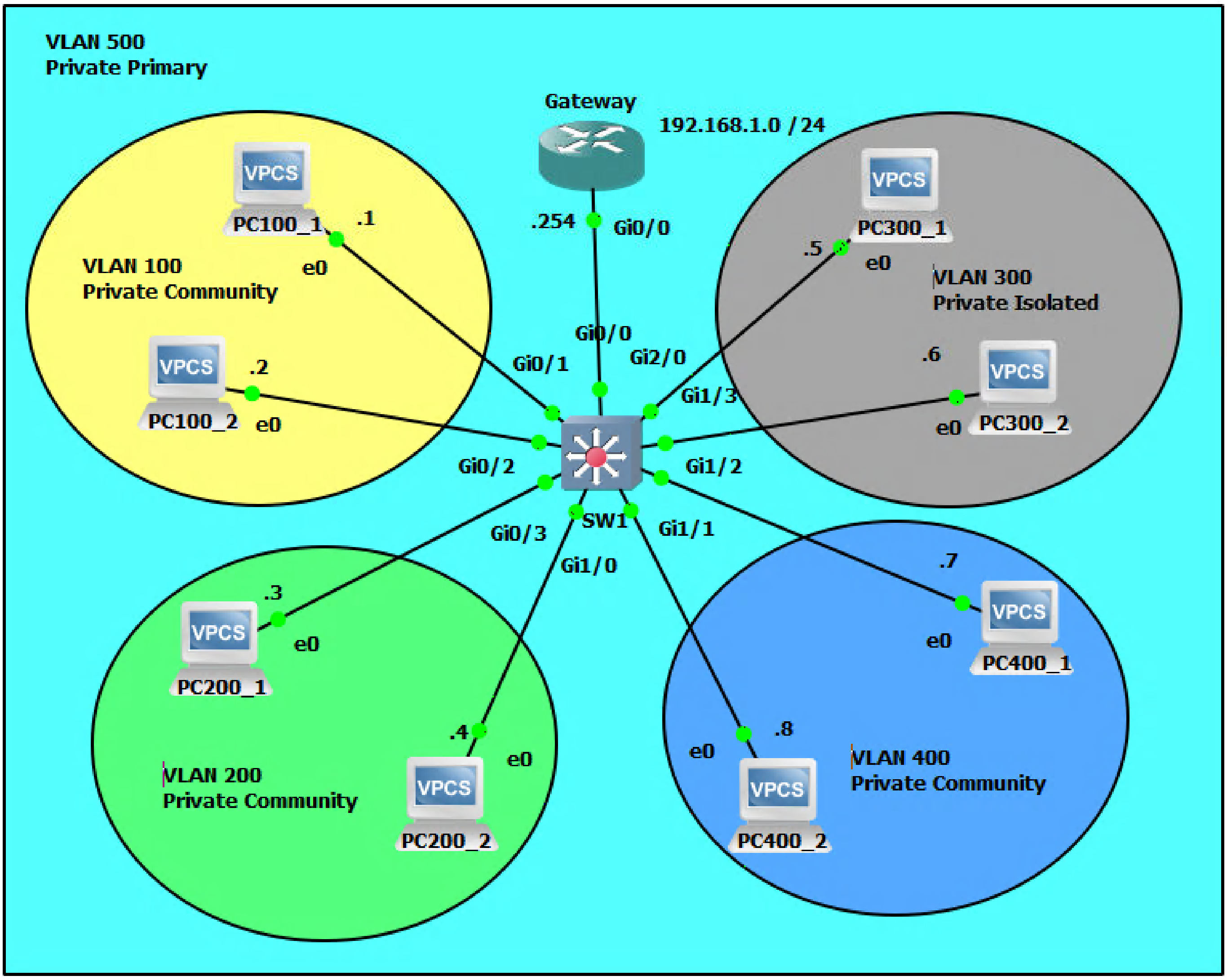
Cisco IOS Private VLANs

Network Topology



What is a Private VLAN?

A private VLAN, also known as a private LAN, is a VLAN (Virtual Local Area Network) that is used to segment a larger network into smaller, more secure subnets. It is used to isolate different types of traffic or to separate sensitive or confidential information from other network traffic.

A private VLAN typically consists of three types of ports: promiscuous ports, host ports, and community ports. Promiscuous ports can communicate with all other ports in the private VLAN, while host ports can only communicate with promiscuous ports. Community ports can only communicate with other ports in the same community. This allows for a high level of granularity in terms of controlling access and isolating different types of traffic on a network.

