

# Private VLANs

---



**Ben Piper**

AUTHOR, *CCNP ENTERPRISE CERTIFICATION STUDY GUIDE: EXAM 350-401*

[benpiper.com](http://benpiper.com)

# Module Overview



**Primary and secondary private VLANs**

**Private VLAN port types**

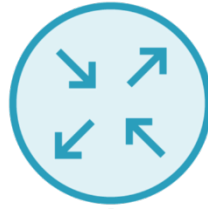
**Isolated private VLANs**

**Community private VLANs**

# Private VLANs

Defined in RFC 5517, *Cisco Systems'*  
*Private VLANs*

192.168.1.1/24

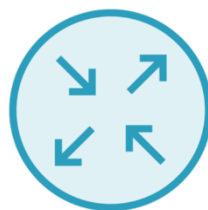


192.168.1.10/24



192.168.1.20/24

192.168.1.1/24



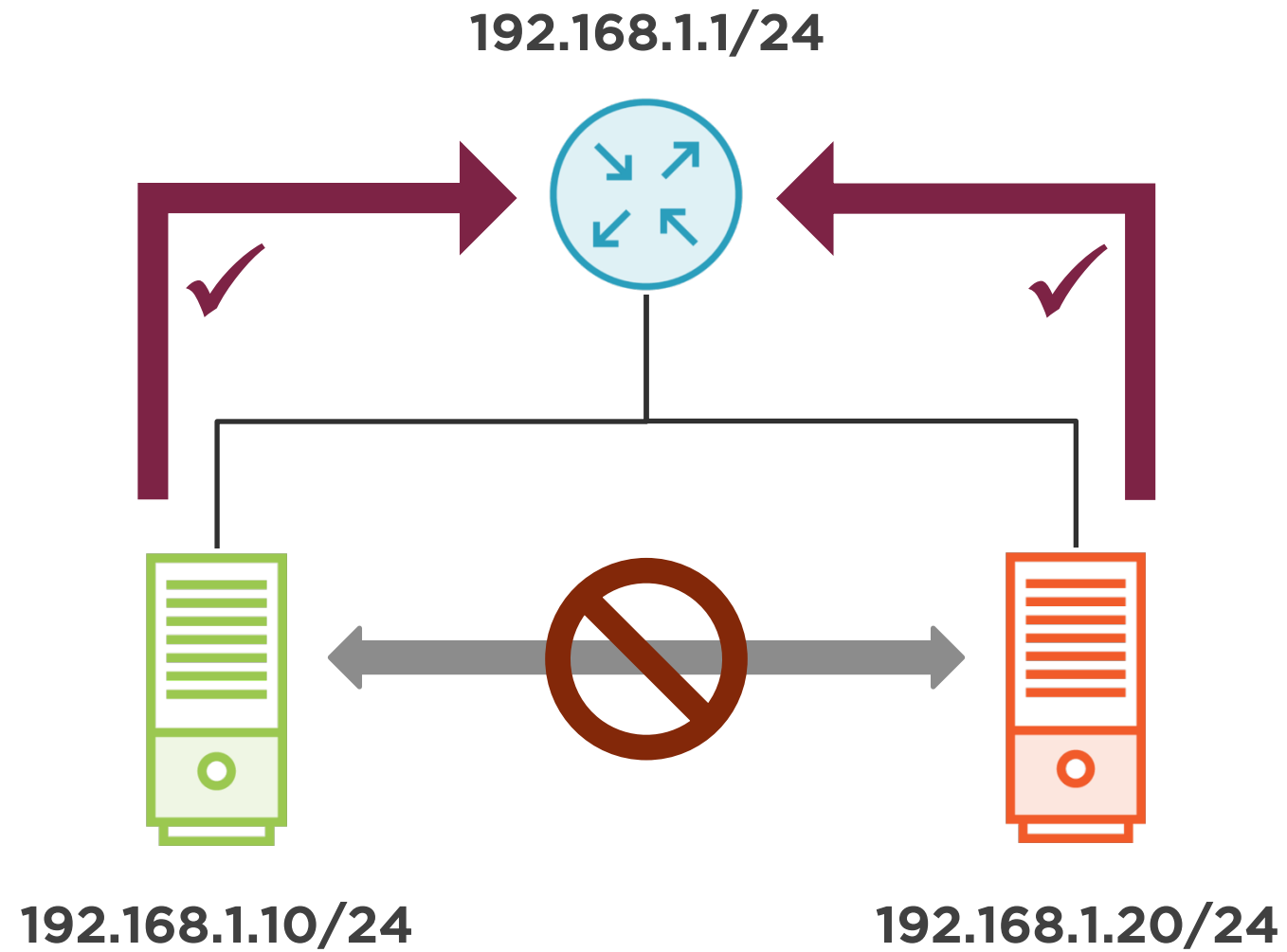
192.168.1.10/24

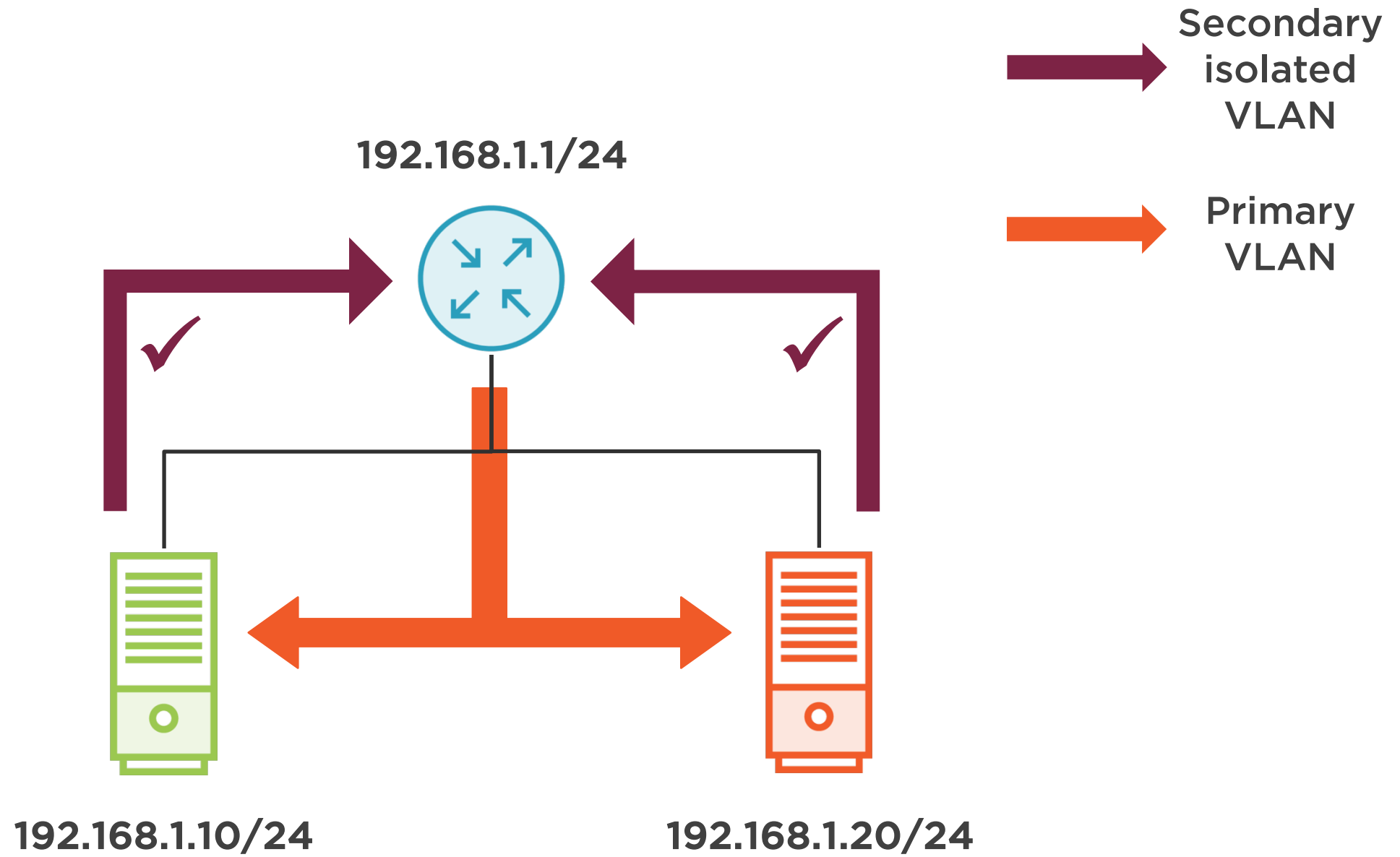


192.168.1.20/24



Secondary  
isolated  
VLAN





# Primary and Secondary VLANs

---

# Primary VLAN

**Carries traffic  
from the default  
gateway to the  
hosts**

**Identifies the  
private VLAN  
domain**

**Contains one or  
more secondary  
VLANs**

## Secondary VLAN

**Carries traffic from the hosts to the default gateway**

