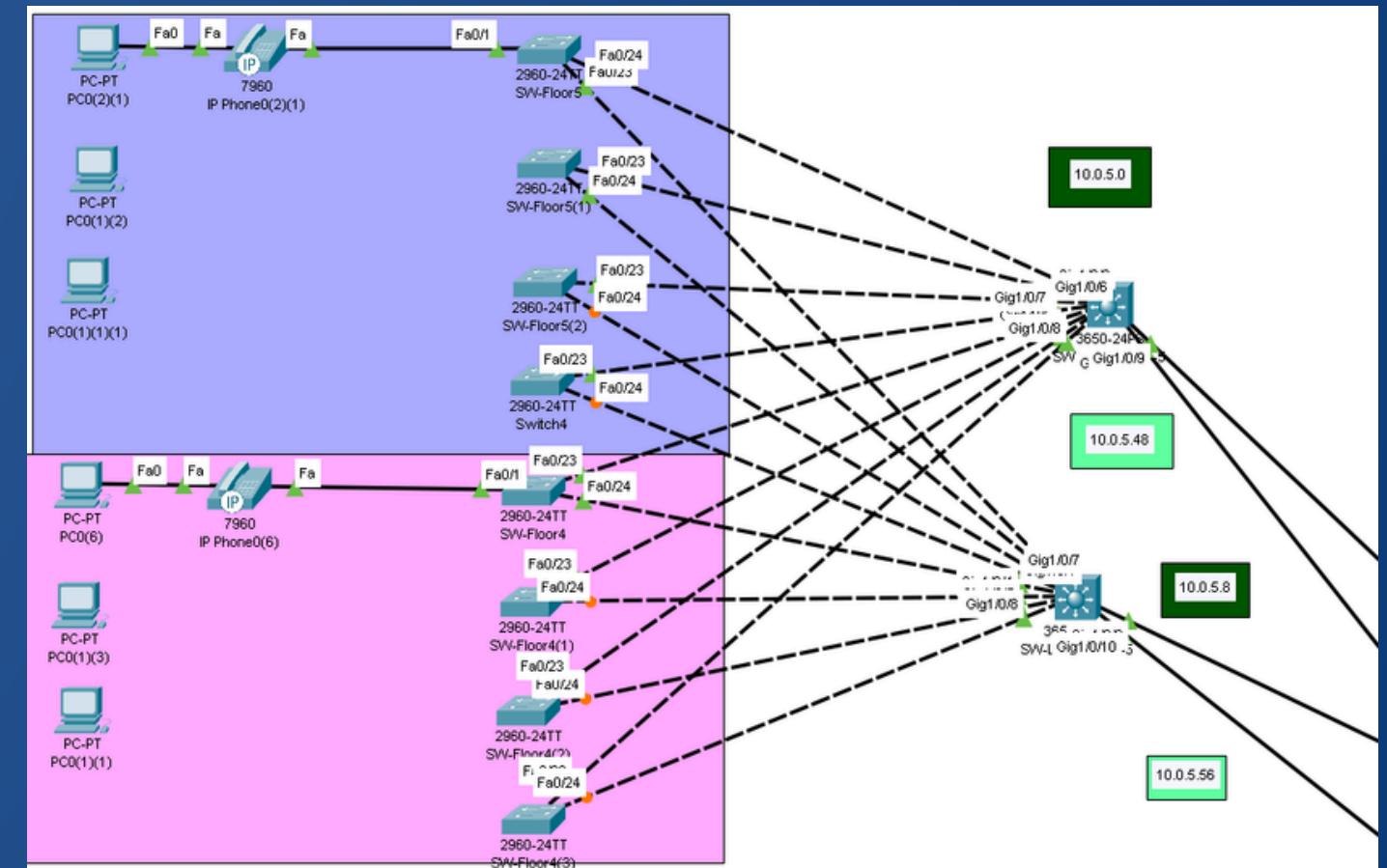
