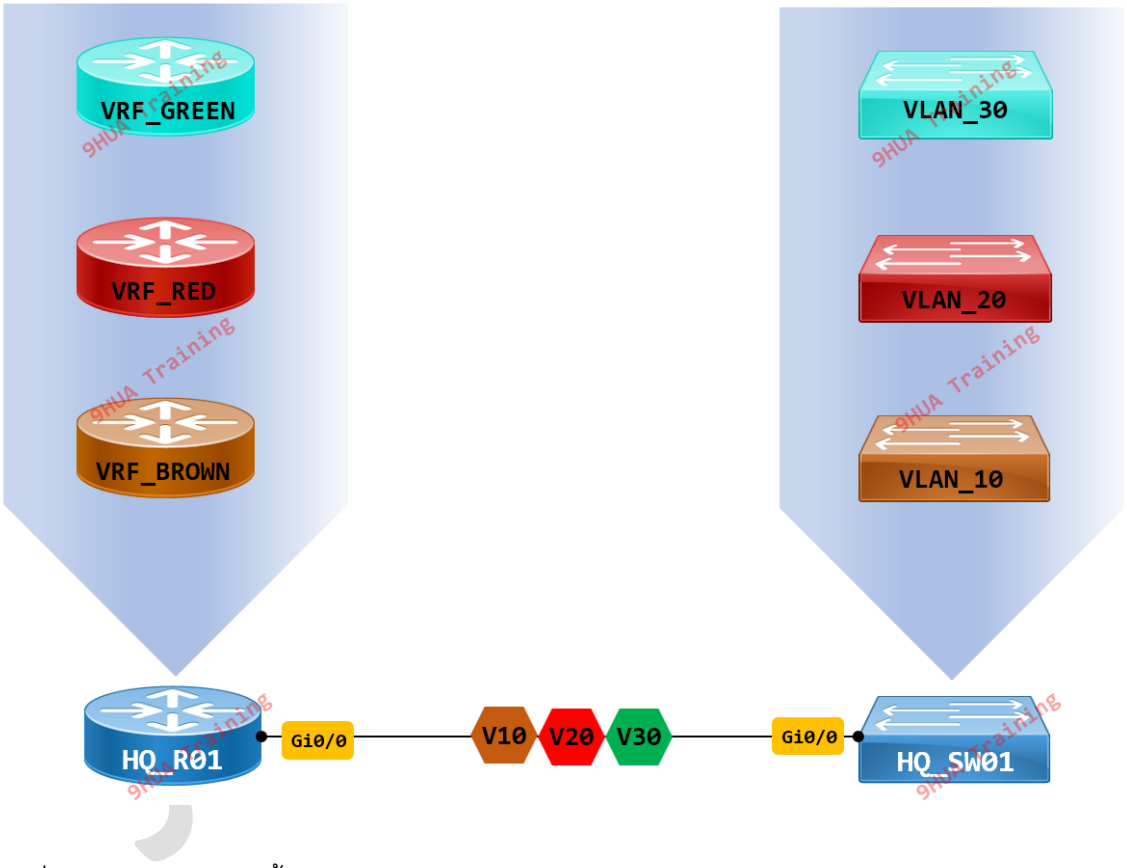
VRF Lite

ในระดับ Layer 2 เราได้ทำความเข้าใจเกี่ยวกับการแบ่งแยก Network ไปแล้ว โดยการทำ VLAN (Virtual LAN) ซึ่งทำให้ Switch 1 ตัว สามารถแยก Broadcast Traffic ออกจากกันได้ แน่นอนในระดับ Layer 3 ก็มีการทำงานในลักษณะนี้ด้วยเช่นกัน นั่นก็คือ VRF: Virtual Routing and Forwarding

