

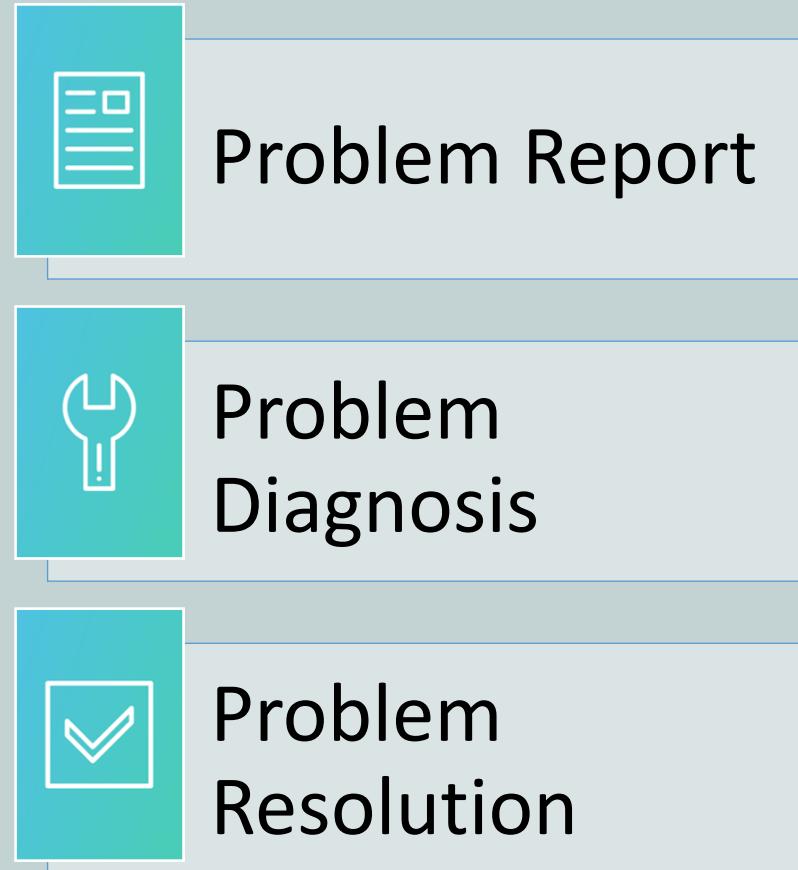


# Troubleshooting Methodology

CompTIA Network+ (N10-007)