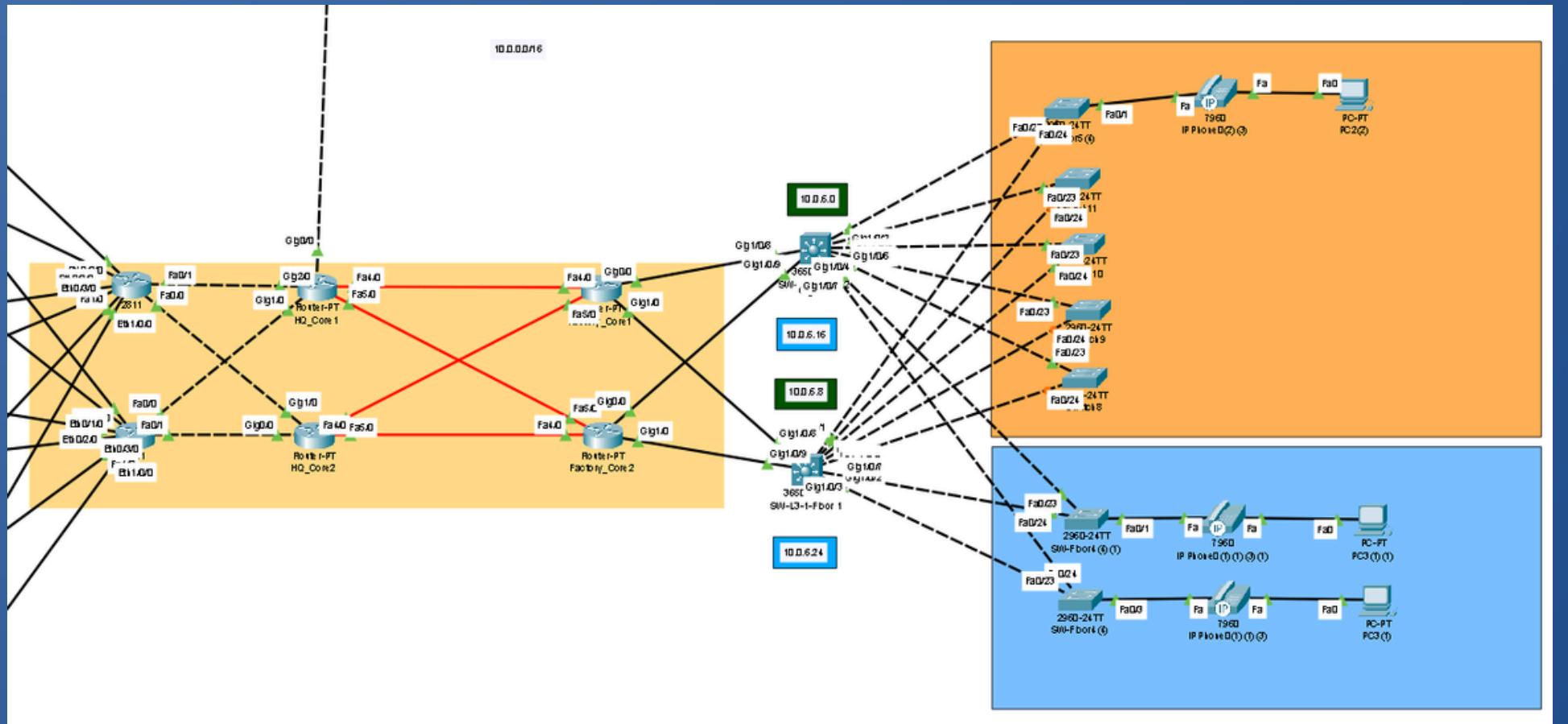