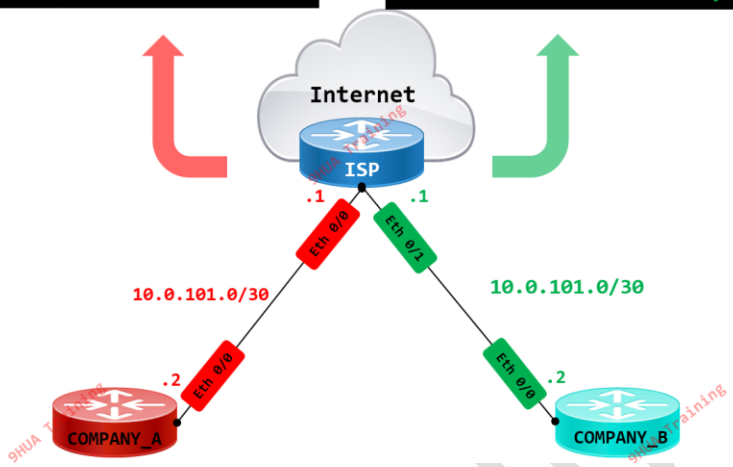
ปกติแล้ว Router จะมี Global Routing Table เพียงตารางเดียว นั่นหมายความว่าเราจะไม่สามารถทำการ Config IP Address ให้ซ้ำกันได้ และ VRF เข้ามาแก้ปัญหานี้โดยจะเสมือนว่ามี Virtual Router ขึ้นมาบน Physical Router ตัวเดียวกัน ตามรูปที่ได้แสดงด้านล่าง จะเห็นได้ว่ามี Virtual Router จำนวน 3 ตัว เท่ากับจำนวน VRF ที่ได้ทำการตั้งค่าคือ VRF_GREEN, VRF_RED และ VRF_BROWN



นั่นทำให้แต่ละ VRF นั้นมี Routing Table และ Forwarding Table เป็นของตัวเอง และโดยแต่ละ VRF จะมองไม่เห็น Routing Table ของ VRF อื่น นอกจาก VRF ของตัวเอง ตามรูปที่ได้แสดงด้านล่าง

```
ISP#show ip route vrf COMPANY_A

Routing Table: COMPANY_A

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.101.0/30 is directly connected, Ethernet0/0
L        10.0.101.1/32 is directly connected, Ethernet0/0
```

```
ISP#show ip route vrf COMPANY_B

Routing Table: COMPANY_B

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.101.0/30 is directly connected, Ethernet0/1
L        10.0.101.1/32 is directly connected, Ethernet0/1
```

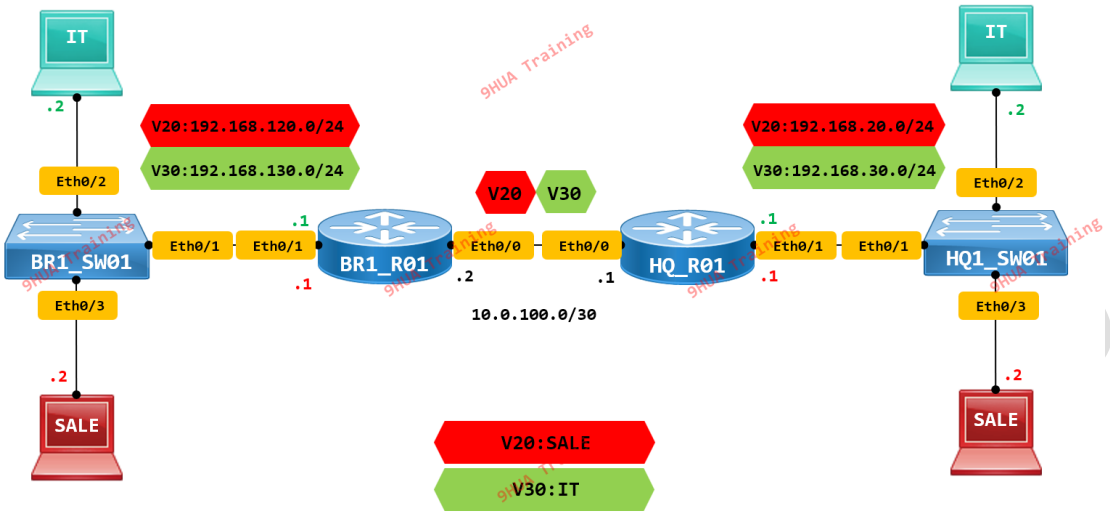


นอกเหนือข้อดีจากการสามารถใช้งาน IP Network ที่ซ้ำกันได้บน Router ตัวเดียวกันแล้ว ในแง่ของความปลอดภัยก็สามารถแบ่งแยก Network ของหน่วยงาน, แผนกต่าง ๆ รวมถึงลูกค้าแต่ละราย ออกจากกันได้