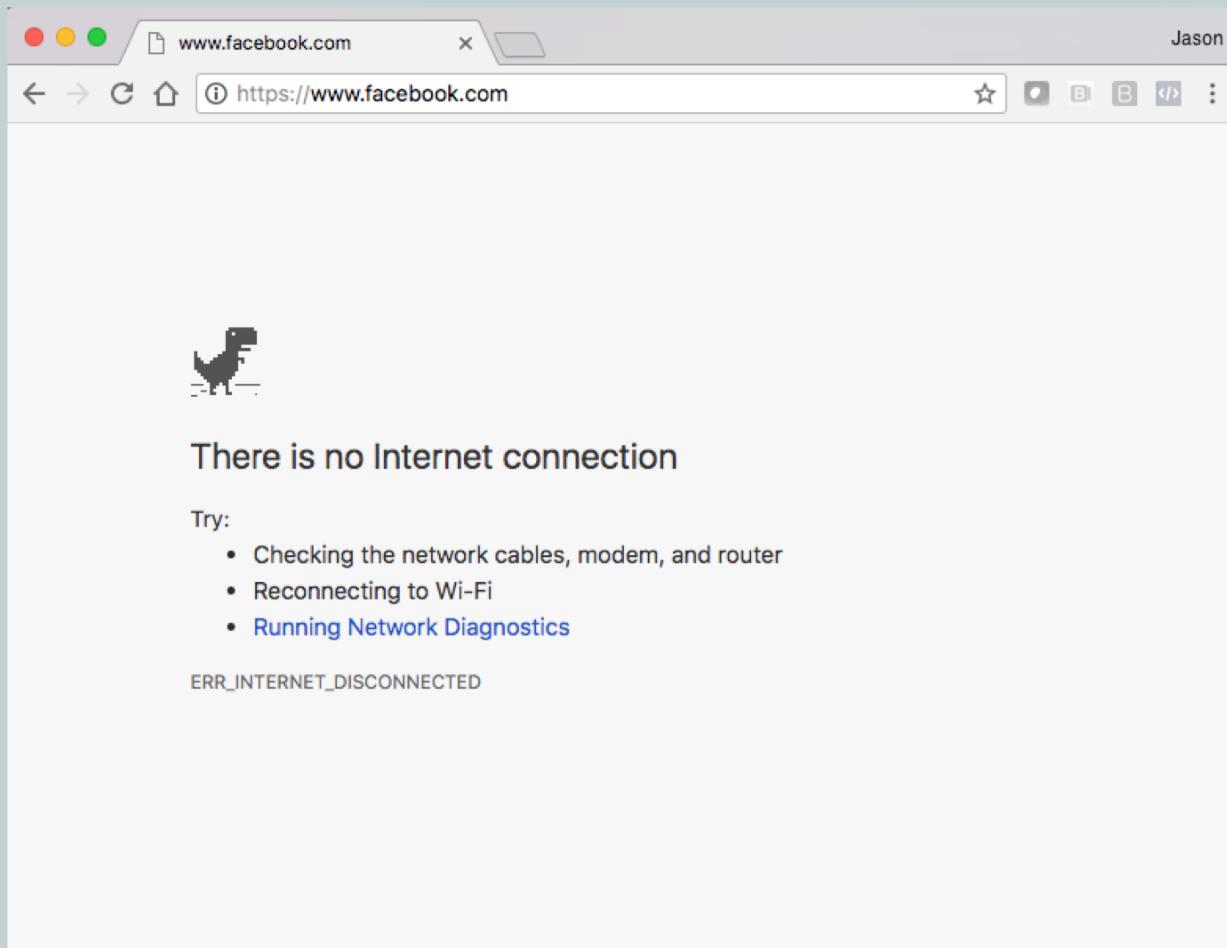
# Troubleshooting Methodology

- Troubleshooting occurs through a three step process



# Problem Report

- Issues are reported either by the end user, by administrators, or by automated systems



# Problem Diagnosis

- Majority of a troubleshooter's efforts are spent diagnosing the problem



Collect information



Examine collected information



Eliminate potential causes



Hypothesize underlying cause



Verify hypothesis



# Problem Resolution

- Occurs once the problem is fixed
- Note it in your trouble ticket system
- Verify user is happy with the resolution