**Must be associated with a primary VLAN in order to function**

# Secondary VLAN

## Isolated

Hosts **cannot** communicate at layer 2

## Community

Hosts **can** communicate with other hosts in the **same** secondary VLAN

# Primary and Secondary VLANs Are Unidirectional

## Primary VLAN

Carries traffic from the default gateway  
to the hosts

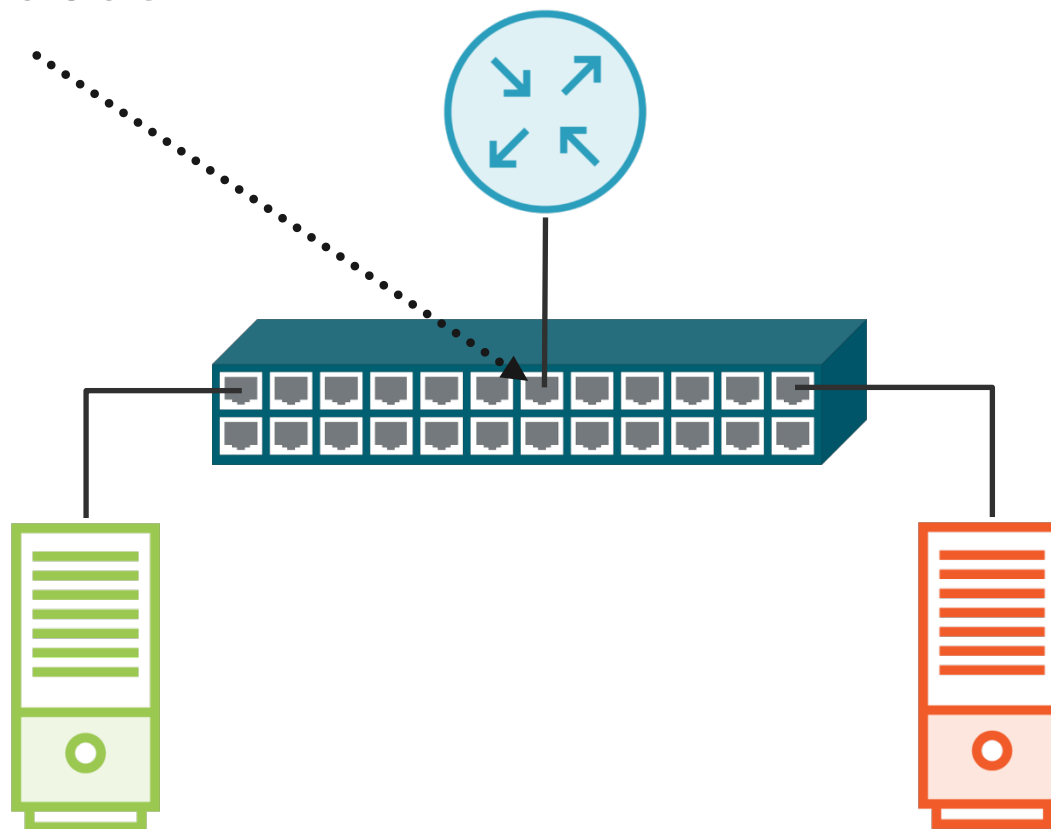
## Secondary VLAN

Carries traffic from the hosts to the  
default gateway