การติดตั้ง firewall และจัดการ Inbound และ Outbound rules ให้เฉพาะบริการที่จำเป็น โดย firewall คือป้องกันอยู่ระหว่างช่องทางออกสู่ Internet เพียงช่องทางเดียวขององค์กร

การใช้ VLAN เพื่อจำกัดการเข้าถึงข้อมูลภายในให้เฉพาะส่วนที่จำเป็น โดยกำหนด VLAN ให้กับกลุ่มผู้ใช้งานหรืออุปกรณ์ที่ต้องการเข้าถึงข้อมูลหรือบริการ ช่วยแยกการสื่อสารออกจากกัน และสามารถแยก broadcast domain ด้วยการใช้ VLAN



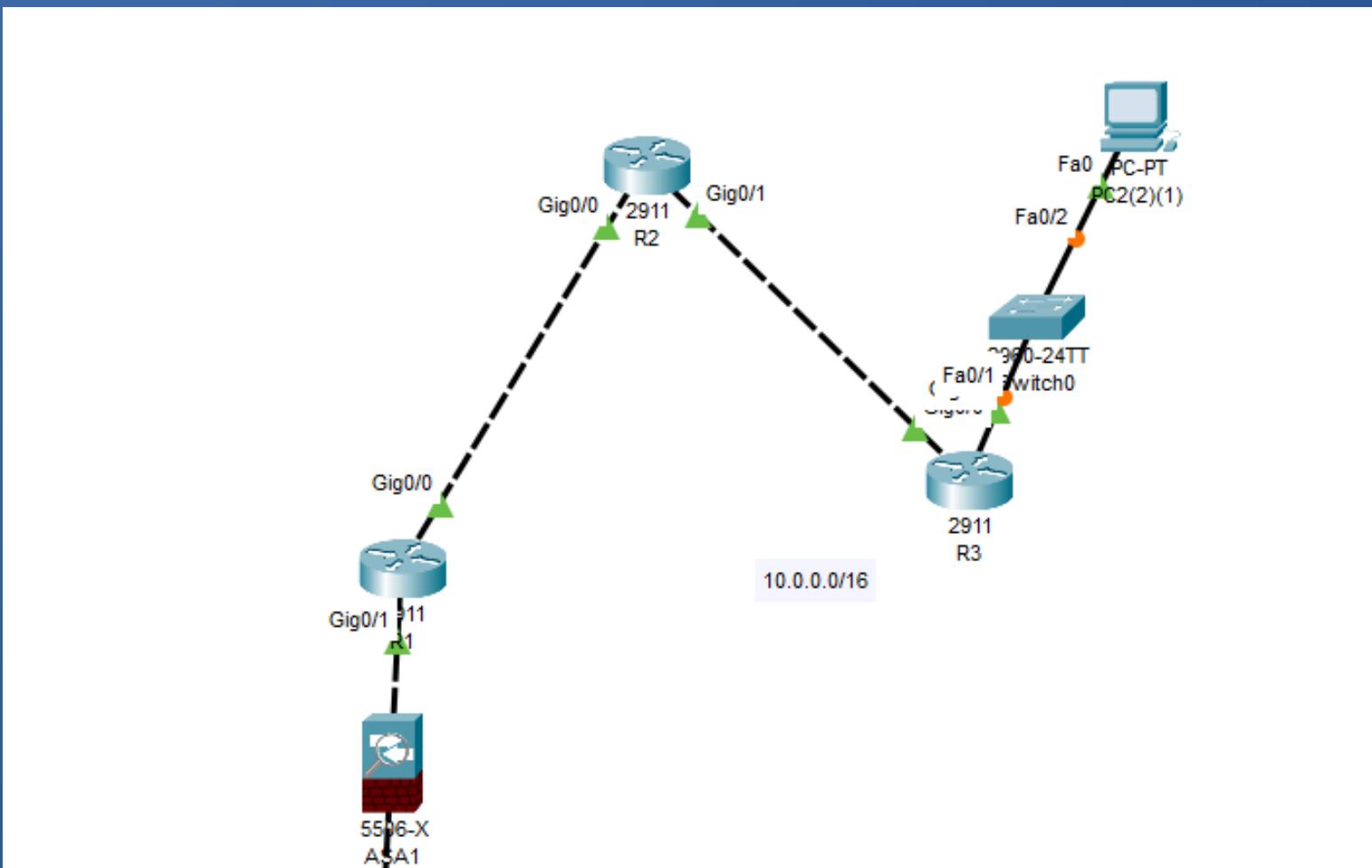
MODULARITY



- โครงสร้างแบบ 3-Layer ชั้นแต่ละชั้นจะทำหน้า
เฉพาะสามารถจัดการแยกได้

- VLAN โดยแบ่งเครือข่ายออกเป็น VLAN และกลุ่มผู้ใช้งาน
- Subnetting แบ่งเครือข่ายออกเป็น subnet ย่อย เพื่อลด
การชนกันของข้อมูล และจัดการ IP ง่ายขึ้น