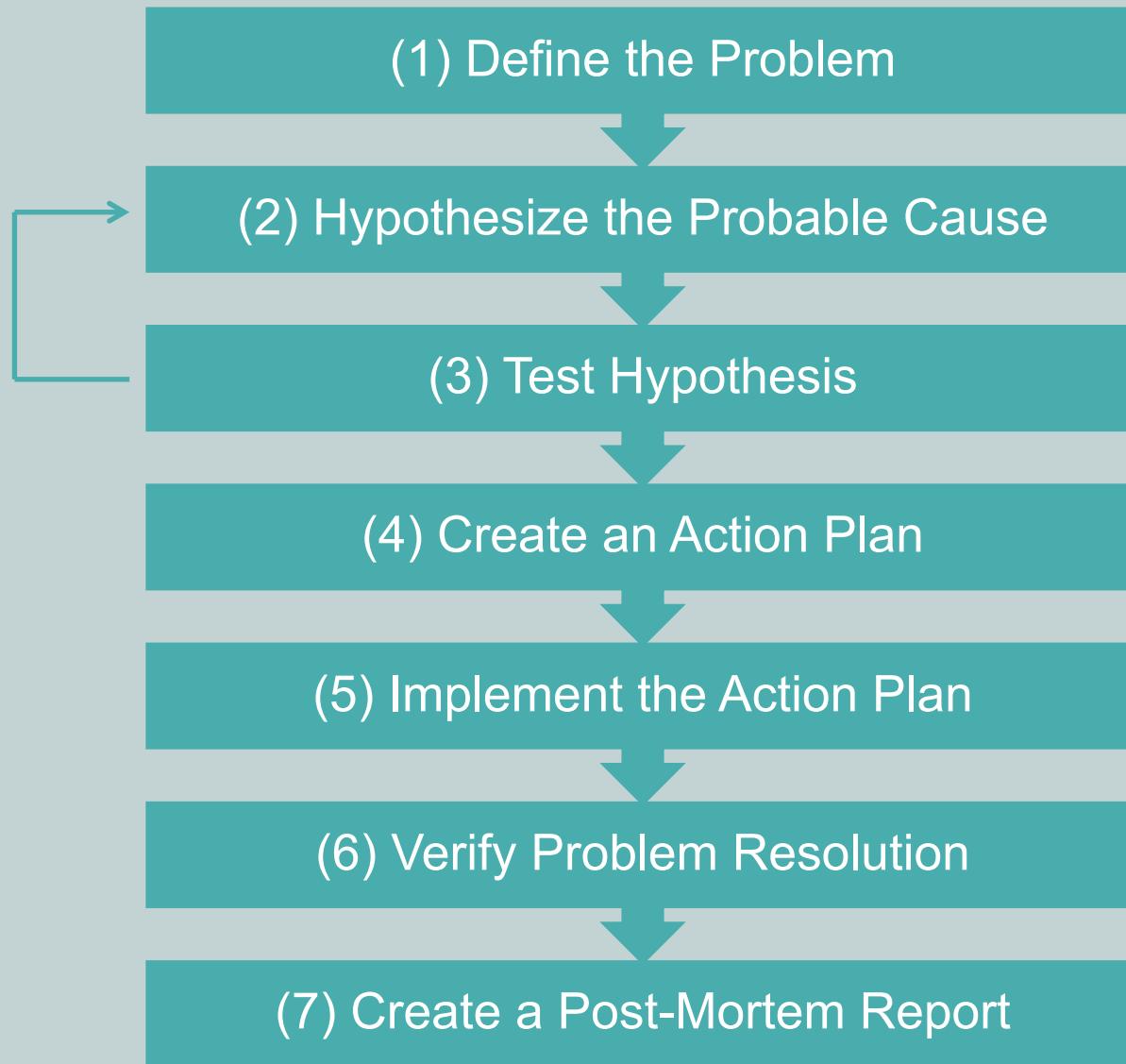


# Why Use A Structured Approach to Troubleshooting?

- Using a structured approach saves time and is repeatable
- Prevents the technician from “hunting and pecking” for the solution
- Many approaches that could be used but for the Network+ exam you **must** use CompTIA’s methodology



# CompTIA's Troubleshooting Methodology





# Troubleshooting (Layer 1)

CompTIA Network+ (N10-007)

# Network Troubleshooting

- Resolving network issues is one of the main roles of a network administrator
- Network Issue Categories
  - Physical Layer
  - Data Link Layer
  - Network Layer
  - Wireless Network



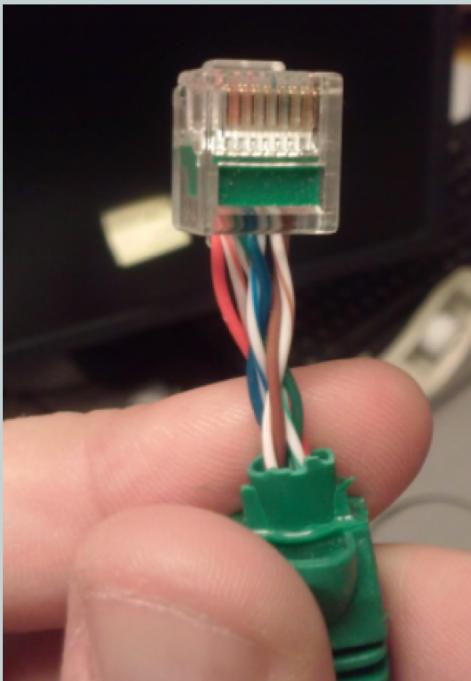
# Physical Layer

- If the physical layer isn't working, none of the other layers will either!
- Common Issues:
  - Bad cables or connectors
  - Cable placement
  - Distance limitations exceeded
  - Splitting pairs in a cable
  - EMI interference/Cross talk
  - Transposed Tx/Rx