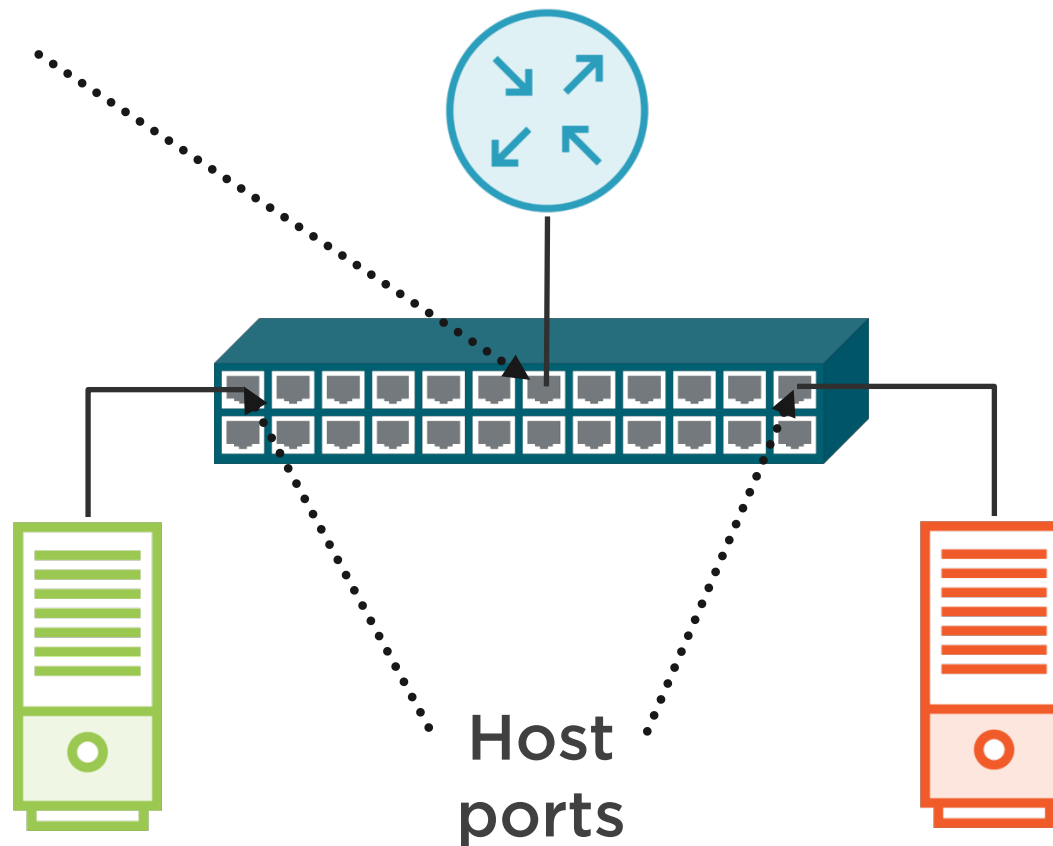
# Private VLAN Port Types

---

Promiscuous  
port

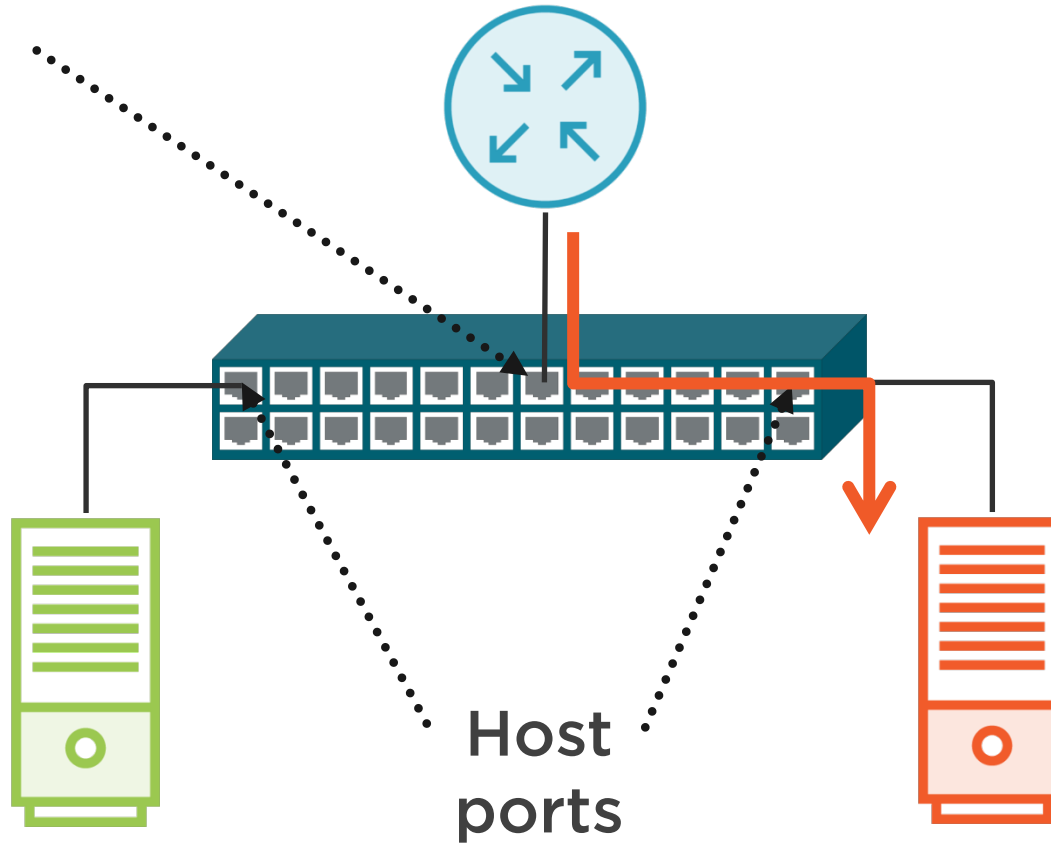


Promiscuous  
port



Host  
ports

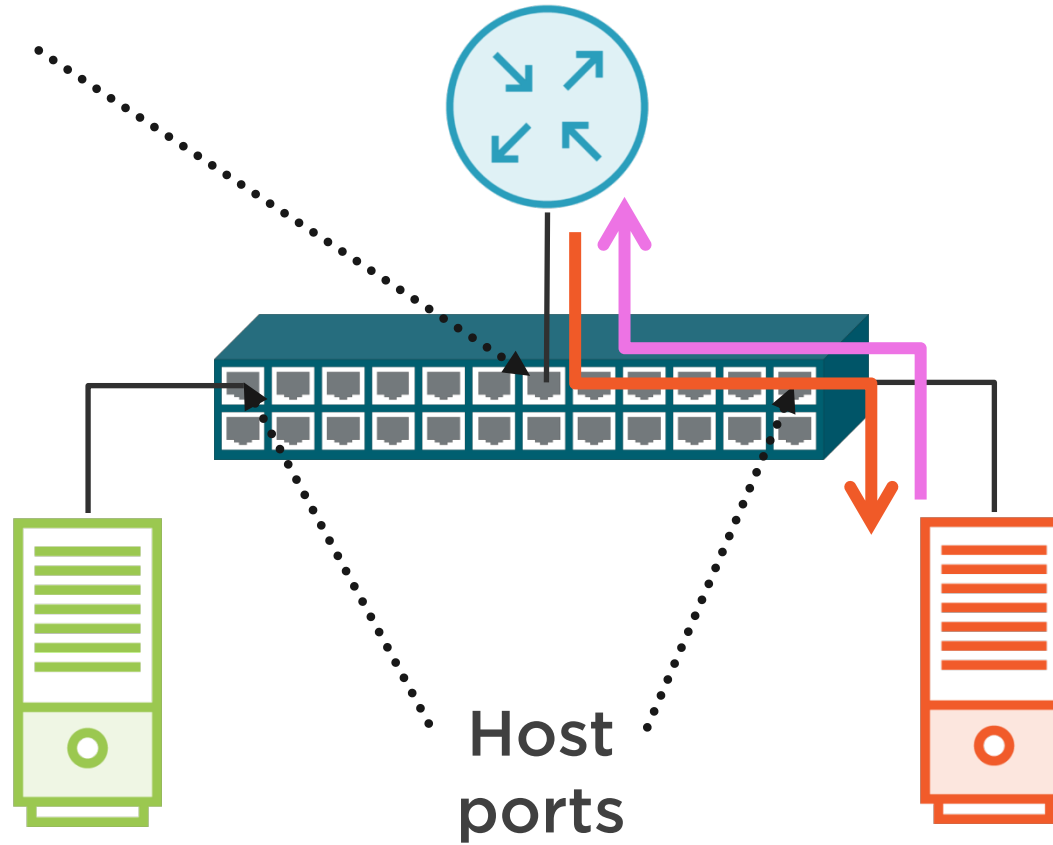
Promiscuous  
port



Host  
ports

Primary  
VLAN

Promiscuous  
port



Secondary  
isolated  
VLAN

Primary  
VLAN

# Host vs. Promiscuous Ports

## Traffic from a host port

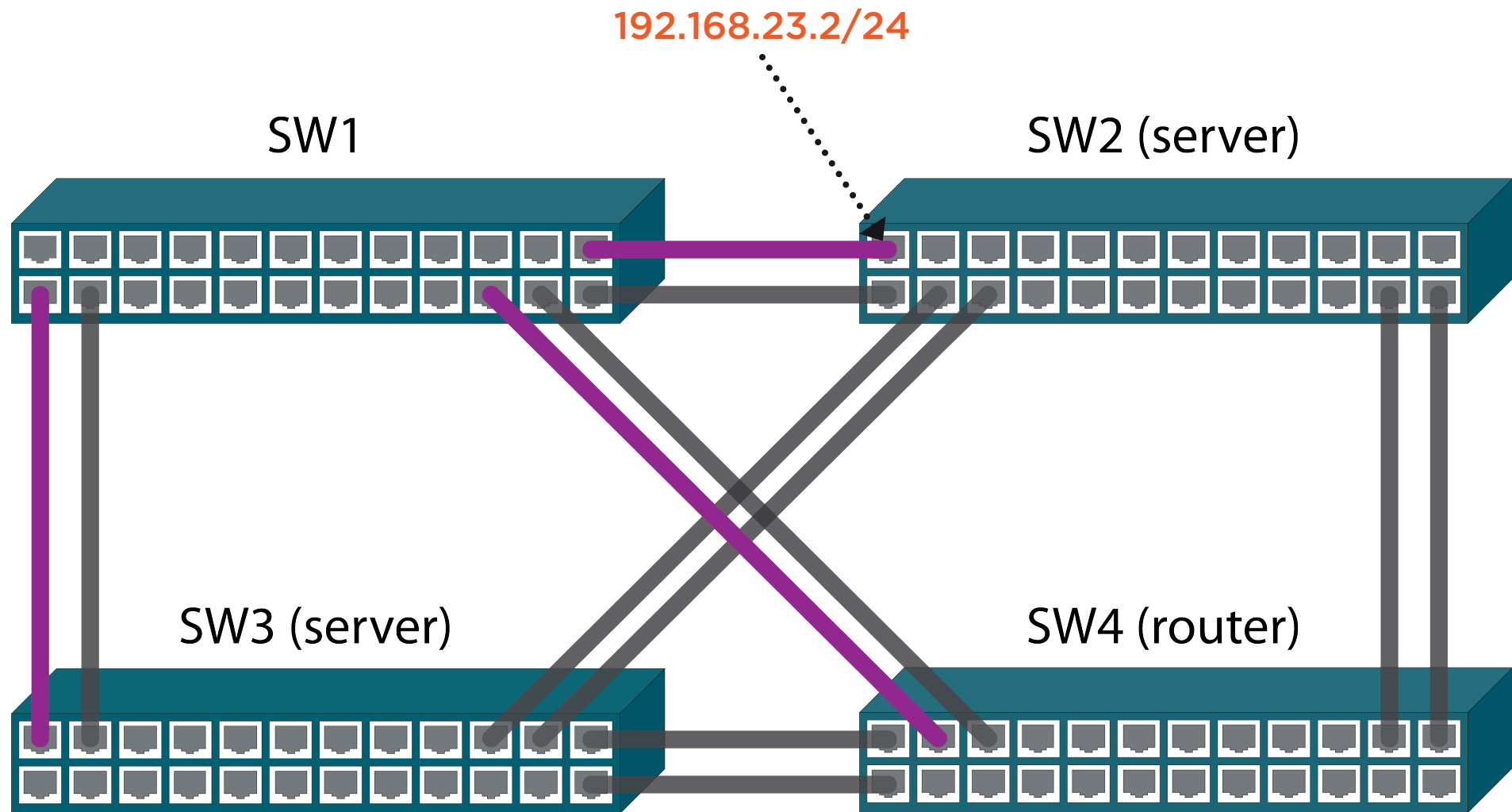
Traverses the **secondary** VLAN to reach a **promiscuous** port