Promiscuous ports, isolated ports, and community ports are different types of ports that are used in private VLAN (PVLAN) environments to control access and isolate different types of traffic on a network.

1. Promiscuous Ports: These ports can communicate with all other ports in the private VLAN, including host and community ports. They are typically used for gateway or router connections and can be used to access shared resources or provide access to other networks.
2. Isolated Ports: These ports can only communicate with the associated promiscuous port and cannot communicate with other isolated or community ports. They are typically used to isolate sensitive or confidential information and prevent it from being accessed by other parts of the network.
3. Community Ports: These ports can only communicate with other ports within the same community and not with other communities or promiscuous ports. They are used to create isolated groups within a private VLAN and to control access to shared resources.

In summary, promiscuous ports allow communication with all other ports in the PVLAN, isolated ports are used to isolate sensitive information and prevent it from being accessed by other parts of the network, and community ports are used to create isolated groups within a PVLAN and control access to shared resources.

Private VLANs are often used in enterprise networks, data centers, and service provider environments to segment traffic and provide additional security. They can also be used to isolate guest or IoT traffic, to separate different departments or groups within an organization, or to separate different types of traffic on a network.

What is a Private Isolated VLAN?

A private isolated VLAN is a good solution for keeping sensitive or confidential information separate from other network traffic. It can be used for segmenting a network into secure and non-secure zones, for example, to isolate traffic from a secure server or database from the rest of the network. Additionally, it can be used to create secure zones for specific departments or groups within an organization, or to separate different types of traffic on a network, such as guest or IoT traffic. Some things that Private VLANs can be beneficial for include:

1. Segmenting a network into secure and non-secure zones: In this scenario, a private isolated VLAN would be used to separate sensitive or confidential information from other network traffic. This could include separating a secure server or database from the rest of the network, or isolating traffic from a specific department or group that handles sensitive information.
2. Isolating guest traffic: In a scenario where guest wireless access is provided, a private isolated VLAN could be used to separate guest traffic from internal network traffic. This would help to prevent guests from accessing sensitive or confidential information on the

internal network.

3. Isolating IoT traffic: In a scenario where there are a large number of IoT devices connected to a network, a private isolated VLAN could be used to separate IoT traffic from other network traffic. This would help to prevent IoT devices from accessing sensitive or confidential information on the network and also prevent any potential security risks from these devices.
4. Isolating different types of traffic: In a scenario where there are multiple types of traffic on a network, such as voice and data traffic, a private isolated VLAN could be used to separate the different types of traffic. This would help to ensure that voice traffic, for example, is prioritized over data traffic, and that there is no interference between the different types of traffic on the network.

Configuration

This configuration is being done in GNS3. In order to accomplish this topology in GNS3 you have to have the Cisco IOSvL2 switch image. The scenario is that the company has three network segments (VLANs 100, 200, and 400) that the departments in those VLANs where the PCs can communicate within the designated VLAN and out through the Gateway. However, as a matter of policy, those three VLANs are not allowed to communicate with e other VLANs. Lastly there is a fourth VLAN (VLAN 300) that is in a LAN segment that has been designated as needing a high degree of security. Therefore, VLAN 300 will be set up as a private isolated VLAN. Thus, the PCs in this VLAN will only be able to communicate with the Gateway. They will even be prevented from communications with each other as part of the isolated private VLANs.

PCs

```
PC100_1>ip 192.168.1.1/24 192.168.1.254
PC100_2>ip 192.168.1.2/24 192.168.1.254
PC200_1>ip 192.168.1.3/24 192.168.1.254
PC200_2>ip 192.168.1.4/24 192.168.1.254
PC300_1>ip 192.168.1.5/24 192.168.1.254
PC300_2>ip 192.168.1.6/24 192.168.1.254
PC400_1>ip 192.168.1.7/24 192.168.1.254
PC400_2>ip 192.168.1.8/24 192.168.1.254
```

Gateway

```
Gateway>enable
Gateway#configure terminal
Gateway(config)#interface gigabitEthernet 0/0
Gateway((config-if)#ip address 192.168.1.254 255.255.255.0
Gateway(config-if)#no shutdown
```

