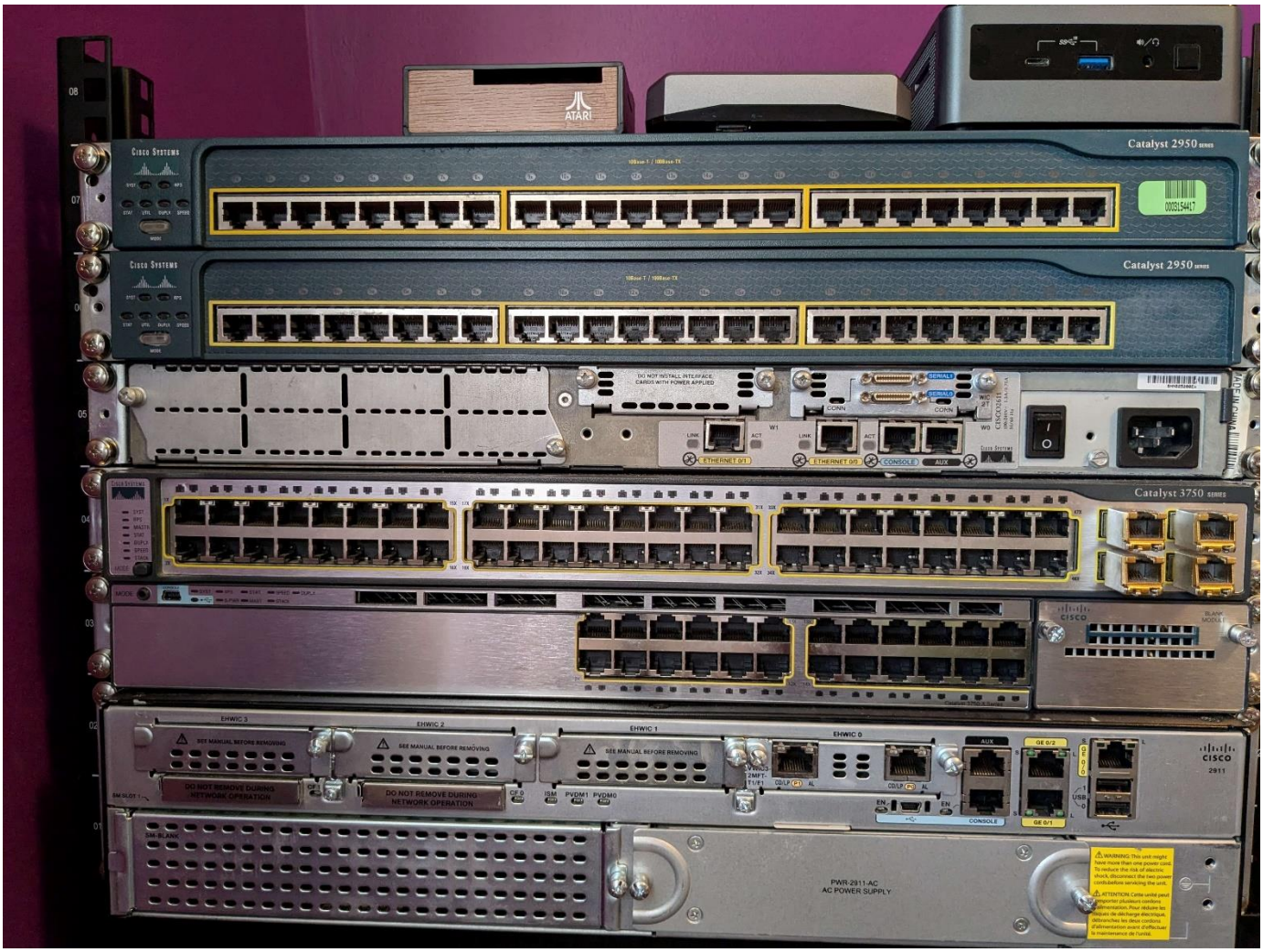
# Networking Reference Guide and Portfolio




*Practical guide and portfolio showcasing my hands-on experience in designing, building, and troubleshooting networking infrastructure.*

*Destiny Clay*

*02/25/2025*

# Contents

# Introduction

My name is Destiny Clay. I am a current network engineering, network security, and cybersecurity student. Before I found my passion for this field, I worked as a phlebotomist in the medical field. My passion revolves around helping others, but I soon realized the medical field was not the right fit for me. My true interest has always been in computers, which started as a hobby, but quickly turned into a career aspiration. One pivotal conversation with my current professor about Danville Community College's Network Engineering and Cybersecurity program changed everything for me. My professor explained to me that I belong in this field. From that moment, I knew I had found my calling, and I haven't looked back since.

I'm currently building a solid foundation in network design and security. I currently hold a Cisco Certified Network Associate certification which has helped me refine my technical skills in areas such as IP connectivity, EIGRP, OSPF, HSRP, VLANs, ACLs, DHCP, DNS, VPNs, NAT, and gain hands on experience with Cisco routers and switches.

In addition to my core skills, I am currently diving into Voice over IP (VoIP) technology and learning to work with Cisco Unified Communications Manager and Cisco Call Manager Express. I also have experience with several operating systems including Windows, several versions of Linux, Apple iOS, and Cisco IOS, and virtualization platforms like VirtualBox, Proxmox, and VMWare. These have allowed me to create multiple virtual machines to simulate active directory, NTFS permissions, user groups, and network shares.

As president of the Danville Community College CyberKnights club, I've had the opportunity to lead meetings and organize activities that foster collaboration and provide a space for my peers to learn and grow. Many students come to me for help with their networking projects and labs, and I take pride in being able to guide them through challenges and offer support to help them succeed in class.

From my Cisco home lab to countless hours spent in my college's server room, I've been able to immerse myself in hands-on learning. These experiences have helped strengthen my technical abilities and gain a deeper understanding.

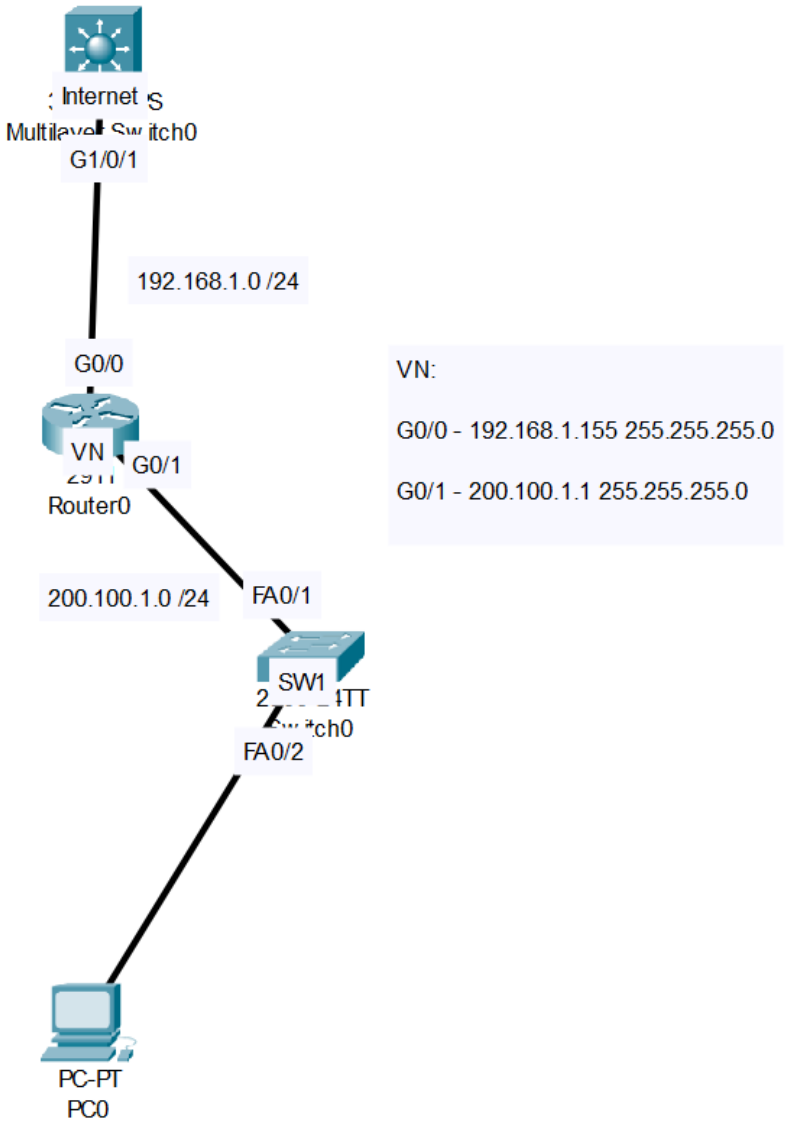
This portfolio represents my journey from the medical field to network engineering. I'm excited to continue developing my skills and contribute to the ever-evolving world of technology.