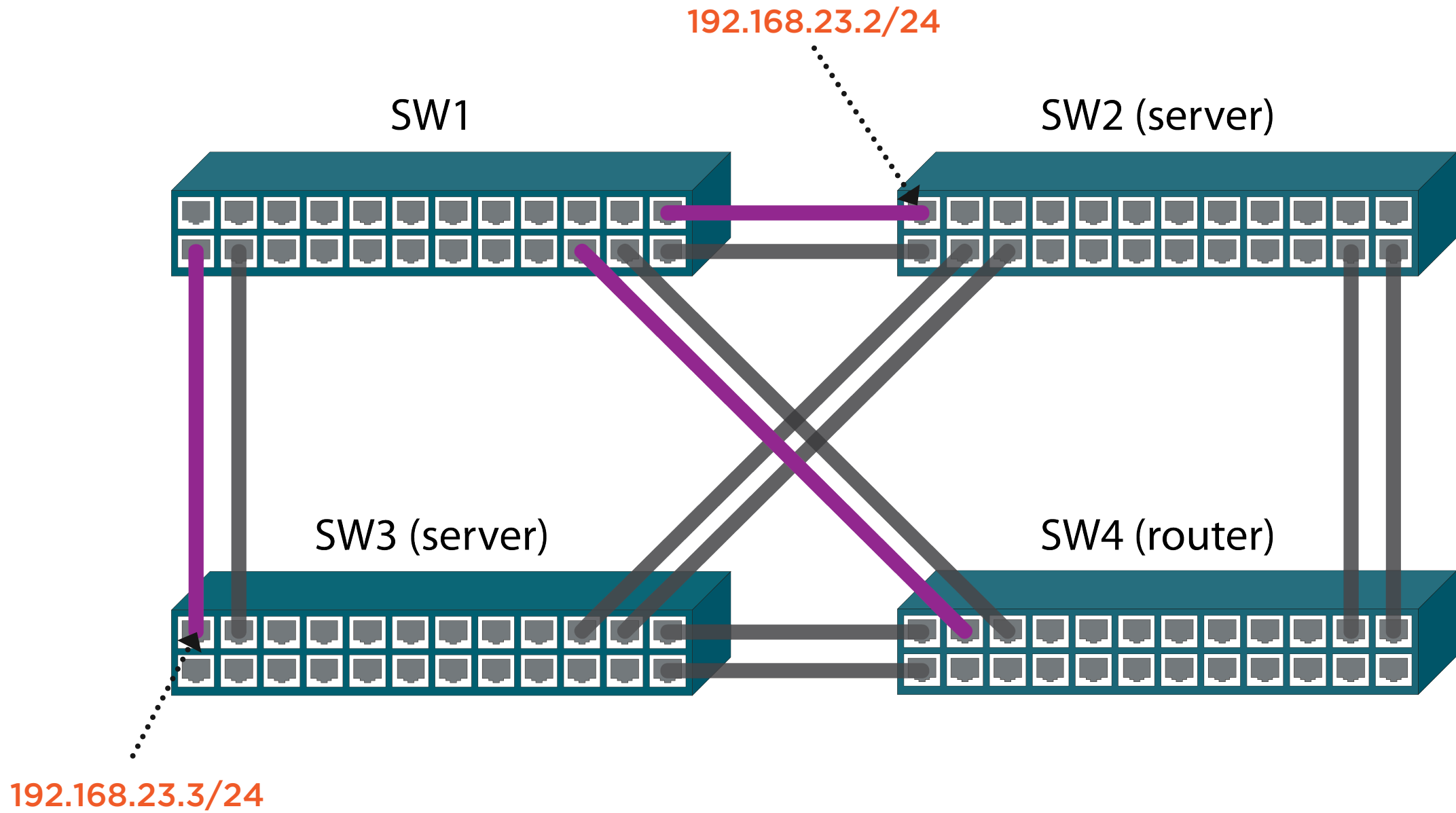
## Traffic from a promiscuous port

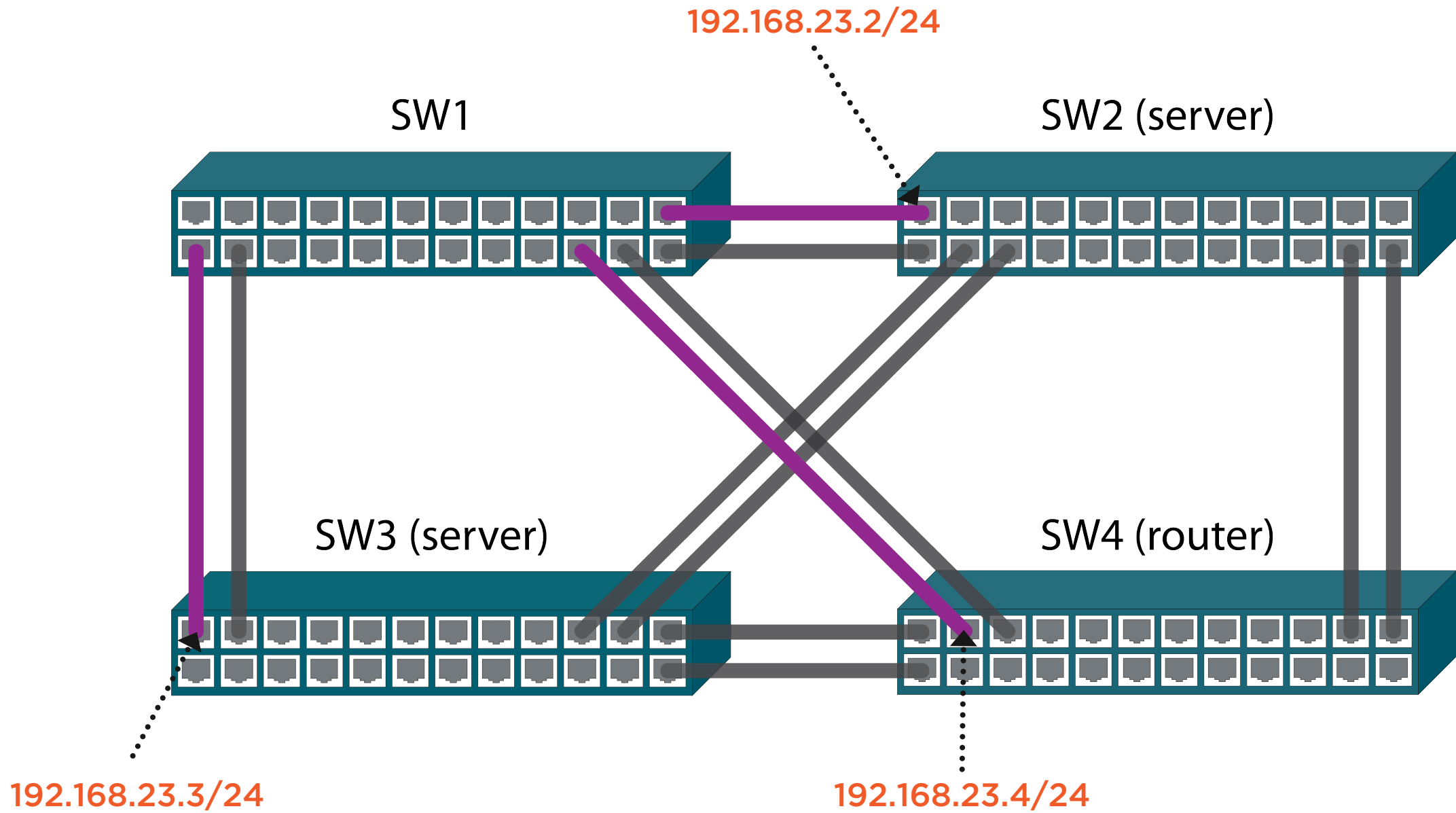
Traverses the **primary** VLAN to reach a **host** port