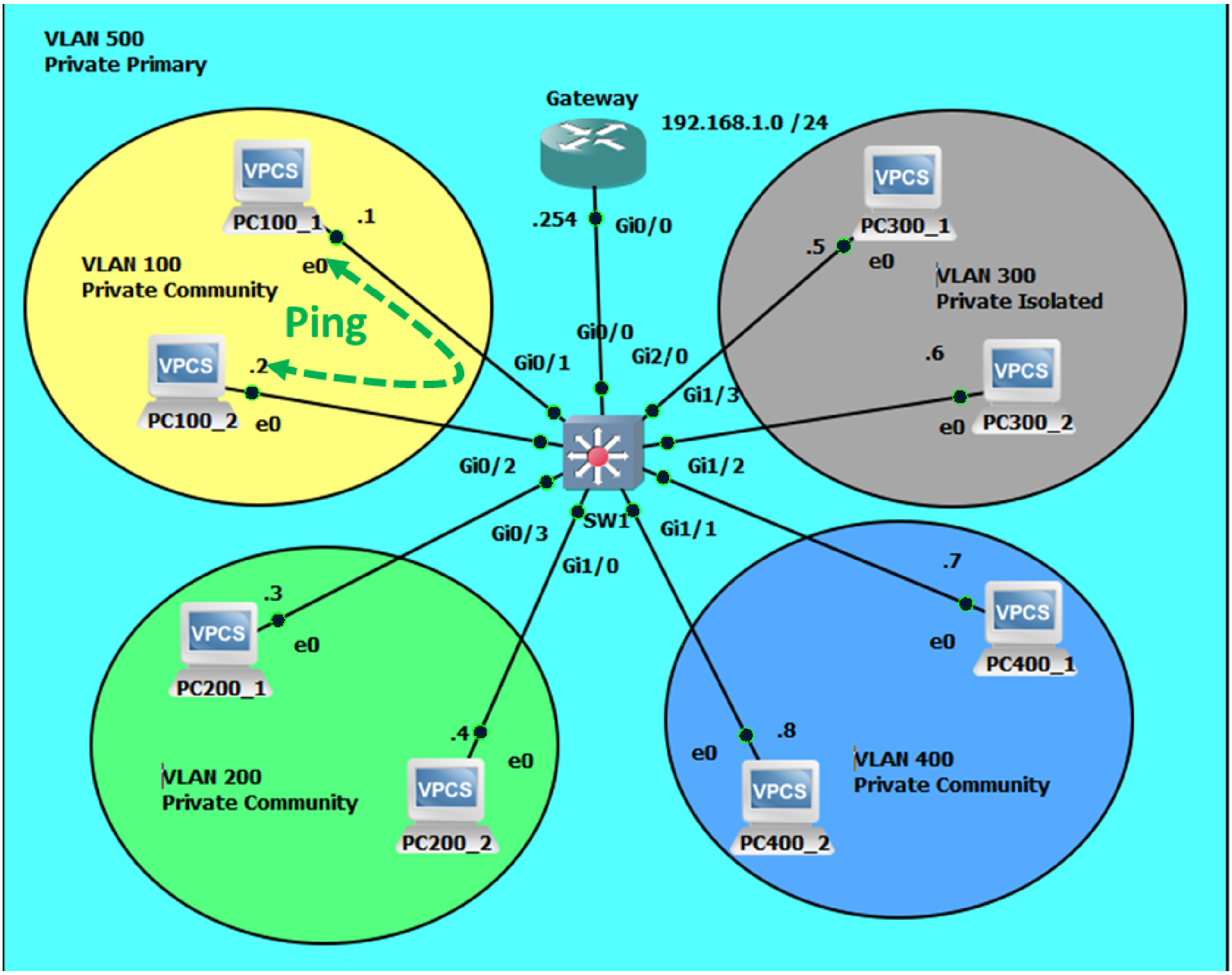
SW1

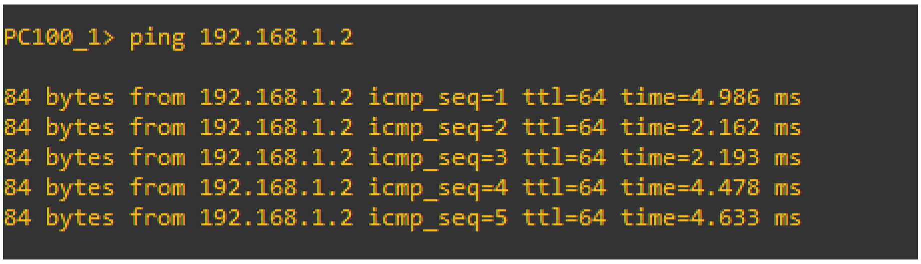
```
SW1>enable
SW1#configure terminal
SW1(config)#vtp mode transparent
SW1(config)#vlan 100
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit
SW1(config)#vlan 200
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit
SW1(config)#vlan 300
SW1(config-vlan)#private-vlan isolated
SW1(config-vlan)#exit
SW1(config)#vlan 400
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit
SW1(config)#vlan 500
SW1(config-vlan)#private-vlan primary
SW1(config-vlan)#private-vlan association 100,200,300,400
SW1(config-vlan)#exit
SW1(config)#interface gigabitEthernet g0/1
SW1(config-if)#switchport mode private-vlan host
SW1(config-if)#switchport private-vlan host-association 500 100
SW1(config)#interface gigabitEthernet g0/2
SW1(config-if)#switchport mode private-vlan host
SW1(config-if)#switchport private-vlan host-association 500 100
SW1(config)#interface gigabitEthernet g0/3
SW1(config-if)#switchport mode private-vlan host
SW1(config-if)#switchport private-vlan host-association 500 200
SW1(config)#interface gigabitEthernet g1/0
SW1(config-if)#switchport mode private-vlan host
SW1(config-if)#switchport private-vlan host-association 500 200
SW1(config)#interface gigabitEthernet g2/0
SW1(config-if)#switchport mode private-vlan host
SW1(confi-if)#switchport private-vlan host-association 500 300
SW1(config)#interface gigabitEthernet g1/3
SW1(config-if)#switchport mode private-vlan host
SW1(confi-if)#switchport private-vlan host-association 500 300
SW1(config)#interface gigabitEthernet g1/2
SW1(config-if)#switchport mode private-vlan host
SW1(confi-if)#switchport private-vlan host-association 500 400
SW1(config)#interface gigabitEthernet g1/1
SW1(config-if)#switchport mode private-vlan host
SW1(confi-if)#switchport private-vlan host-association 500 400
SW1(config)#interface gigabitEthernet g0/0
SW1(config-if)#switchport mode private-vlan promiscuous
SW1(confi-if)#switchport private-vlan mapping 500 100,200,300,400
```

SW1(confi-if)#end

Illustrated Scenarios

Intra-community VLAN Communication will be **Successful**.