# Network Address Translation/Port Address Translation

Network Address Translation and Port Address Translation, otherwise known as NAT and PAT, are two ways we are still able to use IPv4. The pool of Ipv4 addresses has been exhausted for years, but these protocols have been the way we are able to translate private addresses to one singular public Ipv4 address, greatly reducing the need for Ipv4 addresses.

In this example, I am using PAT, also known as NAT overload. This technique allows multiple devices on a private network to share a single public IP address through port numbers rather than a pool of IPv4 addresses.

# Topology




# Configuration

**Internet:**

hostname Internet

```
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.1.1 255.255.255.0
```

**VN:**

```
hostname VN

ip dhcp pool LOCAL
 network 200.100.1.0 255.255.255.0
 default-router 200.100.1.1

interface GigabitEthernet0/0
 ip address 192.168.1.155 255.255.255.0
 ip nat outside
 no shutdown

interface GigabitEthernet0/1
 ip address 200.100.1.1 255.255.255.0
 ip nat inside
 no shutdown

 ip route 0.0.0.0 0.0.0.0 192.168.1.1

ip nat inside source list 1 interface GigabitEthernet0/0 overload
access-list 1 permit any
```

# VLANs

VLANs, virtual local area networks, are simply virtual versions of broadcast domains. A broadcast domain is a part of a network that can communicate with each other by sending messages to the broadcast address. Routers create a barrier between broadcast domains. An example would be a switch, and two PCs connected to the switch. Those devices are the broadcast domain. The router the switch is connected to is part of that broadcast domain but is also the barrier between a different broadcast domain. These are also referred to as subnets. VLANs are widely used to separate traffic. Imagine if we had 50 PCs connected to the same broadcast domain. What would that do for network bandwidth? Every PC would be sharing the same domain. It is important to separate this traffic to not overload a single domain. This can cause slow internet speeds for end users. Another way to decrease the likelihood of slow speeds for multiple users is EtherChannel, which I will talk about later.

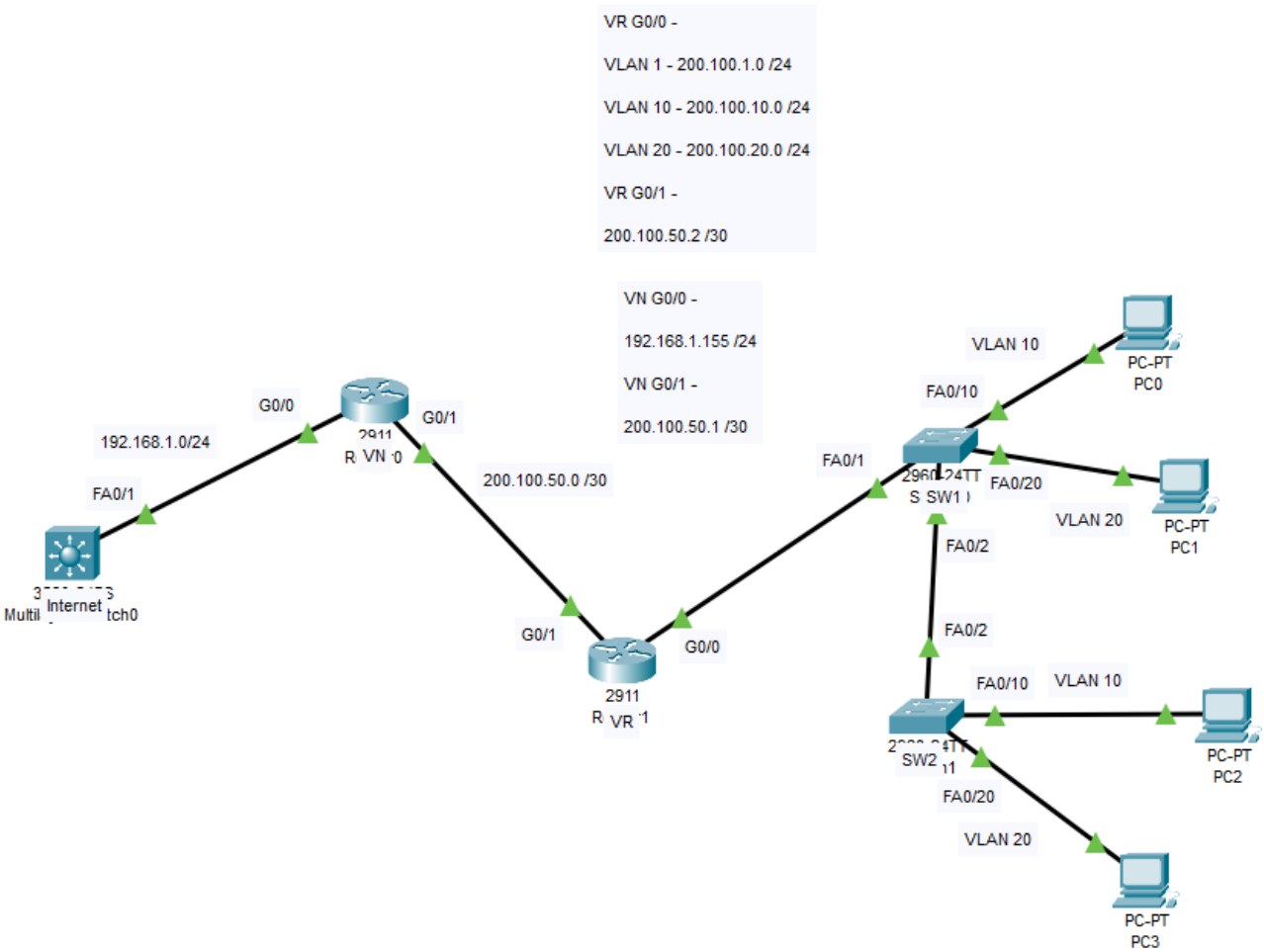
In this example, I am again using PAT, but we are now adding VLANs into the mix. An important part of VLANs is understanding how to subnet. Nowadays, everybody uses a subnet calculator. It is still important to know how to use this skill by memory.

VN will be the router responsible for PAT, and VR will be the router responsible for inter-VLAN routing. I am accomplishing this by using a method known as router on a stick. One link from a router is one subnet, right? What if we were able to have multiple subnets on one link? This is what router on a stick accomplishes. We can make digital interfaces to host multiple IP addresses on a single interface.

We are also using VTP, VLAN trunking protocol. This is a Cisco proprietary protocol that carries over VLAN information across trunked ports between switches. This allows the switches to send advertisements about VLAN information back and forth.

Trunked ports on a switch allows a switch to handle the heavy load of multiple VLANs. The switches will encapsulate the data sent across the trunk link with a unique tag of which VLAN the traffic is associated with.