โดยในบทความนี้ได้กล่าวถึง VRF Lite ซึ่งมีความแตกต่างกับ VRF ที่ถูกใช้บนเครือข่ายของผู้ให้บริการทางด้านโครงข่าย หรือ Service Provider ที่ให้บริการ MPLS-VPN (Multiprotocol Label Switching-Virtual Private Network) ซึ่งได้ใช้ความสามารถของ MPLS และ MP-BGP (Multiprotocol Border Gateway Protocol)

VRF Lite Configuration

สำหรับตัวอย่างการตั้งค่า VRF Lite จะขอใช้ Network Diagram ตามรูปด้านล่าง เพื่อประกอบการ Config



1. จากรูปตัวอย่างต้องการสร้าง VRF เพื่อรองรับการใช้งานของแผนก IT และ SALE หลังจากนั้นทำการตรวจสอบ VRF ที่ได้ถูกสร้างขึ้น โดยใช้คำสั่งตามรูปด้านล่าง

```
HQ_R01(config)#ip vrf [VRF NAME]

HQ_R01(config)#ip vrf SALE
HQ_R01(config)#ip vrf IT
```

```
HQ_R01#show ip vrf
  Name                             Default RD          Interfaces
  IT                               <not set>
  SALE                             <not set>
```

2. นำ VRF ที่ได้สร้างขึ้นไปผูกไว้กับ Interface

2.1 เลือก Interface ที่ต้องการ จากในตัวอย่างนี้คือ Sub-Interface บน Router HQ_R01 และ BR1_R01 คือ Eth0/1.20 [สำหรับ VLAN 20] และ Eth0/1.30 [สำหรับ VLAN 30]

```
HQ_R01(config)#interface ethernet 0/1.20
HQ_R01(config-subif)#ip vrf forwarding SALE

HQ_R01(config)#interface ethernet 0/1.30
HQ_R01(config-subif)#ip vrf forwarding IT
```

2.2 ทำการกำหนด IP Address ลงบน Interface นั้นๆ

```
HQ_R01(config)#interface ethernet 0/1.20
HQ_R01(config-subif)#ip vrf forwarding SALE
HQ_R01(config-subif)#ip address 192.168.20.1 255.255.255.0

HQ_R01(config)#interface ethernet 0/1.30
HQ_R01(config-subif)#ip vrf forwarding IT
HQ_R01(config-subif)#ip address 192.168.30.1 255.255.255.0
```

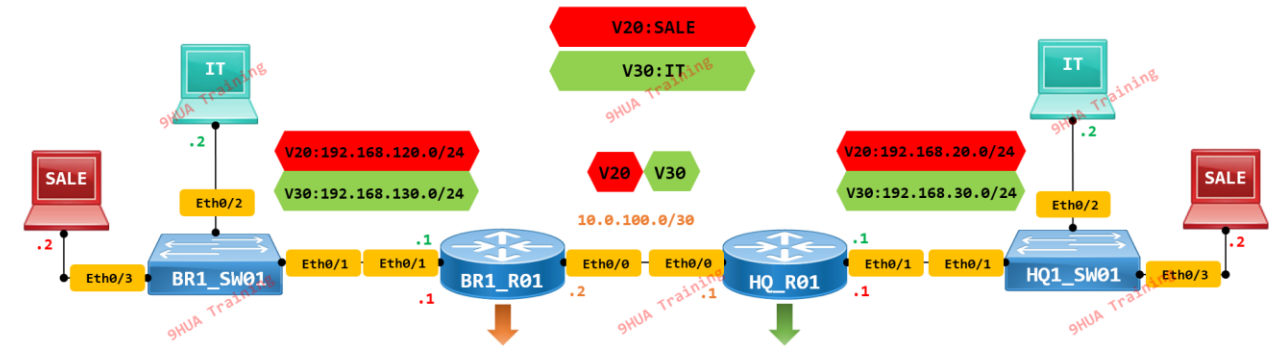
```
BR1_R01(config)#interface ethernet 0/1.20
BR1_R01(config-subif)#ip vrf forwarding SALE
BR1_R01(config-subif)#ip address 192.168.20.1 255.255.255.0

BR1_R01(config)#interface ethernet 0/1.30
BR1_R01(config-subif)#ip vrf forwarding IT
BR1_R01(config-subif)#ip address 192.168.30.1 255.255.255.0
```