# Isolated Private VLANs

---



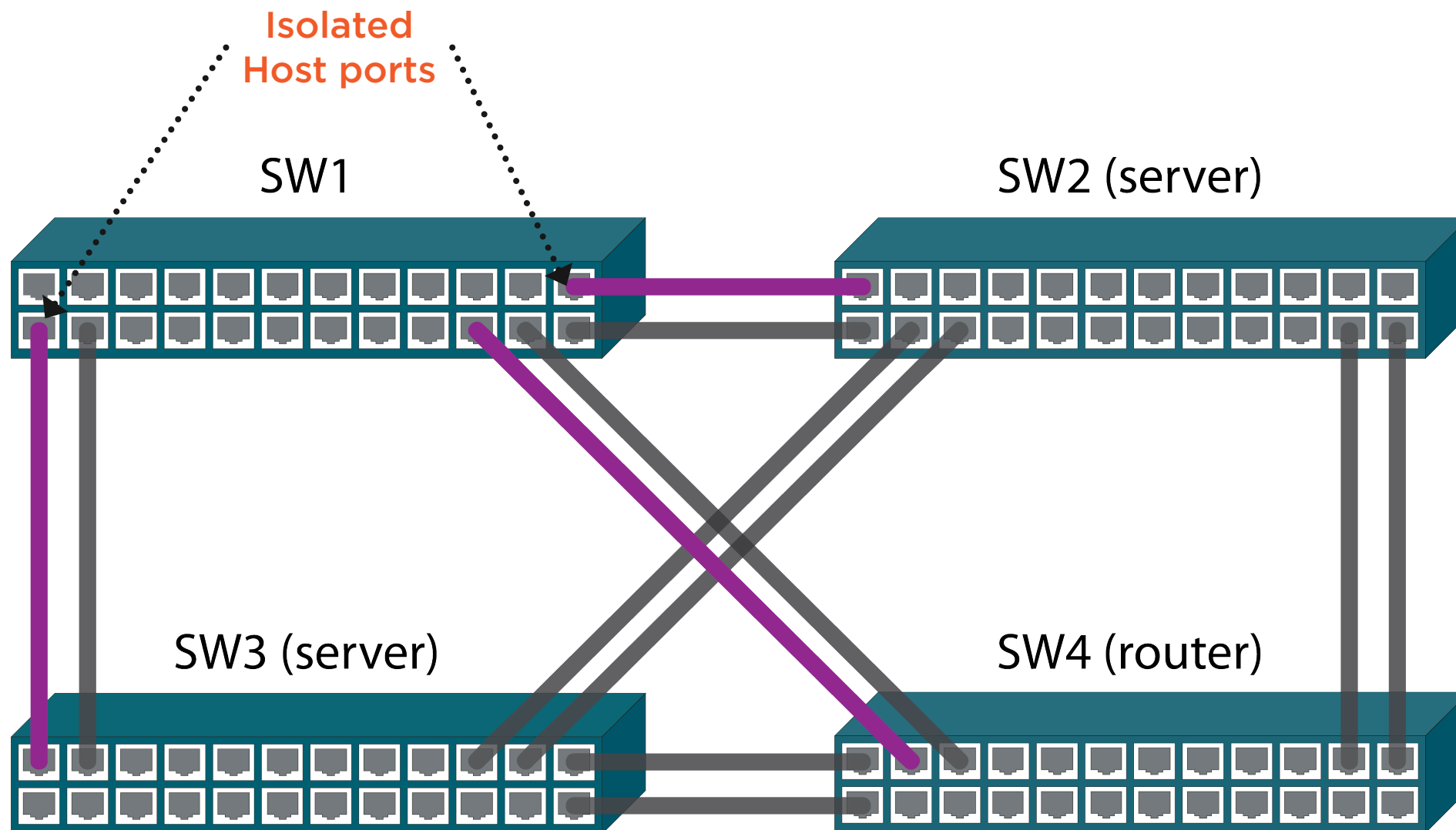


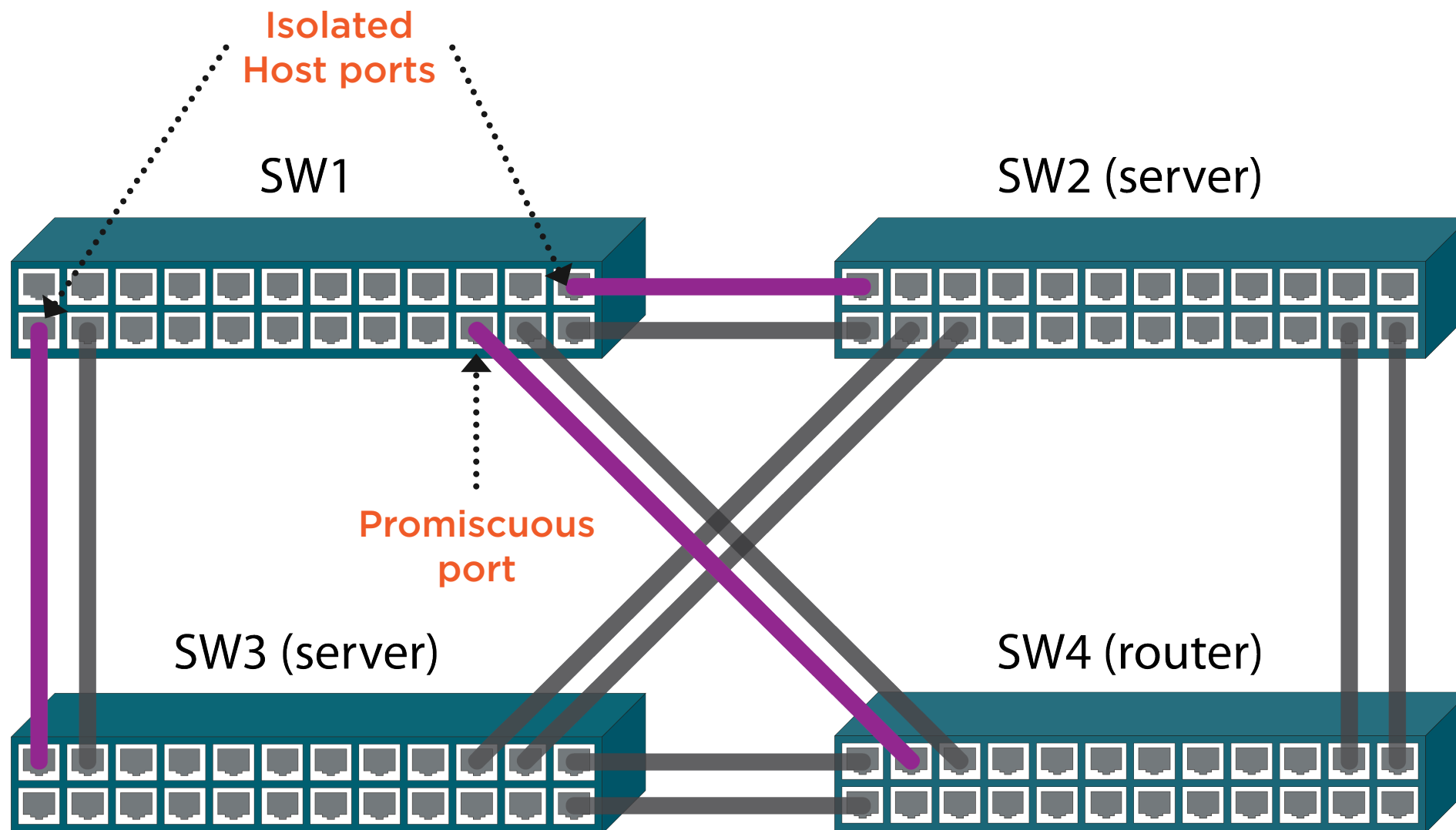


# Requirement

**Configure a private VLAN domain as follows:**

- SW2 and SW3 should not be able to ping each other
- SW2 and SW3 should be able to ping SW4





```
SW1(config)# vlan 223
```

```
SW1(config-vlan)# private-vlan isolated
```

## Configuring a Secondary Isolated VLAN

```
SW1(config)# vlan 200
```

```
SW1(config-vlan)# private-vlan primary
```

```
SW1(config-vlan)# private-vlan association 223
```

## Configuring a Primary VLAN

**Primary VLAN 200 is associated with the secondary VLAN 223**

```
SW1(config)# int fa0/20
```

```
SW1(config-if)# switchport mode private-vlan promiscuous
```

```
SW1(config-if)# switchport private-vlan mapping 200 223
```

## Configuring the Promiscuous Port

**Sets FastEthernet0/20 as a promiscuous port for primary VLAN 200 and secondary VLAN 223**

```
SW1(config)# int range fa0/2,fa0/11
```

```
SW1(config-if-range)# switchport mode private-vlan host
```

```
SW1(config-if-range)# switchport private-vlan host-association 200 223
```