## Topology



# Configuration

**VN:**

```
hostname VN

interface GigabitEthernet0/0
 ip address 192.168.1.155 255.255.255.0
 ip nat outside
no shutdown

interface GigabitEthernet0/1
 ip address 200.100.50.1 255.255.255.252
 ip nat inside
no shutdown

router eigrp 1
 network 192.168.1.0 255.255.255.0
 network 200.100.50.0 255.255.255.252

ip nat inside source list 1 interface GigabitEthernet0/0 overload

ip route 0.0.0.0 0.0.0.0 192.168.1.1

access-list 1 permit any
```

**VR:**

```
hostname VR
```

```
ip dhcp pool VLAN10
 network 200.100.10.0 255.255.255.0
 default-router 200.100.10.1

ip dhcp pool VLAN20
 network 200.100.20.0 255.255.255.0
 default-router 200.100.20.1

router eigrp 1
 network 200.100.50.0 255.255.255.252
 network 200.100.1.0 255.255.255.0
 network 200.100.10.0 255.255.255.0
 network 200.100.20.0 255.255.255.0

interface GigabitEthernet0/0
 no shutdown

interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 200.100.1.1 255.255.255.0

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 200.100.10.1 255.255.255.0

interface GigabitEthernet0/0.20
```

```
 encapsulation dot1Q 20
 ip address 200.100.20.1 255.255.255.0

interface GigabitEthernet0/1
 ip address 200.100.50.2 255.255.255.252
 no shutdown

ip route 0.0.0.0 0.0.0.0 200.100.50.1
```

**SW1:**

```
hostname SW1

vtp mode server
vtp domain cisco

interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access

interface FastEthernet0/20
 switchport access vlan 20
```

```
 switchport mode access

interface Vlan1
 ip address 200.100.1.2 255.255.255.0
 no shutdown
```

**SW2:**

```
hostname SW2

vtp mode client
vtp domain cisco

interface FastEthernet0/2
 switchport mode trunk

interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access

interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access

interface Vlan1
 ip address 200.100.1.3 255.255.255.0
 no shutdown
```

# Dynamic Routing Protocols: EIGRP and OSPF

EIGRP, known as enhanced interior gateway routing protocol, is a distance vector dynamic routing protocol that is used to automate routing decisions. EIGRP is a Cisco proprietary protocol. When there is more than one router running EIGRP, they all exchange route information between themselves, and form an adjacency with each other. Networks can get very large, and applying static routes to every router in a network takes up a lot of time, labor, and resources. A dynamic routing protocol like EIGRP can significantly automate this process. In this example, I am using default route injection into EIGRP, and passive interfaces. A default route is a routers gateway of last resort. When a router has no other destination for the traffic it receives it sends it out of its gateway of last resort. This is usually the connection the router has to the internet.

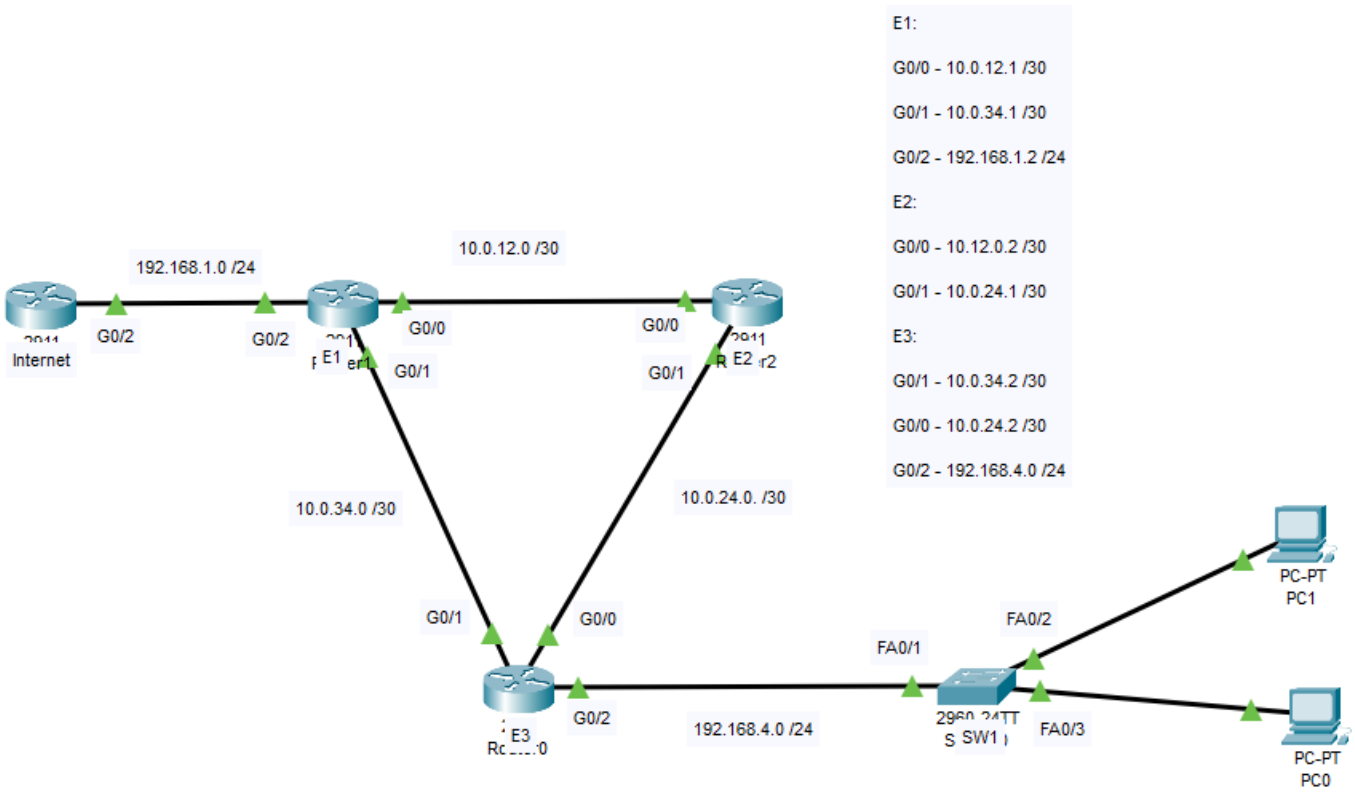
A passive interface is a way to make sure the interface in question does not send or receive routing updates. This is typically applied to loopback interfaces and the interface going towards your ISP's internal router. You do not want your ISP's internal router to know the internals of your network as that is a security issue.

OSPF, open shortest path first, is a link state dynamic routing protocol. It is an open standard routing protocol. OSPF is widely used today. OSPF can construct a topology of the network due to it being able to gather link state information. OSPF routers have states that they go through depending on where they are in the OSPF process. The states are: Down, Init, 2-way, Exstart, Exchange, Loading, and Full. Routers in full state typically are routers that are the designated router or the backup designated router. If a router is not in one of

these states, it will stay in the 2-way state. OSPF requires a few things to achieve a neighbor state. They must be in the same area, have different router ID's, and the same hello and dead timers. OSPF will not converge properly if there is an issue with any of those.

OSPF, like EIGRP, utilizes passive interfaces to control which interfaces send and receive routing updates. OSPF has an easier way for default route injection compared to EIGRP which I will demonstrate in the lab.