VPN

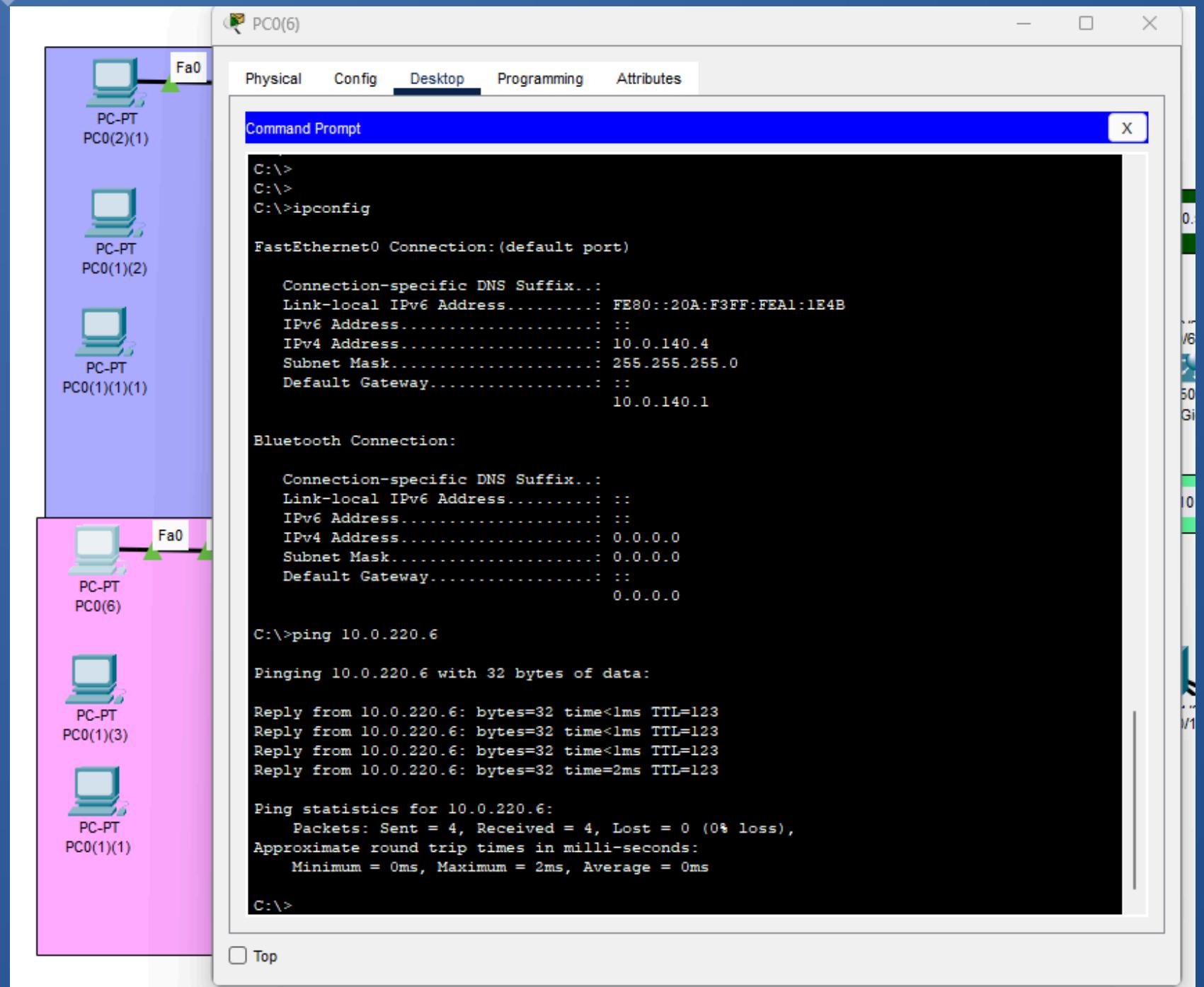


มีการติดตั้ง VPN (Virtual Private Network)
เพื่อติดต่อกับ Partner ภายนอก โดยไม่ผ่าน
ISP แต่ผ่านทาง IPsec Tunnel ที่สร้างขึ้น
ระหว่าง 2 router