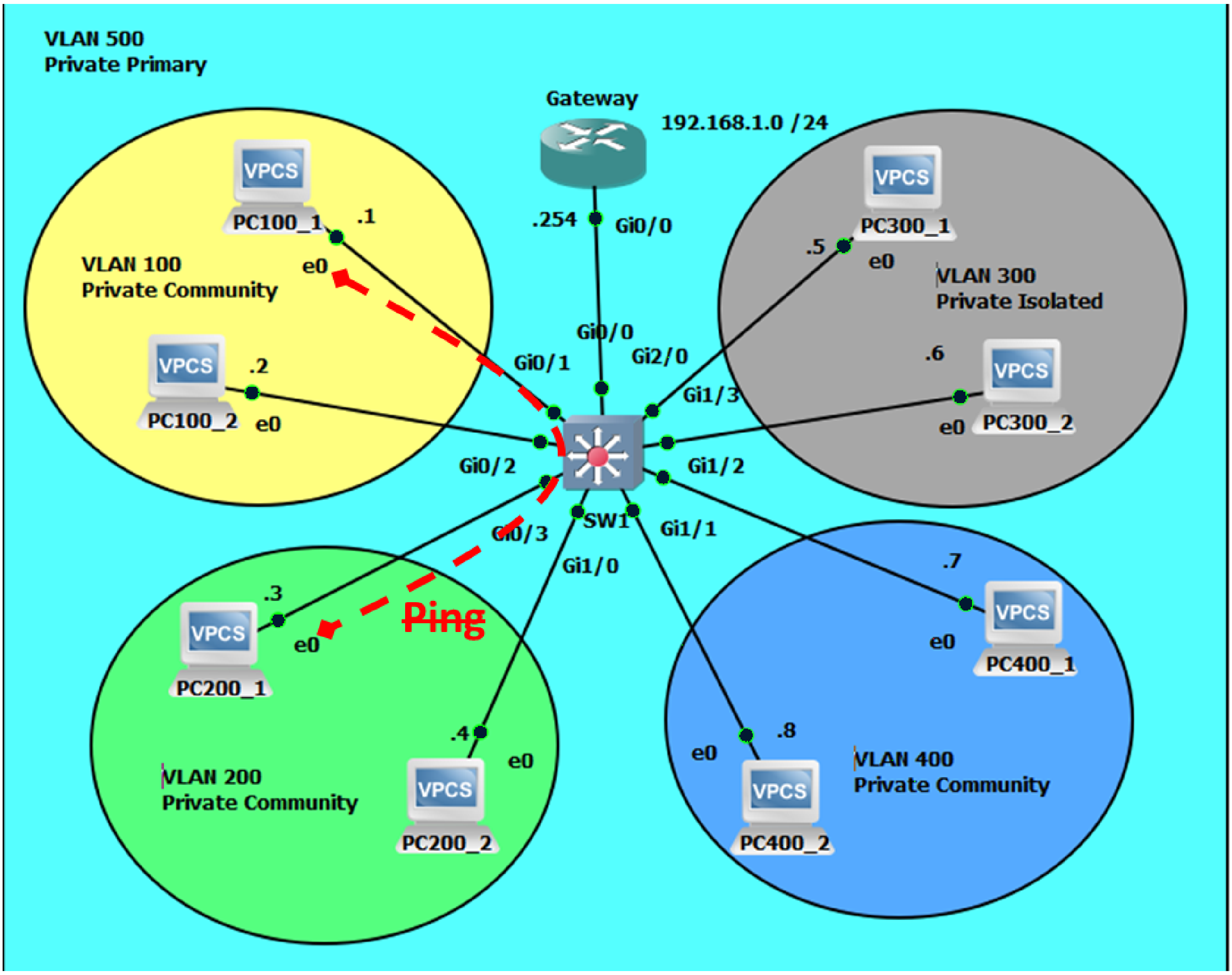


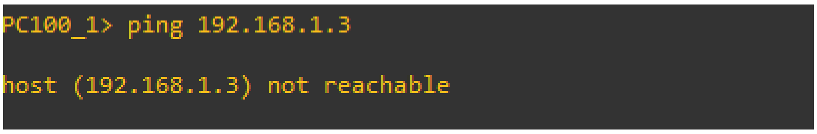


```
PC100_1> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=4.986 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=2.162 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=2.193 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=4.478 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=4.633 ms
```

Extra-community VLAN Communication will **Fail**.