## EIGRP Topology



## EIGRP Configuration

**E1:**

```
hostname E1

interface Loopback0
 ip address 1.1.1.1 255.255.255.255

interface GigabitEthernet0/0
 ip address 10.0.12.1 255.255.255.252
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 5
 no shutdown

interface GigabitEthernet0/1
 ip address 10.0.34.1 255.255.255.252
 no shutdown

interface GigabitEthernet0/2
 ip address 192.168.1.2 255.255.255.0

router eigrp 1
 passive-interface GigabitEthernet0/2
 passive-interface Loopback0
 network 10.0.12.0 0.0.0.3
 network 10.0.34.0 0.0.0.3
```

```
 network 1.1.1.1 0.0.0.0

ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

**E2:**

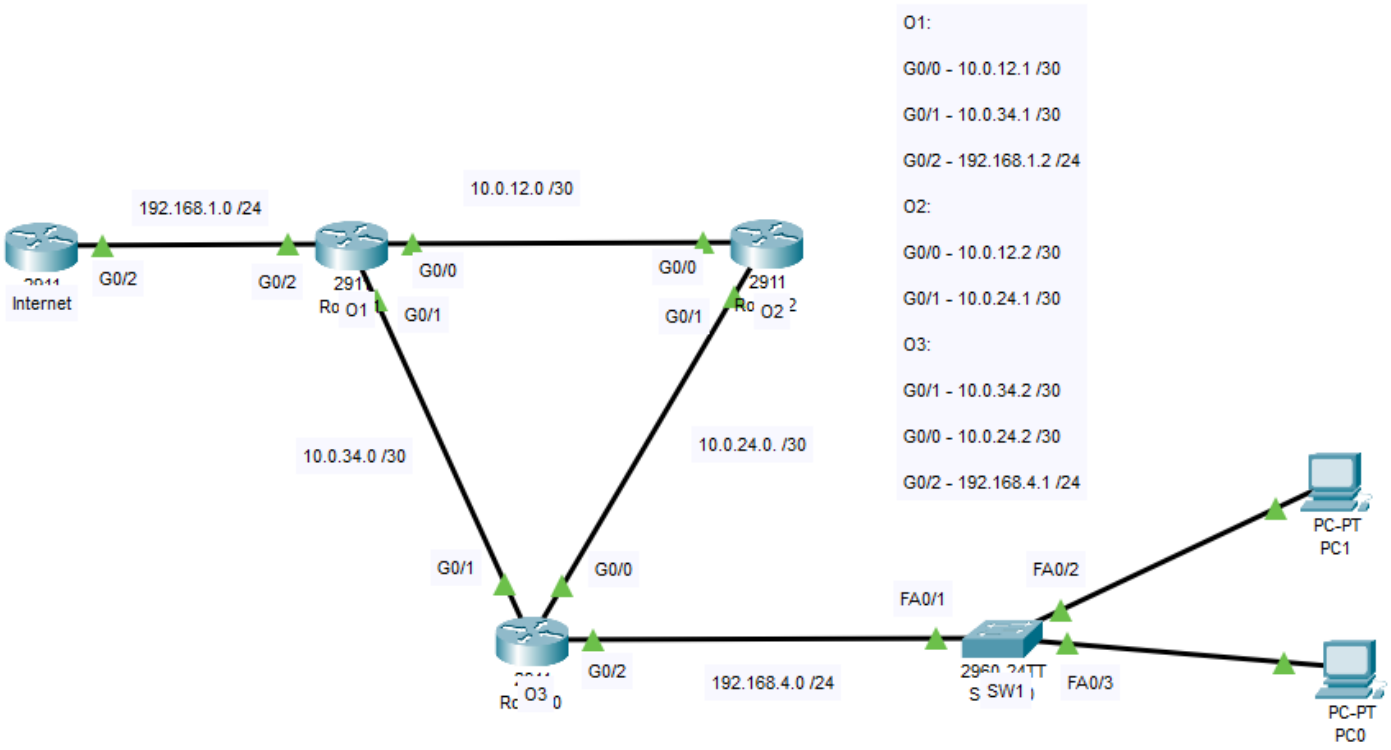
```
hostname E2

interface Loopback0
 ip address 2.2.2.2 255.255.255.255

interface GigabitEthernet0/0
 ip address 10.0.12.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 ip address 10.0.24.1 255.255.255.252
 no shutdown

router eigrp 1
 passive-interface Loopback0
 network 10.0.12.0 0.0.0.3
 network 10.0.24.0 0.0.0.3
 network 2.2.2.2 0.0.0.0
```

**E3:**

```
hostname E3
```

```
interface Loopback0
 ip address 3.3.3.3 255.255.255.255

interface GigabitEthernet0/0
 ip address 10.0.24.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 ip address 10.0.34.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/2
 ip address 192.168.4.1 255.255.255.0
 no shutdown

router eigrp 1
 passive-interface Loopback0
 network 10.0.34.0 0.0.0.3
 network 10.0.24.0 0.0.0.3
 network 192.168.4.0
 network 3.3.3.3 0.0.0.0
```

# OSPF Topology




# OSPF Configuration

**O1:**

hostname O1

interface Loopback0

ip address 1.1.1.1 255.255.255.255

interface GigabitEthernet0/0

```
 ip address 10.0.12.1 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 ip address 10.0.34.1 255.255.255.252
 no shutdown

interface GigabitEthernet0/2
 ip address 192.168.1.2 255.255.255.0
 no shutdown

router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface GigabitEthernet0/2
 passive-interface Loopback0
 network 10.0.12.0 0.0.0.3 area 0
 network 10.0.34.0 0.0.0.3 area 0
 network 1.1.1.1 0.0.0.0 area 0
 default-information originate

ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

**O2:**

```
hostname O2

interface Loopback0
```

```
 ip address 2.2.2.2 255.255.255.255

interface GigabitEthernet0/0
 ip address 10.0.12.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 ip address 10.0.24.1 255.255.255.252
 no shutdown

router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 passive-interface Loopback0
 network 10.0.12.0 0.0.0.3 area 0
 network 10.0.24.0 0.0.0.3 area 0
 network 2.2.2.2 0.0.0.0 area 0
```

**O3:**

```
hostname O3

interface Loopback0
 ip address 3.3.3.3 255.255.255.255

interface GigabitEthernet0/0
 ip address 10.0.24.2 255.255.255.252
 no shutdown
```

```
interface GigabitEthernet0/1
 ip address 10.0.34.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/2
 ip address 192.168.4.1 255.255.255.0
 no shutdown

router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 passive-interface Loopback0
 network 10.0.34.0 0.0.0.3 area 0
 network 10.0.24.0 0.0.0.3 area 0
 network 3.3.3.3 0.0.0.0 area 0
 network 192.168.4.0 0.0.0.255 area 0
```

# Port Security, Dynamic Arp Inspection, and DHCP Snooping

Typically, before any security measures are put in place, switch interfaces are all enabled. This can be a security risk. Port security is a way to control the number of devices allowed to connect to a specific switchport. It is also a validation check. It maps the connected device's mac address with the port it is connected to. Port security has three different modes. Shutdown, restrict, and protect. Shutdown is the default mode. I will be using all three modes in my example. Port security default mode will default to two dynamically learned mac addresses per port. This number can be manually set. You are also able to manually set the mac address to the port, and configure mac address sticky learning, which is another way for the port to dynamically learn the mac address of the device.

Port security shutdown will add to the violation counter, generate a syslog message, and shutdown a port when an unauthorized mac address connects to it.

Port security restrict will add to the violation counter, drop traffic, and generate a syslog message. Restrict will not shut down the port, but it will drop unauthorized traffic.

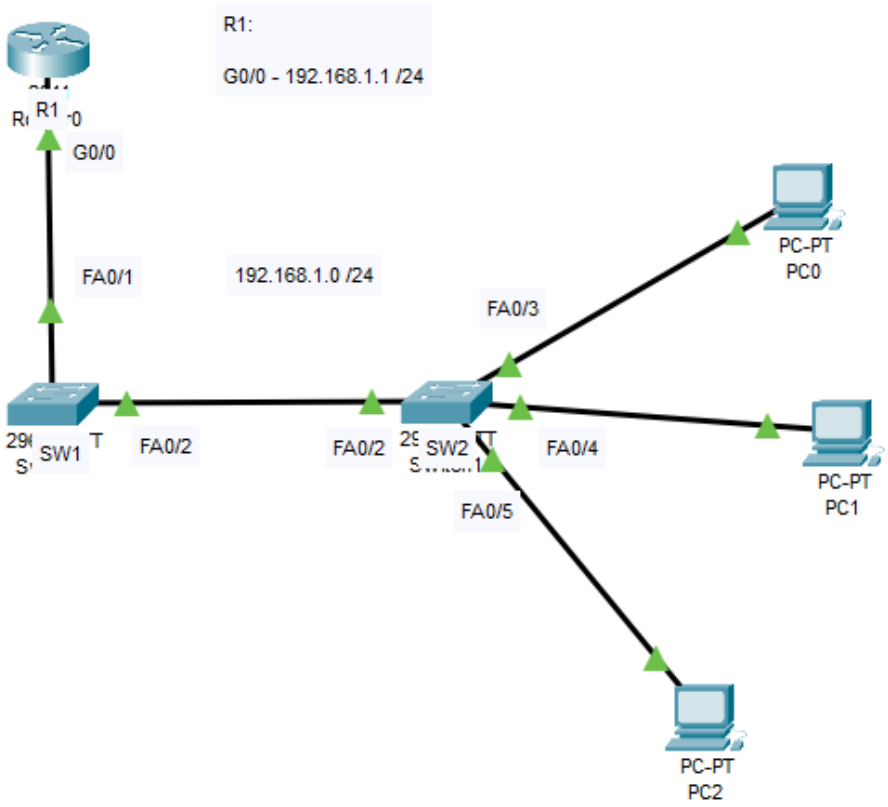
Port security protect will drop traffic and will not generate a syslog message or add to the violation counter. Protect is a way to silently drop unauthorized traffic without setting off any violation counters or syslog messages.