TESTING AND VALIDATION

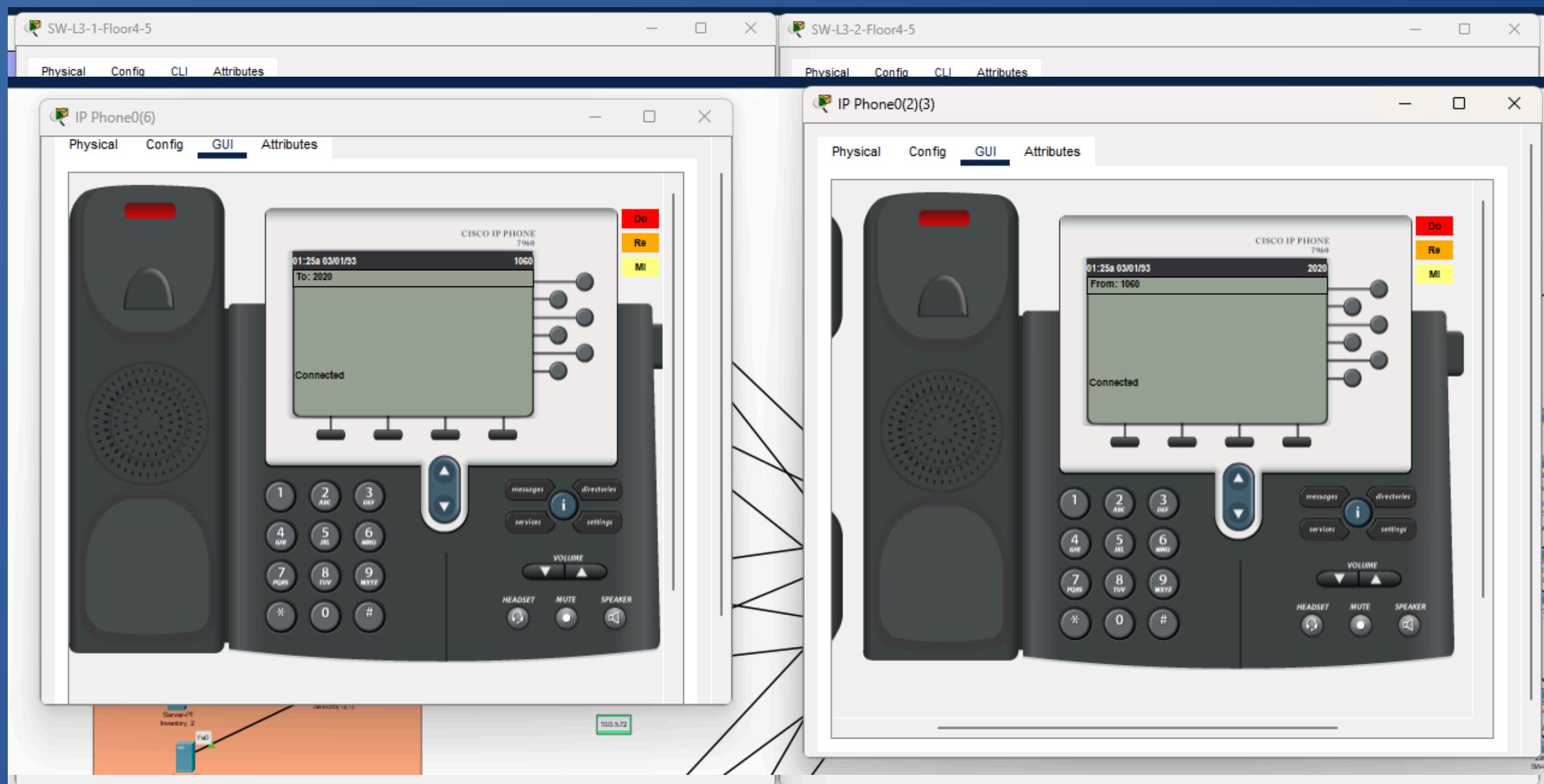
INTERNAL CONNECTIVITY TEST



ทดสอบโดยการ ping test จาก PC ในชั้น 4 ของตึก HQ ไปที่

PC ชั้น 2 ของตึก Factory

VOIP TEST



ตรวจสอบการทำงานของ VOIP โดยการโทรจาก HQ ไป Factory

HSRP VALIDATION

The image displays two terminal windows side-by-side, both titled "SW-L3-1-Floor4-5" and "SW-L3-2-Floor4-5". Both windows are set to the "CLI" tab and show the "IOS Command Line Interface".