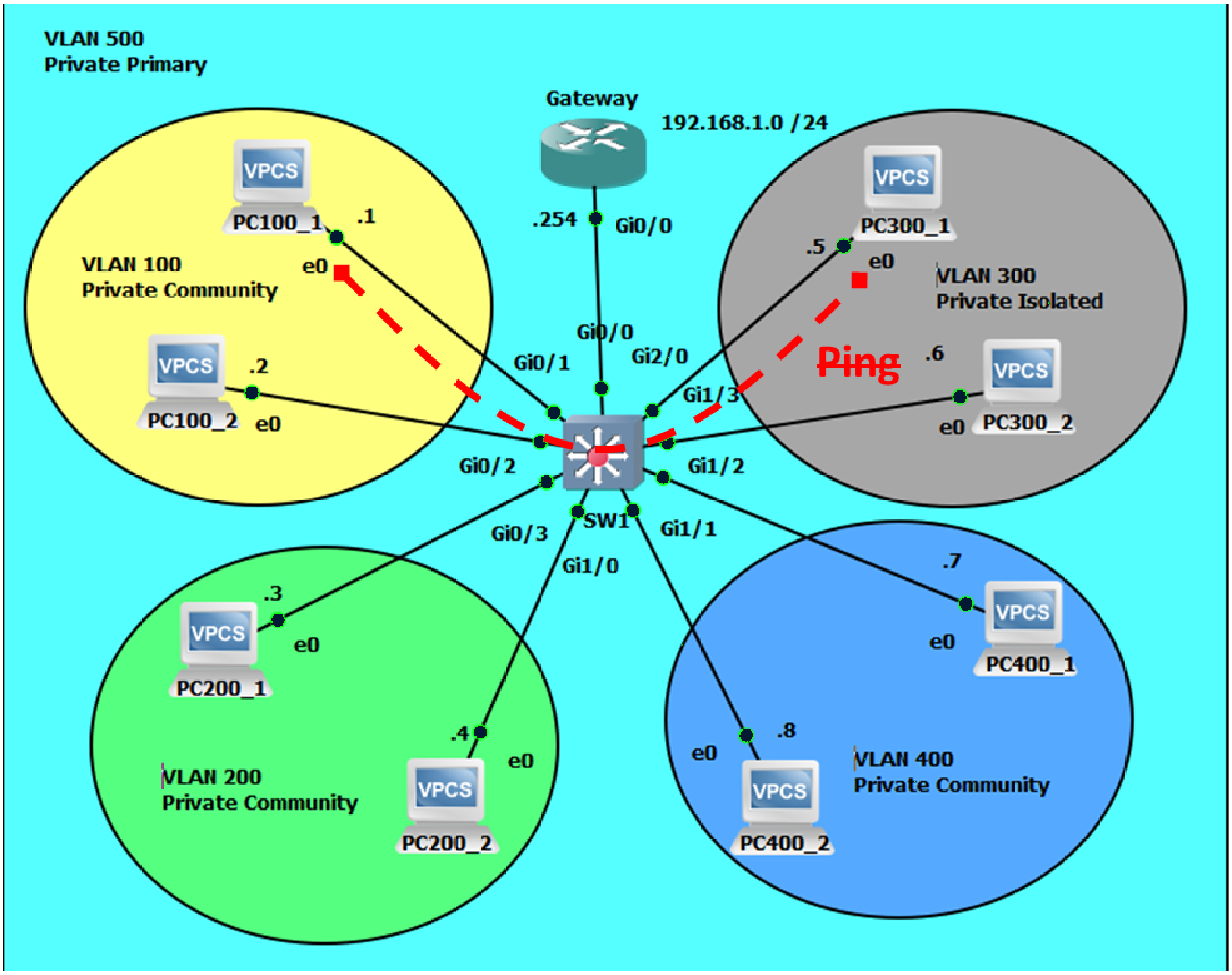


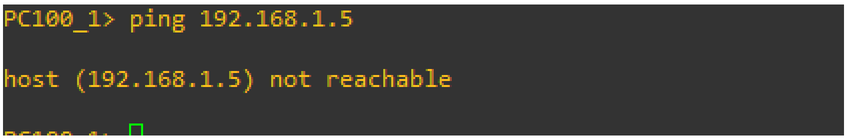


```
PC100_1> ping 192.168.1.3

host (192.168.1.3) not reachable
```

Community-isolated Communications will **Fail**.