Dynamic Arp Inspection works in tandem with the DHCP snooping table to validate ARP packets in the network. ARP poisoning is a common attack by threat actors, and DAI is a

way to mitigate this type of attack. DAI will check the mac address to IP address bindings to make sure the traffic is safe. To avoid these attacks, it is imperative to let only valid ARP requests pass through the network.

DHCP Snooping prevents several types of DHCP attacks. One of them is called DHCP spoofing. Threat actors can set up a rogue DHCP server on a network and provide clients requesting IP addresses with incorrect IP configurations. This can lead to traffic interception, redirection, or network outages. DHCP snooping builds a table that records the mappings of IP addresses to mac addresses of clients on the network. Invalid DHCP traffic is dropped on untrusted ports.

## Topology



# Configuration

**R1:**

```
hostname R1

ip dhcp pool LOCAL
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1

interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
```

**SW1:**

```
hostname SW1

ip arp inspection vlan 1

ip dhcp snooping vlan 1
no ip dhcp snooping information option
ip dhcp snooping

interface FastEthernet0/1
 ip dhcp snooping trust

interface FastEthernet0/2
 ip arp inspection trust
```

**SW2:**

```
hostname SW2

ip arp inspection vlan 1

ip dhcp snooping vlan 1
no ip dhcp snooping information option
ip dhcp snooping

interface FastEthernet0/2
 ip arp inspection trust
 ip dhcp snooping trust

interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address sticky 0002.1780.DBE3

interface FastEthernet0/4
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
```

```
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0004.9A91.C399

interface FastEthernet0/5
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum 1
 switchport port-security violation protect
 switchport port-security mac-address sticky 0030.F26A.18E7
```

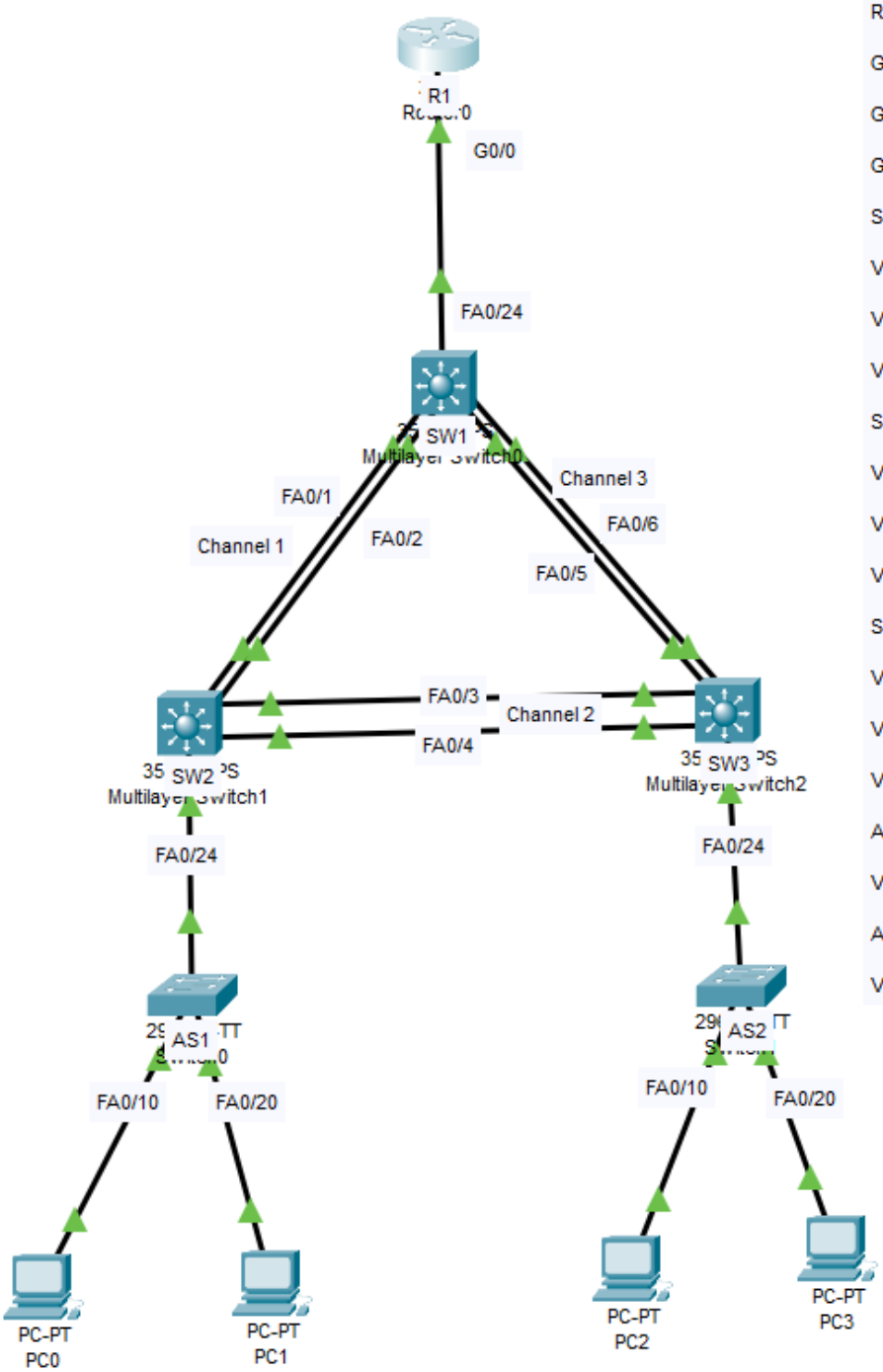
# EtherChannel: PAgP and LACP

EtherChannel combines up to eight physical links into a single logical link. This significantly increases bandwidth for end users. If each link is a gigabit, this means that all eight links would amount up to 8 gigabits of bandwidth! This technique can be helpful when you have many end users sharing bandwidth. Like I mentioned before, VLANs can also play a part in the separation of traffic even further to decrease the load on a single switchport.

EtherChannel has two different protocols: Port Aggregation Protocol, PAgP, and Link Aggregation Control Protocol, LACP. PAgP is a Cisco proprietary protocol. When links are channeled with PAgP, you can use desirable or auto. Using desirable automatically negotiates the channel between the two switchports. When both sides are desirable, both sides agree to form an etherchannel. When both sides are auto, they are in a passive state and will not form an etherchannel. When one side is desirable and the other is auto, an etherchannel is still formed.

LACP is an open standard protocol. When links are channeled with LACP, you can use active or passive. Using active automatically negotiates the channel, using passive does not.