SW-L3-1-Floor4-5 Terminal Output:

```
Switch con0 is now available
Press RETURN to get started.

Switch>
Switch>
Switch>en
Switch#show stan
Switch#show standby br
      P indicates configured to preempt.

Interface  Grp  Pri  P State    Active      Standby      Virtual IP
V1140       1    110  P Active   local       10.0.140.3   10.0.140.1
V1149       1    110  P Active   local       10.0.149.3   10.0.149.1
V1150       1    110  P Active   local       10.0.150.3   10.0.150.1
V1159       1    110  P Active   local       10.0.159.3   10.0.159.1
Switch#
Switch#
```

SW-L3-2-Floor4-5 Terminal Output:

```
00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.159.2 on Vlan149 from LOADING to FULL,
Loading Done

00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.159.2 on Vlan159 from LOADING to FULL,
Loading Done

00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.5.41 on GigabitEthernet1/0/9 from LOADING
to FULL, Loading Done

00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.159.2 on Vlan150 from LOADING to FULL,
Loading Done

%HSRP-6-STATECHANGE: Vlan149 Grp 1 state Speak -> Standby

00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.5.89 on GigabitEthernet1/0/10 from LOADING
to FULL, Loading Done

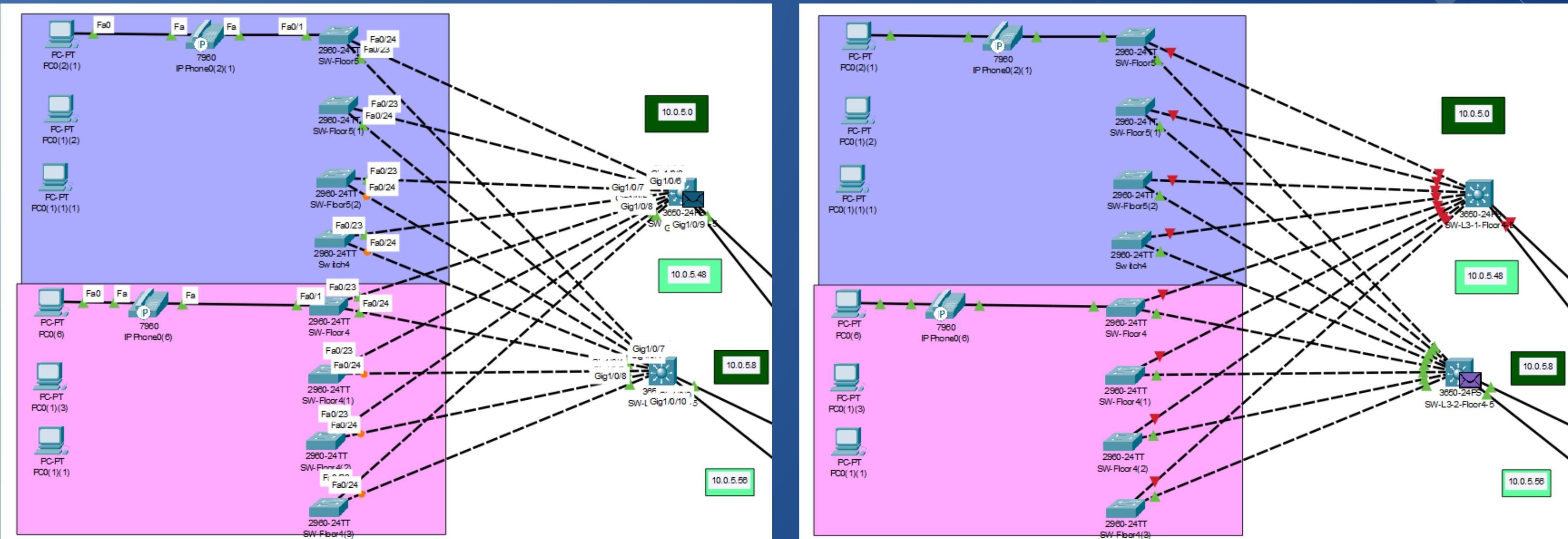
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.159.2 on Vlan140 from LOADING to FULL,
Loading Done

Switch>
Switch>
Switch>
Switch>en
Switch#show sta
Switch#show standb
Switch#show standby br
      P indicates configured to preempt.

Interface  Grp  Pri  P State    Active      Standby      Virtual IP
V1140       1    100  P Standby  10.0.140.2   local       10.0.140.1
V1149       1    100  P Standby  10.0.149.2   local       10.0.149.1
V1150       1    100  P Standby  10.0.150.2   local       10.0.150.1
V1159       1    100  P Standby  10.0.159.2   local       10.0.159.1
Switch#
```