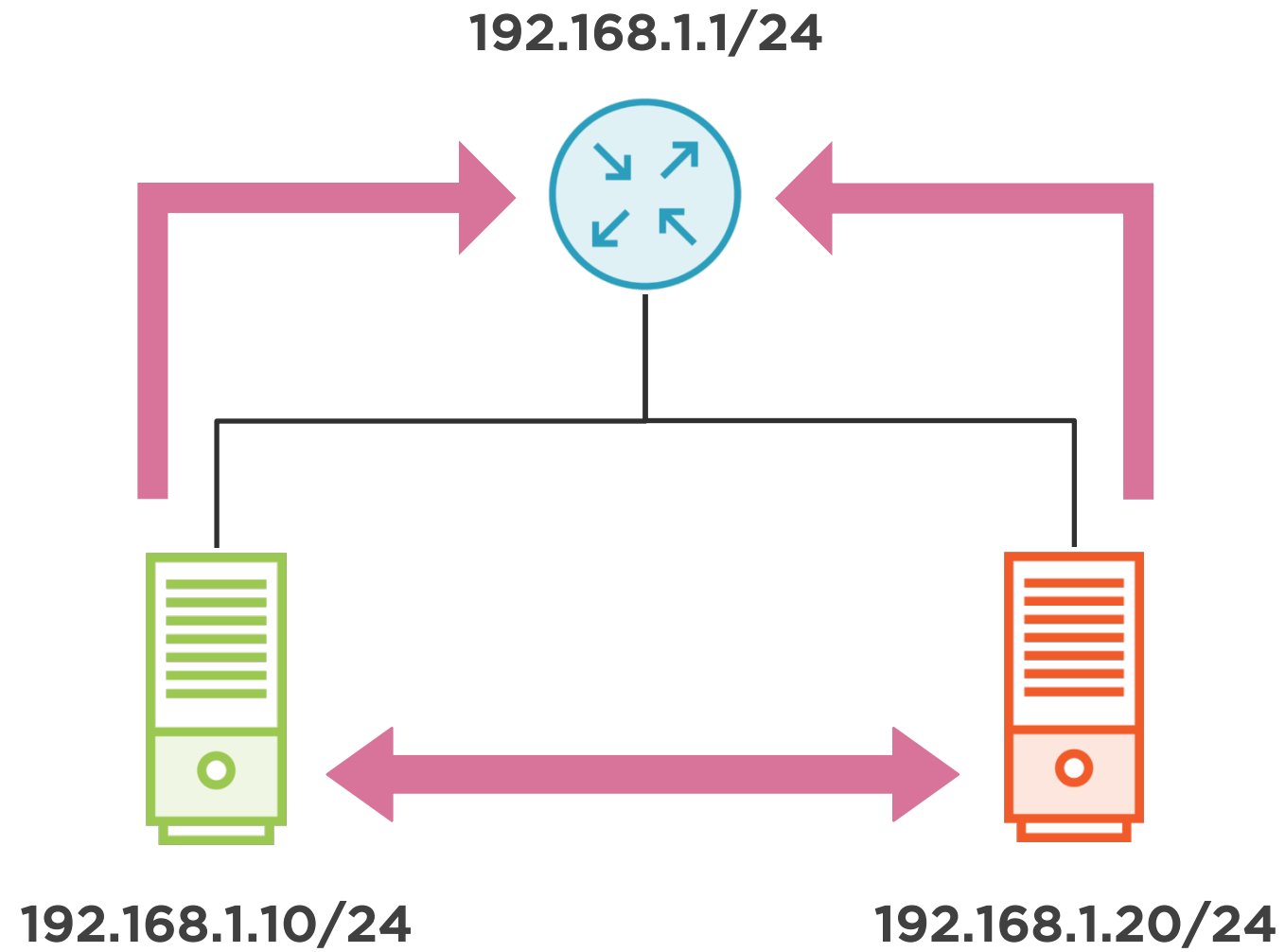
## Configuring the Host Ports

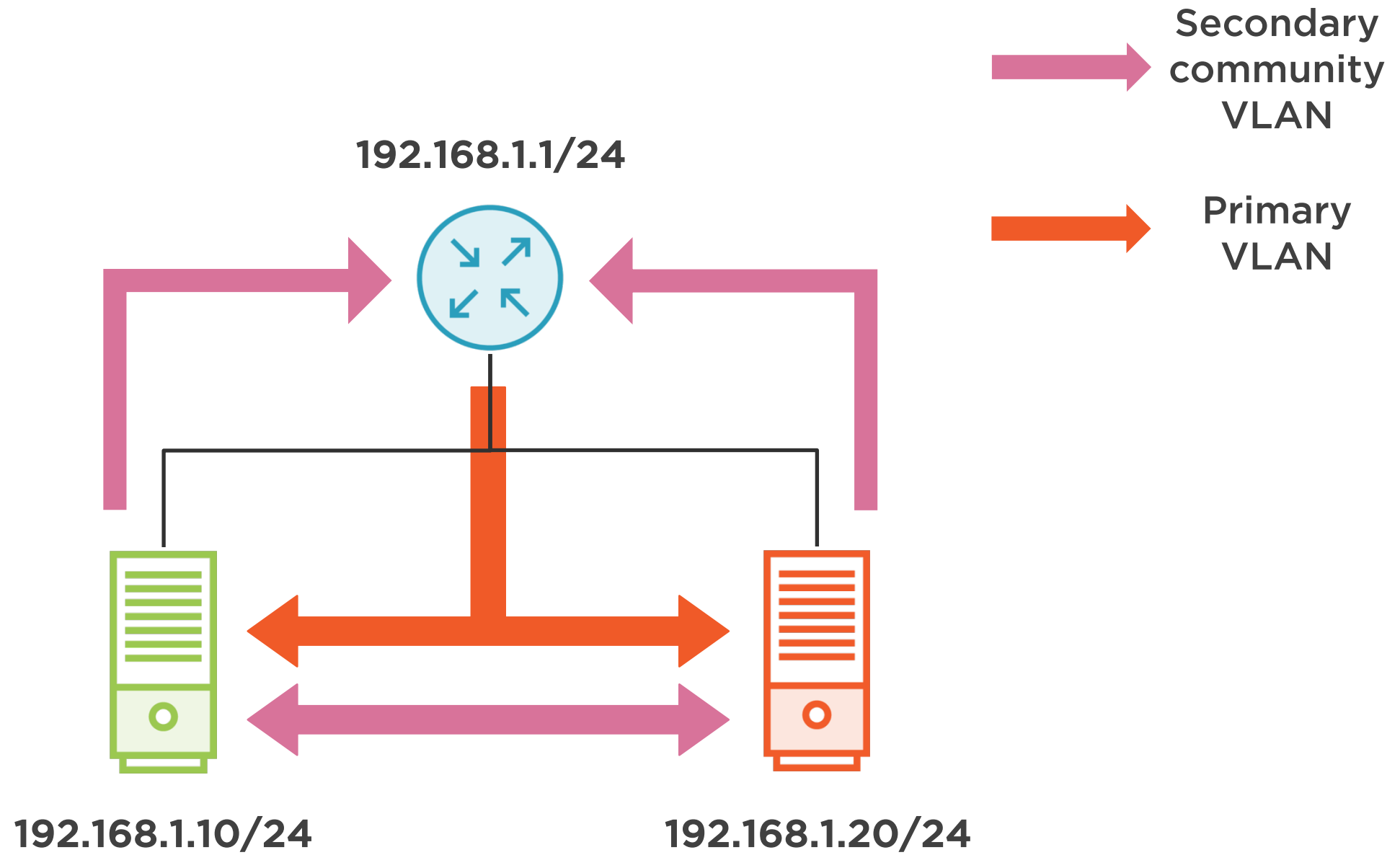
**Sets FastEthernet0/2 and 0/11 as host ports for primary VLAN 200 and secondary VLAN 223**