# PAgP and LACP Topology




R1:

G0/0.1 - 200.100.1.1 /24

G0/0.10 - 200.100.10.1 /24

G0/0.20 - 200.100.20.1 /24

SW1:

VLAN1 - 200.100.1.2 /24

VLAN 10 - 200.100.10.2 /24

VLAN 20 - 200.100.20.2 /24

SW2:

VLAN1 - 200.100.1.3 /24

VLAN10 - 200.100.10.3 /24

VLAN 20 - 200.100.20.3 /24

SW3:

VLAN1 - 200.100.1.4 /24

VLAN10 - 200.100.10.4 /24

VLAN 20 - 200.100.20.4 / 24

AS1:

VLAN1 - 200.100.1.5 /24

AS2:

VLAN1 - 200.100.1.6 /24

# PAgP Configuration

**R1:**

```
hostname R1

ip dhcp excluded-address 200.100.1.1 200.100.1.6
ip dhcp excluded-address 200.100.10.1 200.100.10.4
ip dhcp excluded-address 200.100.20.1 200.100.20.4

ip dhcp pool VLAN10
 network 200.100.10.0 255.255.255.0
 default-router 200.100.10.1

ip dhcp pool VLAN20
 network 200.100.20.0 255.255.255.0
 default-router 200.100.20.1

interface GigabitEthernet0/0
 no shutdown

interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 200.100.1.1 255.255.255.0

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 200.100.10.1 255.255.255.0
```

```
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 200.100.20.1 255.255.255.0

router eigrp 1
 network 200.100.1.0
 network 200.100.10.0
 network 200.100.20.0
```

**SW1:**

```
hostname SW1

vtp mode server
vtp domain cisco

interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 channel-protocol pagp
 channel-group 1 mode desirable

interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 1 mode desirable

interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 3 mode desirable

interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 3 mode desirable

interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Vlan1
 ip address 200.100.1.2 255.255.255.0
```

```
 no shutdown

interface Vlan10
 ip address 200.100.10.2 255.255.255.0

interface Vlan20
 ip address 200.100.20.2 255.255.255.0
```

**SW2:**

```
hostname SW2

vtp mode client
vtp domain cisco

interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 1 mode desirable
```

```
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 1 mode desirable

interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 2 mode desirable

interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 2 mode desirable

interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Vlan1
 ip address 200.100.1.3 255.255.255.0
 no shutdown
```

```
interface Vlan10
 ip address 200.100.10.3 255.255.255.0

interface Vlan20
 ip address 200.100.20.3 255.255.255.0
```

**SW3:**

```
hostname SW3

vtp mode client
vtp domain cisco

interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 2 mode desirable

interface FastEthernet0/4
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 2 mode desirable

interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 3 mode desirable

interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol pagp
 channel-group 3 mode desirable

interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Vlan1
 ip address 200.100.1.4 255.255.255.0
 no shutdown

interface Vlan10
 ip address 200.100.10.4 255.255.255.0
```

```
interface Vlan20
 ip address 200.100.20.4 255.255.255.0
```

**AS1:**

```
hostname AS1

vtp mode client
vtp domain cisco

interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access

interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access

interface FastEthernet0/24
 switchport mode trunk

interface Vlan1
 ip address 200.100.1.5 255.255.255.0
 no shutdown
```

**AS2:**

```
hostname AS2
```

```
vtp mode client
vtp domain cisco

interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access

interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access

interface Vlan1
 ip address 200.100.1.6 255.255.255.0
 no shutdown
```

## LACP Configuration

**R1:**

```
hostname R1

ip dhcp excluded-address 200.100.1.1 200.100.1.6
ip dhcp excluded-address 200.100.10.1 200.100.10.4
ip dhcp excluded-address 200.100.20.1 200.100.20.4

ip dhcp pool VLAN10
 network 200.100.10.0 255.255.255.0
```

```
 default-router 200.100.10.1

ip dhcp pool VLAN20
 network 200.100.20.0 255.255.255.0
 default-router 200.100.20.1

interface GigabitEthernet0/0
 no shutdown

interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 200.100.1.1 255.255.255.0

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 200.100.10.1 255.255.255.0
```

**SW1:**

```
hostname SW1

vtp mode server
vtp domain cisco

interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active

interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active

interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 3 mode active

interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 3 mode active
```

```
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Vlan1
 ip address 200.100.1.2 255.255.255.0
 no shutdown

interface Vlan10
 ip address 200.100.10.2 255.255.255.0

interface Vlan20
 ip address 200.100.20.2 255.255.255.0
```

**SW2:**

```
hostname SW2

vtp mode client
vtp domain cisco

interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Port-channel2
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active

interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active

interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 2 mode active

interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 2 mode active

interface FastEthernet0/24
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Vlan1
 ip address 200.100.1.3 255.255.255.0
 no shutdown

interface Vlan10
 ip address 200.100.10.3 255.255.255.0

interface Vlan20
 ip address 200.100.20.3 255.255.255.0
```

**SW3:**

```
hostname SW3

vtp mode client
vtp domain cisco

interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 2 mode active

interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 2 mode active

interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 3 mode active

interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 3 mode active

interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
interface Vlan1
 ip address 200.100.1.4 255.255.255.0
 no shutdown

interface Vlan10
 ip address 200.100.10.4 255.255.255.0

interface Vlan20
 ip address 200.100.20.4 255.255.255.0
```

**AS1:**

```
hostname AS1

vtp mode client
vtp domain cisco

interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access

interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access

interface FastEthernet0/24
 switchport mode trunk
```

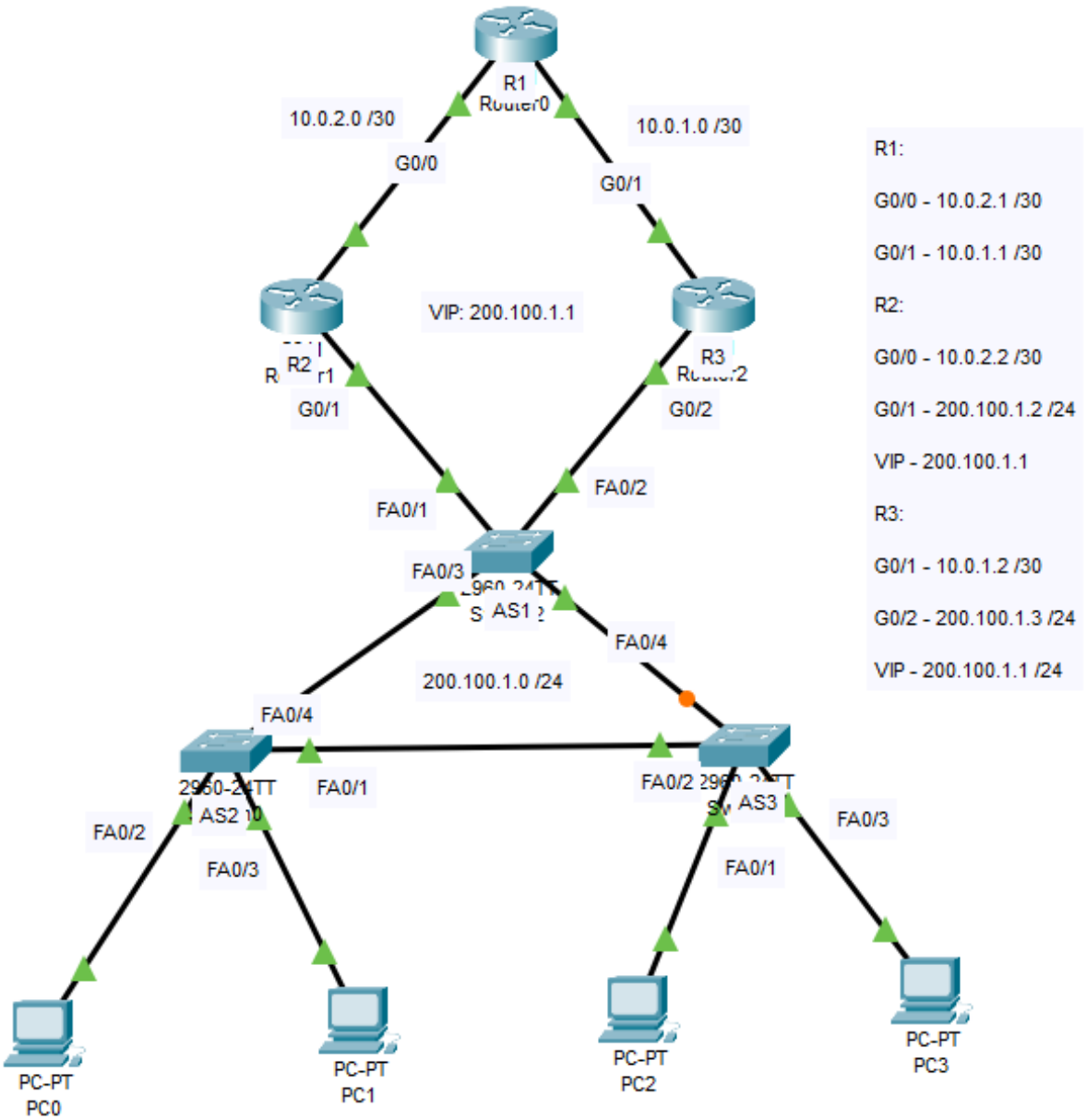
**AS2:**

```
hostname AS2

vtp mode client
vtp domain cisco

interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access

interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access

interface Vlan1
 ip address 200.100.1.6 255.255.255.0
 no shutdown
```