*ถ้าหากทำตั้งค่า IP Address ก่อนที่นำ VRF มาผูกกับ Interface จะทำให้ IP Address ที่ได้ Config ไว้ก่อนนั้นถูกลบออกจาก Interface

2.3 ทำการตรวจสอบโดยใช้คำสั่ง “show ip vrf” จะเห็นได้ว่ามี VRF ถูกผูกไว้กับ Interface แล้ว

```
HQ_R01#show ip vrf
  Name                             Default RD          Interfaces
  IT                               <not set>           Et0/1.30
  SALE                             <not set>           Et0/1.20
```

3. การเชื่อมต่อระหว่าง Router HQ_R01 และ BR1_R01 แต่ละ VRF นั้น ได้ทำการเชื่อมต่อโดยใช้ IP Address ชุดเดียวกันคือ 10.0.100.0/30 เพื่อเป็น WAN [Wide Area Network] ตามรูปที่ได้แสดงด้านล่าง

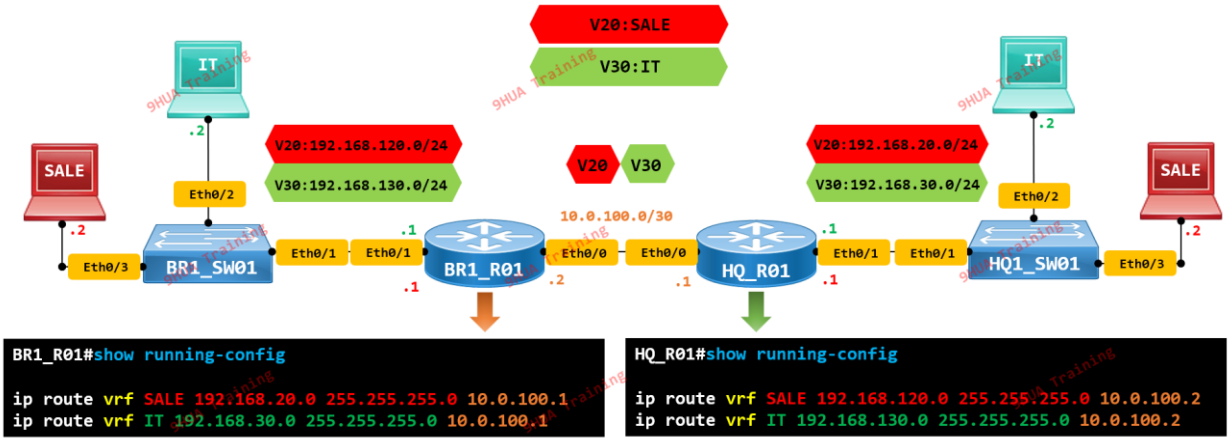



```
BR1_R01#show running-config interface ethernet 0/0.20
interface Ethernet0/0.20
 encapsulation dot1Q 20
 ip vrf forwarding SALE
 ip address 10.0.100.2 255.255.255.252

BR1_R01#show running-config interface ethernet 0/0.30
interface Ethernet0/0.30
 encapsulation dot1Q 30
 ip vrf forwarding IT
 ip address 10.0.100.2 255.255.255.252
```