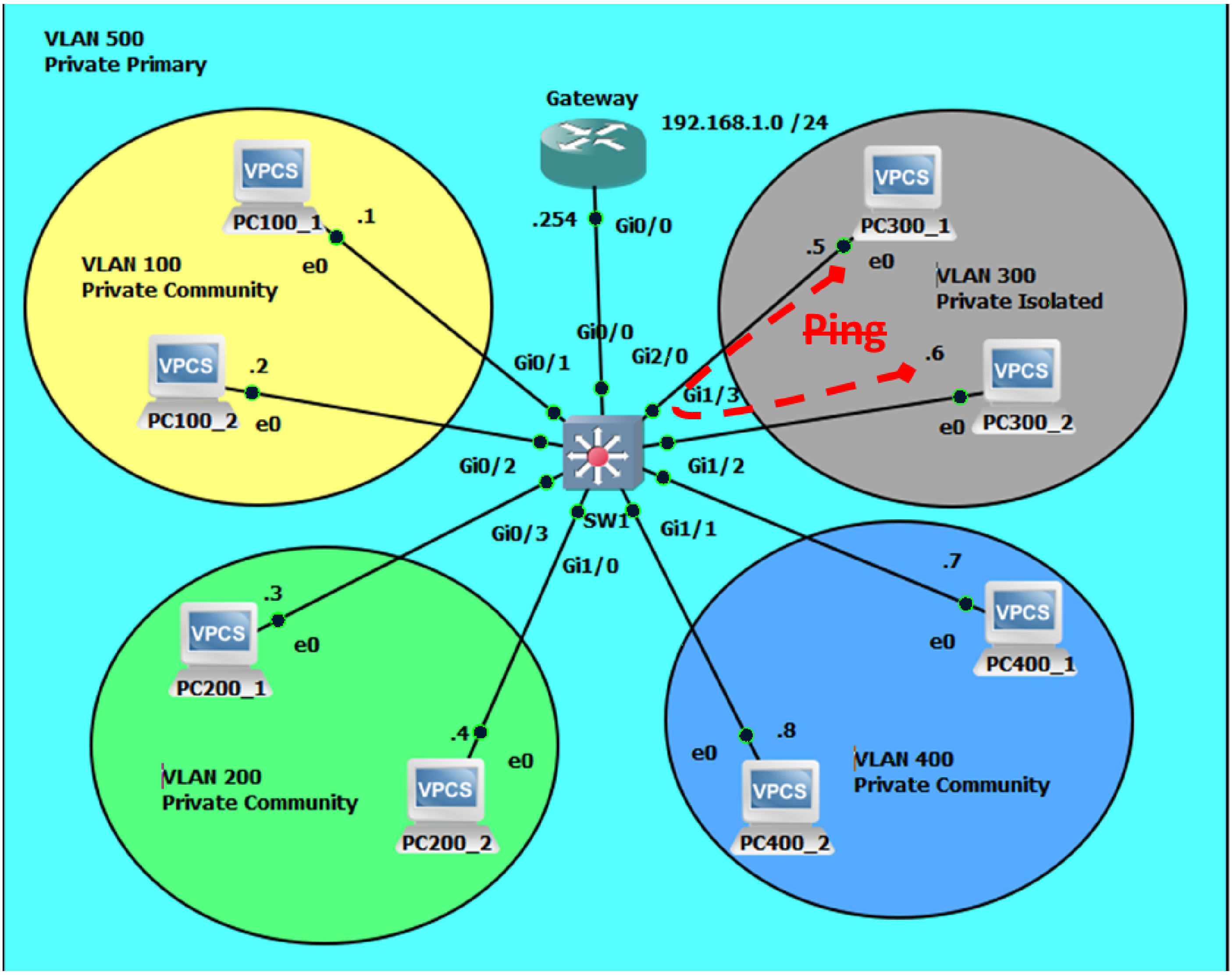


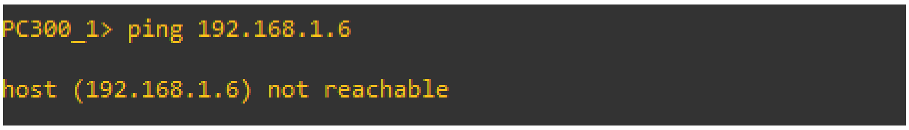
```
PC100_1> ping 192.168.1.5

host (192.168.1.5) not reachable

PC100_1>
```

Intra-isolated Communications will **Fail**.