# Hot Standby Router Protocol

Hot Standby Router Protocol is a Cisco proprietary router redundancy protocol that establishes an active router and a standby router. This ensures that if the active router fails, there is failover to the standby router. HSRP uses a virtual IP address that is shared between two routers. This means that virtual IP address will always be accessible to end users as their default gateway. For a router to become the active router, eligibility is first determined by priority value, and then the highest IP address. Cisco has another proprietary router redundancy protocol called Gateway Load Balancing Protocol. The open standard protocol is called Virtual Router Redundancy Protocol.

# Topology


R1
10.0.2.0 /30
10.0.1.0 /30
G0/0
G0/1
VIP: 200.100.1.1
R2
R3
G0/1
G0/2
FA0/1
FA0/2
FA0/3
FA0/4
200.100.1.0 /24
FA0/4
FA0/1
FA0/2
FA0/3
FA0/2
FA0/3
FA0/1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
R1:
G0/0 - 10.0.2.1 /30
G0/1 - 10.0.1.1 /30
R2:
G0/0 - 10.0.2.2 /30
G0/1 - 200.100.1.2 /24
VIP - 200.100.1.1
R3:
G0/1 - 10.0.1.2 /30
G0/2 - 200.100.1.3 /24
VIP - 200.100.1.1 /24

## Configuration

**R1:**

```
hostname R1

interface GigabitEthernet0/0
 ip address 10.0.2.1 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 ip address 10.0.1.1 255.255.255.252
 no shutdown

router eigrp 1
 network 10.0.2.0 0.0.0.3
 network 10.0.1.0 0.0.0.3
```

**R2:**

```
hostname R2

interface GigabitEthernet0/0
 ip address 10.0.2.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 ip address 200.100.1.2 255.255.255.0
```

```
 standby 1 ip 200.100.1.1
 standby 1 preempt
 no shutdown

router eigrp 1
 network 10.0.2.0 0.0.0.3
 network 200.100.1.0

ip route 0.0.0.0 0.0.0.0 10.0.2.1
```

**R3:**

```
hostname R3

interface GigabitEthernet0/1
 ip address 10.0.1.2 255.255.255.252
 no shutdown

interface GigabitEthernet0/2
 ip address 200.100.1.3 255.255.255.0
 standby 1 ip 200.100.1.1
 standby 1 preempt
 no shutdown

router eigrp 1
 network 10.0.1.0 0.0.0.3
 network 200.100.1.0
ip route 0.0.0.0 0.0.0.0 10.0.1.1
```

# VLAN and DHCP Redundancy: Fall 2024's Semester Final Networking Project

In the Fall semester of 2024, my networking professor expressed to me that he wanted to add VLAN and DHCP redundancy to our final networking project at the time, and did not have the time to come up with it. He asked me to try and figure it out on my own. I was very interested in contributing to the project, so I said yes. After that class I spent the next couple days doing research and testing how the redundancy would work on packet tracer and with my Cisco home lab. In class, we use our Cisco routers as DHCP servers and router on a stick for VLAN configuration.

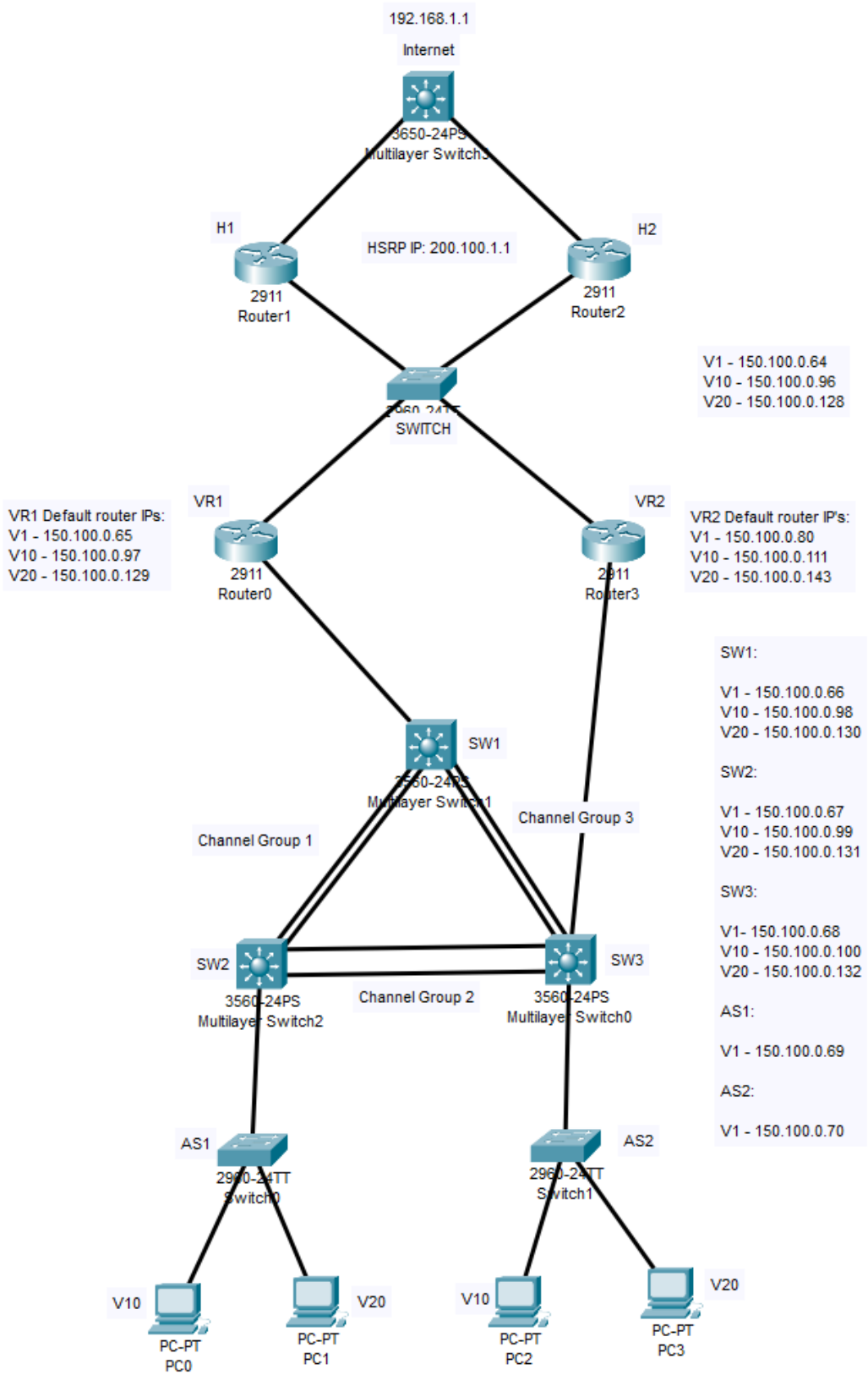
Since we can add a priority in the form of administrative distance on static routes, I figured it may be possible to prioritize one DHCP pool over the other. That did not end up being the case. I found that the only way to add redundancy between two routers for VLANs and DHCP was to split the address pool in half. I split the address pool in half and gave the primary router the first address in each subnet I was using for VLANs 1, 10, and 20. The second router got the first address in the second half of the pool for VLANs 1, 10, and 20. This translated over to the routers DHCP pools. I then made a DHCP address exclusion on both routers, so they are only handing out addresses in their respective parts of the pools. Since DHCP clients accept the first address they receive from a DHCP offer message, either router would give out addresses in their respective part of the pool.