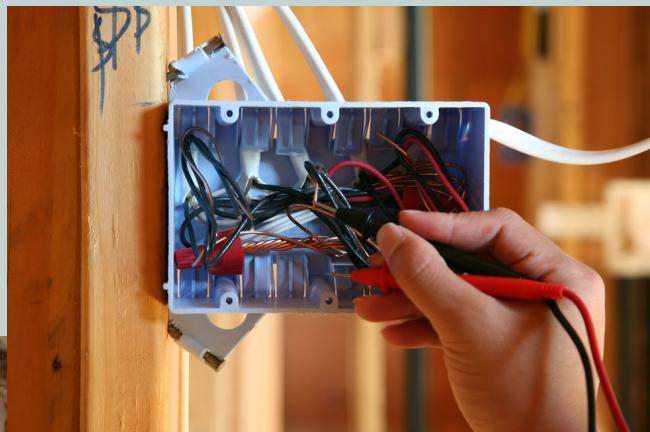
# Bad Cables or Connectors (Physical Layer)

- Faulty cables or connectors
- Wrong category of cable for the purpose



# Cable Placement (Physical Layer)

- Too close to high voltage cables, generators, motors or radio transmitters



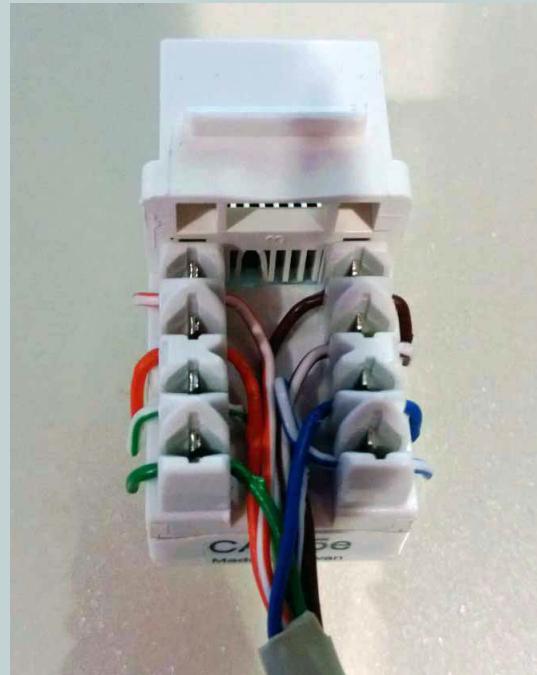
# Distance Limits Exceeded (Physical Layer)

- Exceeding the Ethernet distance limitations can degrade the transmission
- Remember, always be less than 100 meters for copper cabling (CAT 5, 5e, 6, 6a, 7)
- If running high bandwidth applications (like 4k video), then keep it under 70 meters



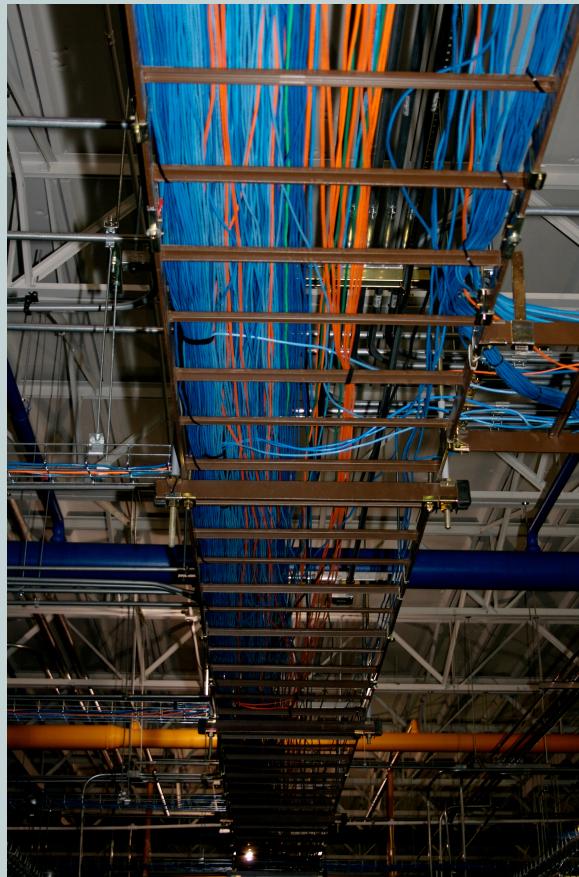
# Splitting Pairs in a Cable (Physical Layer)