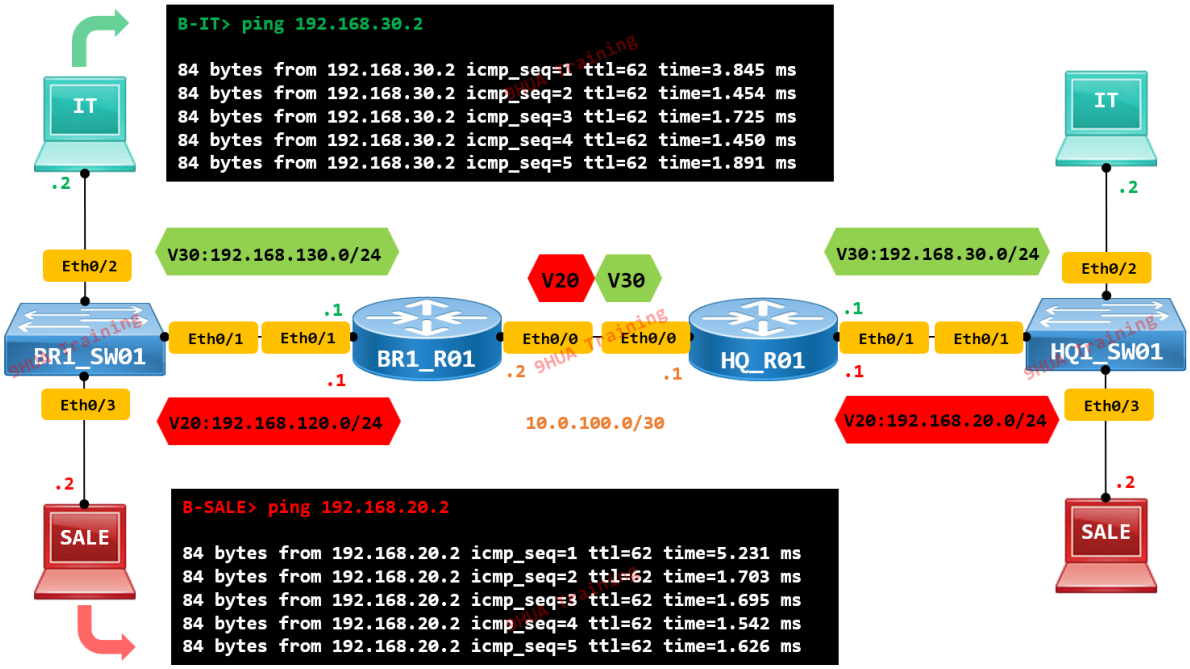
```
HQ_R01#show running-config interface ethernet 0/0.20
interface Ethernet0/0.20
 encapsulation dot1Q 20
 ip vrf forwarding SALE
 ip address 10.0.100.1 255.255.255.252

HQ_R01#show running-config interface ethernet 0/0.30
interface Ethernet0/0.30
 encapsulation dot1Q 30
 ip vrf forwarding IT
 ip address 10.0.100.1 255.255.255.252
```

4. การตั้งค่า Routing สำหรับในตัวอย่างนี้ ได้ใช้ Static Route เพื่อให้ VRF เดียวกันสามารถสื่อสารติดต่อกันได้ และตัวอย่างการใช้คำสั่งเพื่อให้แต่ละ VRF ใช้งาน Static Route นั้นได้แสดงตามรูปด้านล่าง