I successfully tested this and presented it to my professor. He was very impressed and had me present this part of the project to the class. I drew the topology for the class and taught

them how to accurately configure it. The class then tested this configuration on our college's Cisco lab and found that it works perfectly. If classmates had trouble, I was there to answer questions and help them correct their configuration. The fail-over worked properly, and clients that got an address from a router they lost access to would pull an address and VLAN from the backup router.

This topology and configuration subsequently added to the project for future students, and students at this moment are still learning this technique. I am very proud of my contribution to the project, and plan to contribute more in the future.

# Topology


192.168.1.1
Internet
3650-24PS
Multilayer Switch3
H1
H2
HSRP IP: 200.100.1.1
2911
Router1
2911
Router2
V1 - 150.100.0.64
V10 - 150.100.0.96
V20 - 150.100.0.128
SWITCH
VR1
VR2
VR1 Default router IPs:
V1 - 150.100.0.65
V10 - 150.100.0.97
V20 - 150.100.0.129
2911
Router0
2911
Router3
VR2 Default router IP's:
V1 - 150.100.0.80
V10 - 150.100.0.111
V20 - 150.100.0.143
SW1:
V1 - 150.100.0.66
V10 - 150.100.0.98
V20 - 150.100.0.130
SW2:
V1 - 150.100.0.67
V10 - 150.100.0.99
V20 - 150.100.0.131
SW3:
V1- 150.100.0.68
V10 - 150.100.0.100
V20 - 150.100.0.132
AS1:
V1 - 150.100.0.69
AS2:
V1 - 150.100.0.70
SW1
Channel Group 1
Channel Group 3
SW2
SW3
3560-24PS
Multilayer Switch2
Channel Group 2
3560-24PS
Multilayer Switch0
AS1
AS2
2960-24TT
Switch0
2960-24TT
Switch1
V10
V20
V10
V20
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3

# Configuration

**H1:**

```
hostname H1

interface GigabitEthernet0/0
 ip address 200.100.1.2 255.255.255.0
 ip nat inside
 standby 1 ip 200.100.1.1
 standby 1 priority 105
 standby 1 preempt
 no shutdown

interface GigabitEthernet0/1
 ip address 192.168.1.155 255.255.255.0
 ip nat outside
 no shutdown

router eigrp 1
 network 200.100.1.0

ip nat inside source list 1 interface GigabitEthernet0/1 overload

ip route 0.0.0.0 0.0.0.0 192.168.1.1

access-list 1 permit any
```

**H2:**

```
hostname H2

interface GigabitEthernet0/0
 ip address 200.100.1.3 255.255.255.0
 ip nat inside
 standby 1 ip 200.100.1.1
 standby 1 preempt
 no shutdown

interface GigabitEthernet0/1
 ip address 192.168.1.156 255.255.255.0
 ip nat outside
 no shutdown

router eigrp 1
 network 200.100.1.0

ip nat inside source list 1 interface GigabitEthernet0/1 overload

ip route 0.0.0.0 0.0.0.0 192.168.1.1

access-list 1 permit any
```

**VR1:**

```
hostname VR1
```

```
ip dhcp excluded-address 150.100.0.80 150.100.0.94
ip dhcp excluded-address 150.100.0.111 150.100.0.126
ip dhcp excluded-address 150.100.0.143 150.100.0.158

ip dhcp pool local
 network 150.100.0.96 255.255.255.224
 default-router 150.100.0.97
 dns-server 8.8.8.8

ip dhcp pool local2
 network 150.100.0.128 255.255.255.224
 default-router 150.100.0.129
 dns-server 8.8.8.8

interface GigabitEthernet0/0
 no shutdown

interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 150.100.0.65 255.255.255.224

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 150.100.0.97 255.255.255.224

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
```

```
 ip address 150.100.0.129 255.255.255.224

interface GigabitEthernet0/1
 ip address 200.100.1.4 255.255.255.0
 no shutdown

router eigrp 1
 network 150.100.0.64 0.0.0.31
 network 150.100.0.96 0.0.0.31
 network 150.100.0.128 0.0.0.31
 network 200.100.1.0

ip route 0.0.0.0 0.0.0.0 200.100.1.1
```

**VR2:**

```
hostname VR2

ip dhcp excluded-address 150.100.0.65 150.100.0.79
ip dhcp excluded-address 150.100.0.97 150.100.0.110
ip dhcp excluded-address 150.100.0.129 150.100.0.142

ip dhcp pool VLAN10
 network 150.100.0.96 255.255.255.224
 default-router 150.100.0.111
 dns-server 8.8.8.8

ip dhcp pool VLAN20
```

```
 network 150.100.0.128 255.255.255.224
 default-router 150.100.0.143
 dns-server 8.8.8.8

interface GigabitEthernet0/0
 no shutdown

interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 150.100.0.80 255.255.255.224

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 150.100.0.111 255.255.255.224

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 150.100.0.143 255.255.255.224

interface GigabitEthernet0/1
 ip address 200.100.1.5 255.255.255.0
 no shutdown

router eigrp 1
 network 150.100.0.64 0.0.0.31
 network 150.100.0.96 0.0.0.31
 network 150.100.0.128 0.0.0.31
```

```
 network 200.100.1.0

ip route 0.0.0.0 0.0.0.0 200.100.1.1
```

**SW1:**

```
hostname SW1

ip routing

interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable

interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
```

```
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable

interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable

interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Vlan1
 ip address 150.100.0.66 255.255.255.224

interface Vlan10
 ip address 150.100.0.98 255.255.255.224

interface Vlan20
 ip address 150.100.0.130 255.255.255.224
```

```
router eigrp 1
 network 150.100.0.64 0.0.0.31
 network 150.100.0.96 0.0.0.31
 network 150.100.0.128 0.0.0.31
```

**SW2:**

```
hostname SW2

ip routing

interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable

interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode desirable
```

```
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable

interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable

interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Vlan1
 ip address 150.100.0.67 255.255.255.224

interface Vlan10
 ip address 150.100.0.99 255.255.255.224

interface Vlan20
 ip address 150.100.0.131 255.255.255.224

router eigrp 1
 network 150.100.0.64 0.0.0.31
 network 150.100.0.96 0.0.0.31
```

```
 network 150.100.0.128 0.0.0.31
```

**SW3:**

```
hostname SW3

ip routing

interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable

interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 channel-group 2 mode desirable

interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable

interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable

interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Vlan1
 ip address 150.100.0.68 255.255.255.224

interface Vlan10
 ip address 150.100.0.100 255.255.255.224

interface Vlan20
 ip address 150.100.0.132 255.255.255.224

router eigrp 1
 network 150.100.0.64 0.0.0.31
```

```
 network 150.100.0.96 0.0.0.31
 network 150.100.0.128 0.0.0.31
```

**AS1:**

```
hostname AS1

ip dhcp snooping vlan 10,20
ip dhcp snooping

interface FastEthernet0/10
 switchport access vlan 10
 ip dhcp snooping trust
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict

interface FastEthernet0/20
 switchport access vlan 20
 ip dhcp snooping trust
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict

interface FastEthernet0/24
 ip dhcp snooping trust
```

```
 switchport mode trunk

interface Vlan1
 ip address 150.100.0.69 255.255.255.224
```

**AS2:**

```
hostname AS2

ip dhcp snooping vlan 10,20
ip dhcp snooping

interface FastEthernet0/10
 switchport access vlan 10
 ip dhcp snooping trust
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict

interface FastEthernet0/20
 switchport access vlan 20
 ip dhcp snooping trust
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
```

```
interface FastEthernet0/24
 ip dhcp snooping trust
 switchport mode trunk

interface Vlan1
 ip address 150.100.0.70 255.255.255.224
```