# Community Private VLANs

---

→ Secondary  
community  
VLAN





# Requirement

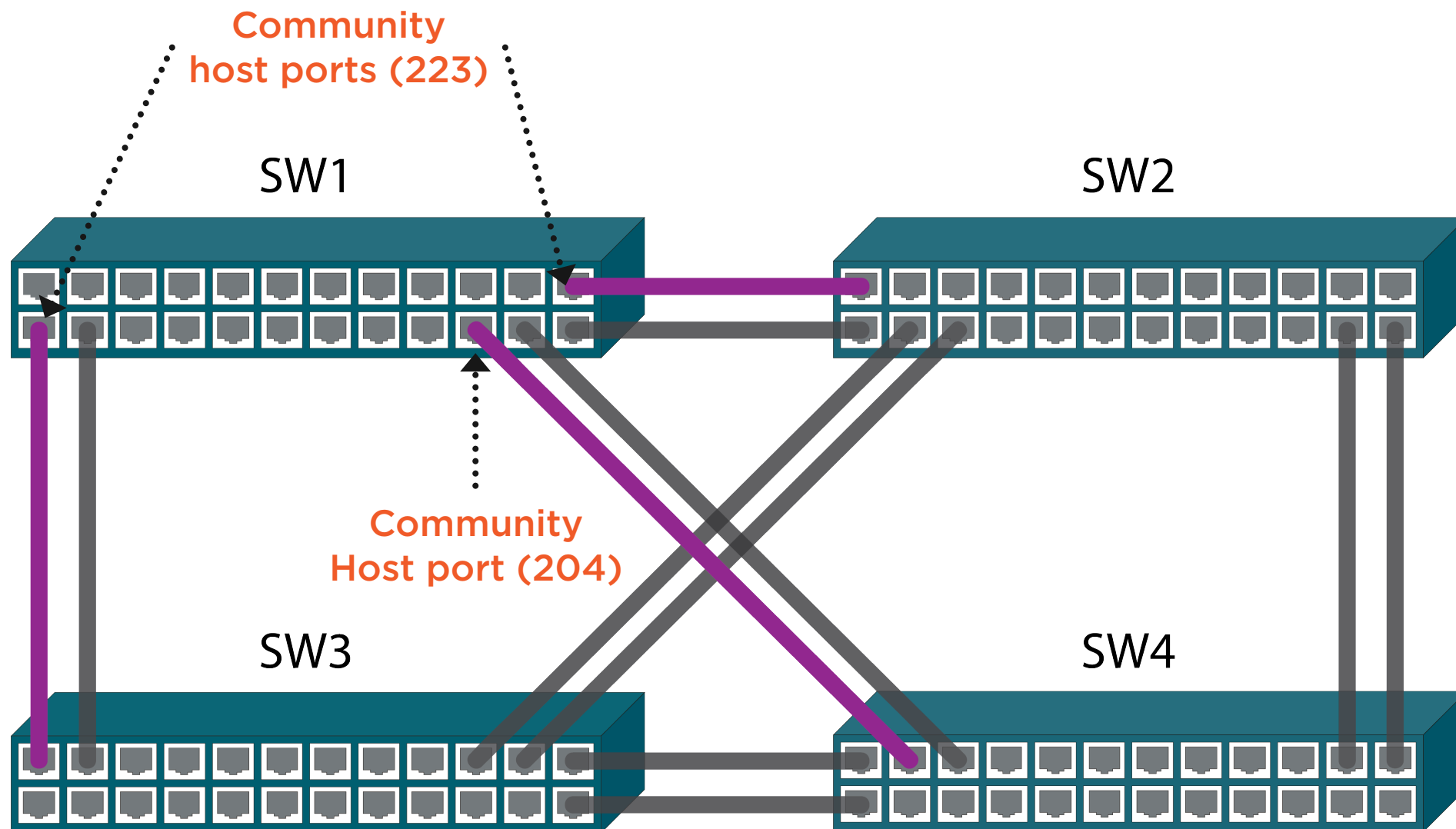
**Ensure SW2 and SW3 are in the same secondary VLAN 223**

- SW2 and SW3 should be able to ping each other, but not be able to ping SW4

**Place SW4 in secondary VLAN 204**

- Ensure SW4 can communicate with any future devices in the same secondary VLAN

**Both secondary VLANs should associated with primary VLAN 200**



```
SW1(config)# vlan 204
```

```
SW1(config-vlan)# private-vlan community
```

## Configuring a Secondary Community VLAN

```
SW1(config)# vlan 200
```

```
SW1(config-vlan)# private-vlan association add 204
```

## Adding a Secondary VLAN Association

The **add** keyword maps an additional secondary VLAN to a primary VLAN without removing any existing secondary VLANs.

# Summary

---

# Summary



What does a private VLAN domain consist of and how do you identify it?

It consists of a primary and at least one secondary VLAN

The primary VLAN ID identifies the private VLAN domain

# Summary



What does the secondary VLAN do?

It carries layer 2 traffic from the hosts to the promiscuous port

# Summary



**What is an isolated VLAN?**

**A type of secondary VLAN that does not allow layer 2 traffic between hosts within the VLAN**

# Summary



**What is a community VLAN?**

**A type of secondary VLAN that allows layer 2 traffic between hosts within the VLAN**

# Summary



Can layer 2 traffic from one community VLAN cross over to another community VLAN?

No, traffic can flow freely only within the VLAN

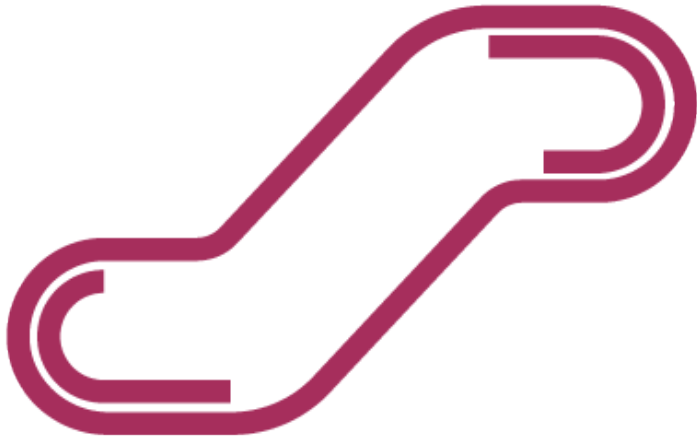
# Summary



**What is a promiscuous port?**

**A port that can send traffic to any host port in any isolated or community VLAN**

# Summary



**What is the role of the primary VLAN?**

**To carry traffic from the promiscuous port down to the host ports**

# Summary



**Are primary and secondary VLANs  
bidirectional or unidirectional?**

**Unidirectional between host and  
promiscuous ports**

## In the Next Module



**We're going to cover manual  
VLAN trunking!**