ตรวจสอบการทำงานของ HSRP โดยการ show standby br เพื่อดู status ของ hsrp
จะเห็นว่าทั้ง 2 ตัวมี 1 ตัว standby และ 1 ตัว active

HSRP TEST



ทดสอบ HSRP โดยการปิด L3 Switch ที่ active อยู่แล้วทดสอบ ping อีกรอบจะเห็นว่า packet เปลี่ยน path จาก L3 Switch ตัวบนเป็น L3 Switch ตัวล่าง

OSPF VALIDATION

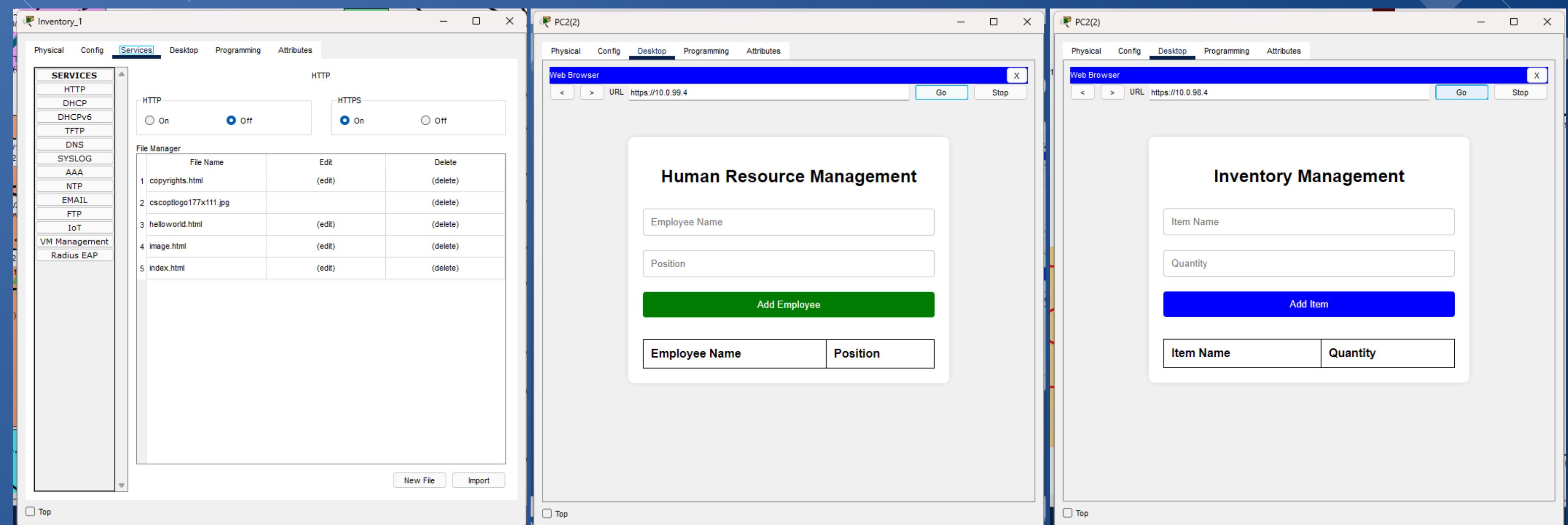
```
Switch#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 10.0.5.1 to network 0.0.0.0

  10.0.0.0/8 is variably subnetted, 41 subnets, 3 masks
O IA  10.0.2.0/29 [110/3] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
      [110/3] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
O IA  10.0.2.8/29 [110/3] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
      [110/3] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
O IA  10.0.2.16/29 [110/3] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
      [110/3] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
O IA  10.0.2.24/29 [110/3] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
      [110/3] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
O IA  10.0.3.0/30 [110/2] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
O IA  10.0.3.4/30 [110/2] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
O IA  10.0.3.8/30 [110/2] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
O IA  10.0.3.12/30 [110/2] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
C  10.0.5.0/29 is directly connected, GigabitEthernet1/0/9
O  10.0.5.8/29 [110/2] via 10.0.140.3, 01:12:44, Vlan140
      [110/2] via 10.0.149.3, 01:12:44, Vlan149
      [110/2] via 10.0.150.3, 01:12:44, Vlan150
      [110/2] via 10.0.159.3, 01:12:44, Vlan159
O  10.0.5.16/29 [110/11] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
O  10.0.5.24/29 [110/11] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
O  10.0.5.32/29 [110/2] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
O  10.0.5.40/29 [110/11] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
C  10.0.5.48/29 is directly connected, GigabitEthernet1/0/10
O  10.0.5.56/29 [110/2] via 10.0.140.3, 01:12:44, Vlan140
      [110/2] via 10.0.149.3, 01:12:44, Vlan149
      [110/2] via 10.0.150.3, 01:12:44, Vlan150
      [110/2] via 10.0.159.3, 01:12:44, Vlan159
O  10.0.5.64/29 [110/11] via 10.0.5.49, 01:12:44, GigabitEthernet1/0/10
O  10.0.5.72/29 [110/11] via 10.0.5.49, 01:12:59, GigabitEthernet1/0/10
O  10.0.5.80/29 [110/2] via 10.0.5.49, 01:12:59, GigabitEthernet1/0/10
O  10.0.5.88/29 [110/11] via 10.0.5.49, 01:12:44, GigabitEthernet1/0/10
O IA  10.0.6.0/29 [110/4] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
      [110/4] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
O IA  10.0.6.8/29 [110/4] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
      [110/4] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
O IA  10.0.6.16/29 [110/4] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
      [110/4] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
O IA  10.0.6.24/29 [110/4] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
      [110/4] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
O IA  10.0.7.0/30 [110/3] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
      [110/3] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
O  10.0.98.0/24 [110/12] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
      [110/12] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
O  10.0.99.0/24 [110/12] via 10.0.5.49, 01:12:34, GigabitEthernet1/0/10
      [110/12] via 10.0.5.1, 01:12:34, GigabitEthernet1/0/9
O  10.0.110.0/24 [110/3] via 10.0.5.49, 00:12:43, GigabitEthernet1/0/10
```