- Ethernet only uses 2 pairs of the cable
  - 4 of 8 wires used
- Technicians sometimes use other pairs to create a second jack instead of running new cables
- Leads to nonstandard wiring of the jack and possible EMI/crosstalk



# EMI Interference/Crosstalk (Physical Layer)

- Can be caused by cable placement
  - Cables over fluorescent lights, in same cable tray as electrical wires, etc.
- Caused by crosstalk inside the wire bundles
- Shielded cables can alleviate this problem



# Transposed Tx/Rx (Physical Layer)

- Medium Dependent Interface Crossover (MDIX) allows a switch port to configure itself as a crossover or normal port
- Older switches don't support MDIX and require a crossover cable
- With fiber cables, each fiber is Tx or Rx





# Troubleshooting (Layer 2)

CompTIA Network+ (N10-007)

# Data Link Layer

- Understanding the Layer 2 operations is critical to troubleshooting many LAN issues
- Common Issues:
  - Bad module
  - Layer 2 loops
  - Port misconfiguration
  - VLAN configuration



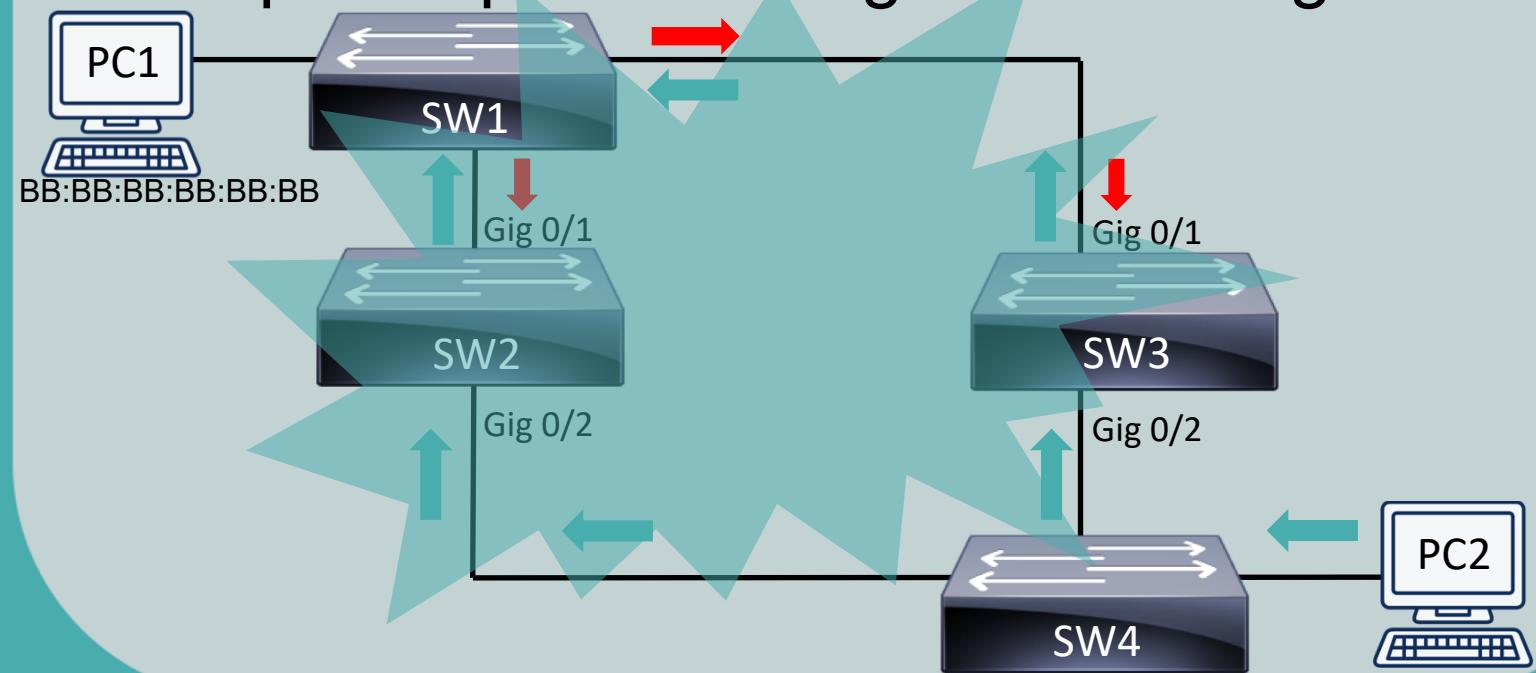
# Bad Module (Data Link Layer)