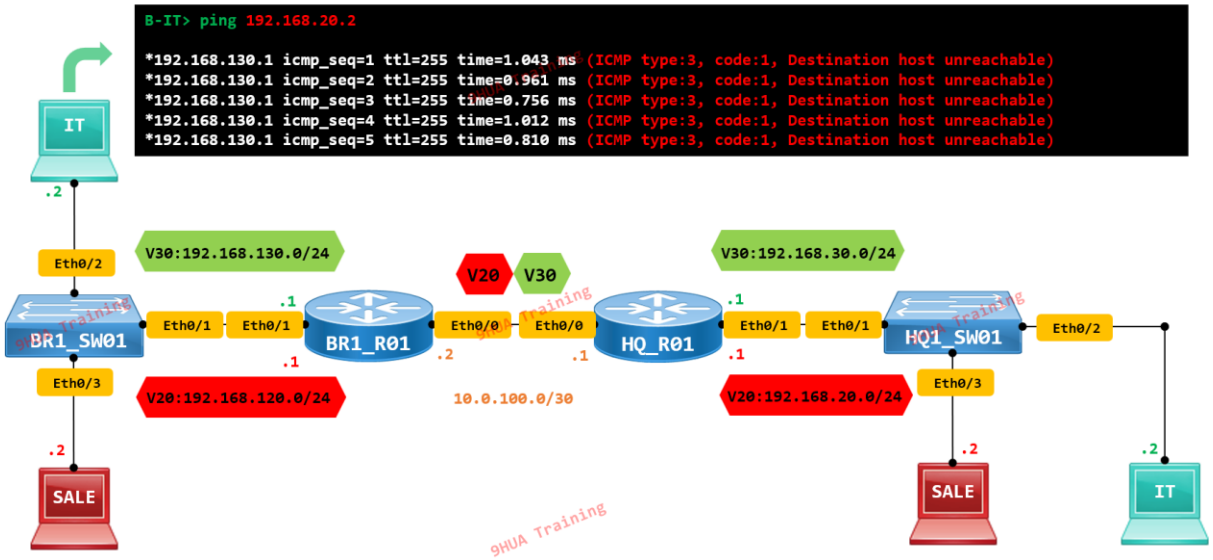
```
HQ_R01(config)#ip route vrf [VRF] [Prefix] [Mask] [IP next-hop]

HQ_R01(config)#ip route vrf SALE 192.168.120.0 255.255.255.0 10.0.100.2
HQ_R01(config)#ip route vrf IT 192.168.130.0 255.255.255.0 10.0.100.2
```



5. ทำการทดสอบโดยการ Ping จาก PC-IT และ PC-SALE ที่อยู่ฝั่ง BR1 ไปยัง PC-IT และ PC-SALE ที่อยู่ฝั่ง HQ ตามรูปที่ได้แสดงด้านล่างและจะเห็นได้ว่า PC แต่ละฝั่ง สามารถติดต่อกับแผนกของตัวเองได้แล้ว แต่จะไม่สามารถติดต่อกับต่างแนกได้ เนื่องจากได้มีการตั้งค่า VRF ไว้ จึงทำให้เกิด Routing Table ที่แยกออกจากกัน ตามแต่ละ VRF นั่นเอง