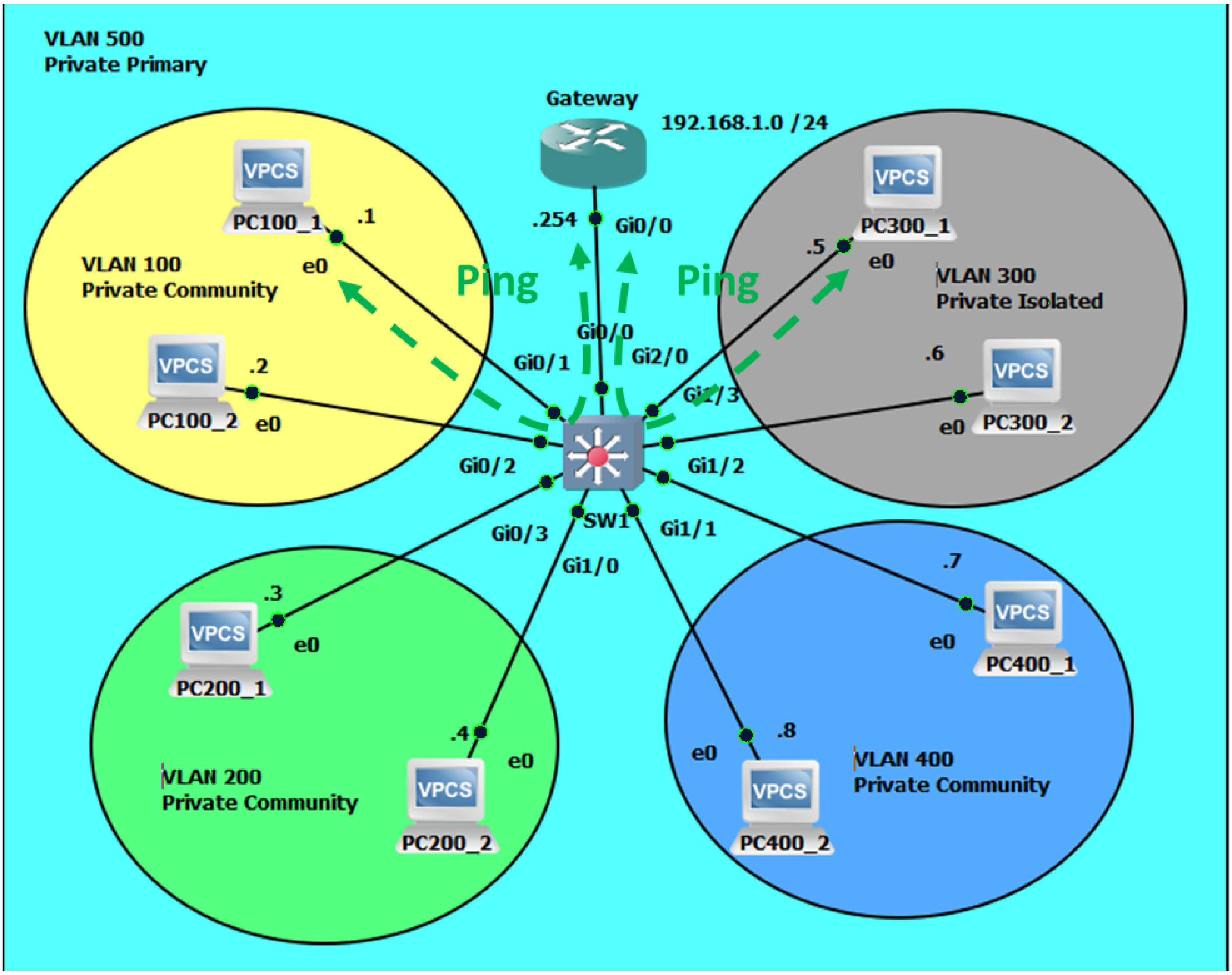


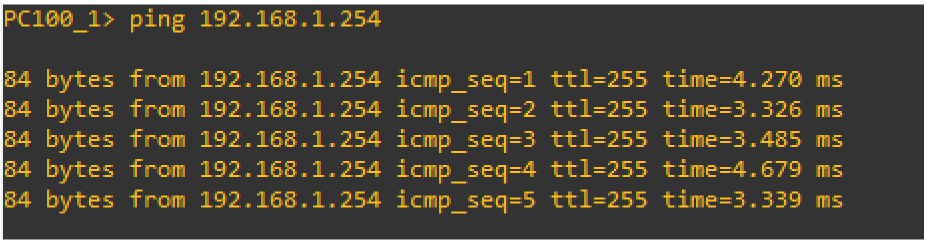


```
PC300_1> ping 192.168.1.6

host (192.168.1.6) not reachable
```

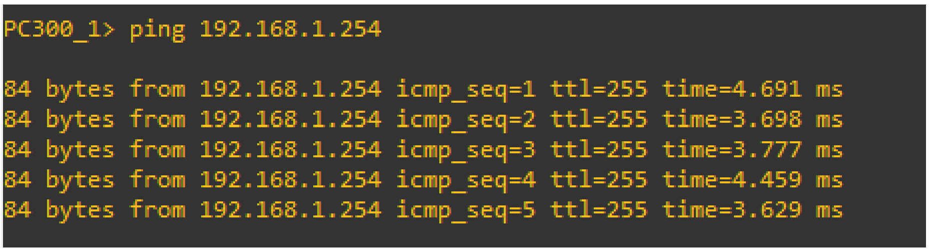
Community-gateway Communicatons will be **Successful**.
Isolated-gateway Communications will also be **Successful**.





```
PC100_1> ping 192.168.1.254

84 bytes from 192.168.1.254 icmp_seq=1 ttl=255 time=4.270 ms
84 bytes from 192.168.1.254 icmp_seq=2 ttl=255 time=3.326 ms
84 bytes from 192.168.1.254 icmp_seq=3 ttl=255 time=3.485 ms
84 bytes from 192.168.1.254 icmp_seq=4 ttl=255 time=4.679 ms
84 bytes from 192.168.1.254 icmp_seq=5 ttl=255 time=3.339 ms
```



```
PC300_1> ping 192.168.1.254

84 bytes from 192.168.1.254 icmp_seq=1 ttl=255 time=4.691 ms
84 bytes from 192.168.1.254 icmp_seq=2 ttl=255 time=3.698 ms
84 bytes from 192.168.1.254 icmp_seq=3 ttl=255 time=3.777 ms
84 bytes from 192.168.1.254 icmp_seq=4 ttl=255 time=4.459 ms
84 bytes from 192.168.1.254 icmp_seq=5 ttl=255 time=3.629 ms
```

GNS3 File

private vlan 2.gns3

Revision #2
Created 22 January 2023 20:02:31 by Glen Taylor
Updated 24 January 2023 22:41:54 by Glen Taylor