ตรวจสอบการทำงานของ OSPF โดยการ show ip route จะเห็นว่า L3 Switch ได้รับ route จากโปรโตคอล OSPF สังเกตได้จากที่ routing table ในบาง route มี O, O IA นำหน้าและได้รับ last resort gateway จาก OSPF เพื่อให้รู้ว่าถ้าต้องส่งไป external ต้องส่งไปที่ IP อะไร

APPLICATIONS TEST



ตรวจสอบการทำงานของ Applications โดยการเข้าใช้งาน website ของ Inventory management และ human resource management ผ่าน browser และใช้ HTTPS

RECOMMENDATIONS

การเพิ่มช่อง
ทางออกสู่
INTERNET
ภายนอก

เพิ่มจำนวน
FIREWALL

ลด **LATENCY** ลง
ในบางจุด

ALL MEMBER

นาย กิตต์ชินก้าร์ย์ ธรรมานนท์โชติ รหัสนักศึกษา 65070018
นาย ณัฐนันท์ วงศ์หน่องแวง รหัสนักศึกษา 65070076
นาย ณัฐพงศ์ มาสำราญ รหัสนักศึกษา 65070078
นาย ธีรภัทร์ สังข์สี รหัสนักศึกษา 65070108
นาย ไพบูลย์ มาดไทย รหัสนักศึกษา 65070141
นาย ภูมิไชย อุดมศิลป์ รหัสนักศึกษา 65070178



**THANK
YOU**