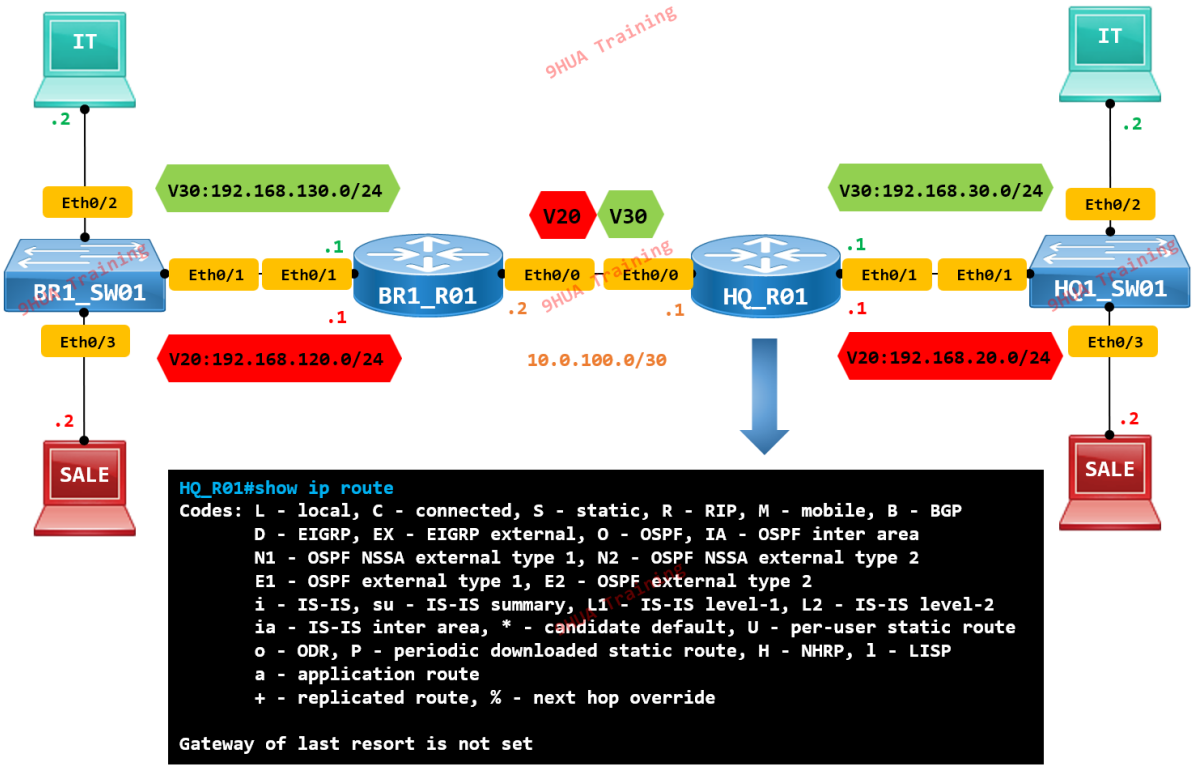


ผลจากการทดสอบการ Ping ไปยังแผนกอื่น โดยในรูปด้านล่าง PC-IT ฝั่ง BR1 ได้ Ping ไปยัง PC-SALE ฝั่ง HQ จะเห็นได้ว่าไม่สามารถติดต่อด้วยกันได้



6. ทำการตรวจสอบ Routing Table แต่ละ VRF โดยใช้คำสั่ง “show ip route vrf [VRF]” เห็นได้ว่าแต่ละ VRF ก็จะมี Routing Table เป็นของตัวเอง

ใช้คำสั่ง “show ip route” เพื่อตรวจสอบเส้นทางภายใต้ Global Routing Table ก็จะไม่มีเส้นทางที่อยู่ใน Global Routing Table เลย เนื่องจากในตัวอย่างนี้แต่ Interface ที่ใช้งานนั้นได้อยู่ภายใต้ VRF นั่นเอง



สำหรับข้อดีของการทำ VRF นั้น ก็มีหลากหลายด้วยกัน อย่างเช่น ในด้านความปลอดภัย Traffic ของแต่ละ VRF จะไม่สามารถมองเห็นหรือสื่อสารกับ VRF อื่นได้โดยตรง การใช้ IP Address ที่ซ้ำกันได้หรือ Overlapping IP Address เพราะแต่ละ VRF มี Routing Table เป็นของตัวเอง จึงทำให้ใช้ IP Address ที่ซ้ำกันได้ โดยส่วนใหญ่แล้วจะพบได้กับเครือข่ายของผู้ให้บริการโครงข่าย หรือ Service Provider ส่วนในเรื่องของความคุ้มค่านั้น ก็เปรียบเสมือนกับการตั้งค่า VLAN ที่ทำให้ 1 Physical Switch สามารถสร้าง Virtual Switch เพื่อรองรับการใช้งานแต่ละ VLAN และแยก Broadcast Traffic ออกจากกัน ก็เช่นเดียวกันกับ Router ที่สามารถตั้งค่า VRF เพื่อเป็น Virtual Router ที่อยู่ภายในเพื่อแยก Routing Table ออกจากกันได้