- Modular interfaces can be swapped out and replaced



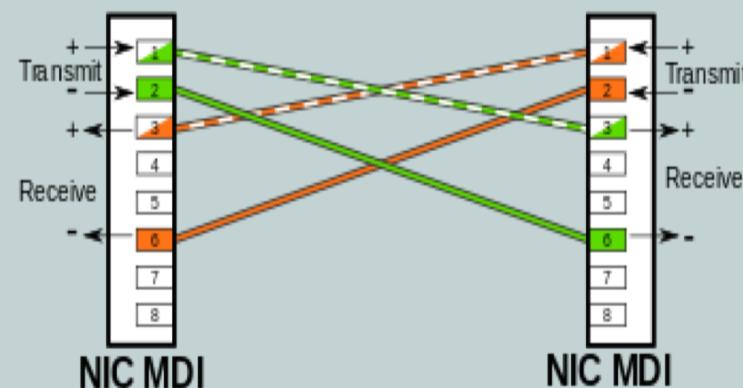
# Layer 2 Loop (Data Link Layer)

- If Spanning Tree Protocol (STP) fails, a spanning-tree loop can result and cause a broadcast storm
- Misconfigured STP can cause traffic to take a suboptimal path causing network degradation

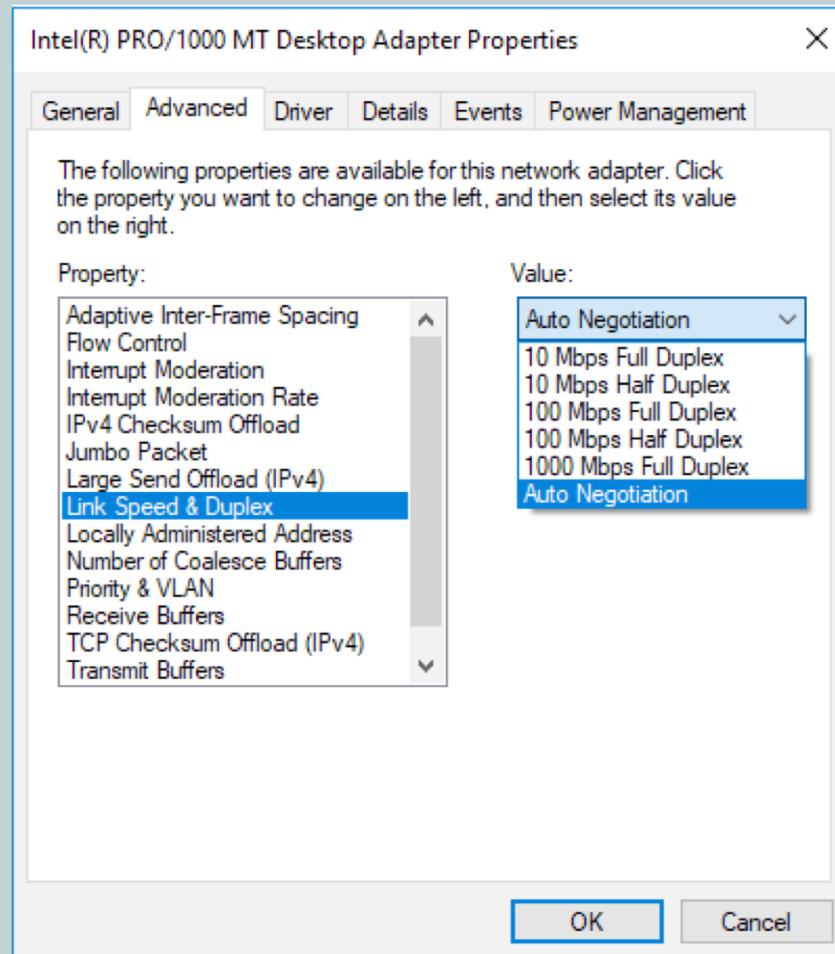


# Port Misconfiguration (Data Link Layer)

- Mismatched speed, duplex, or MDIX settings on a switch port to a workstation can result in slow or no communication

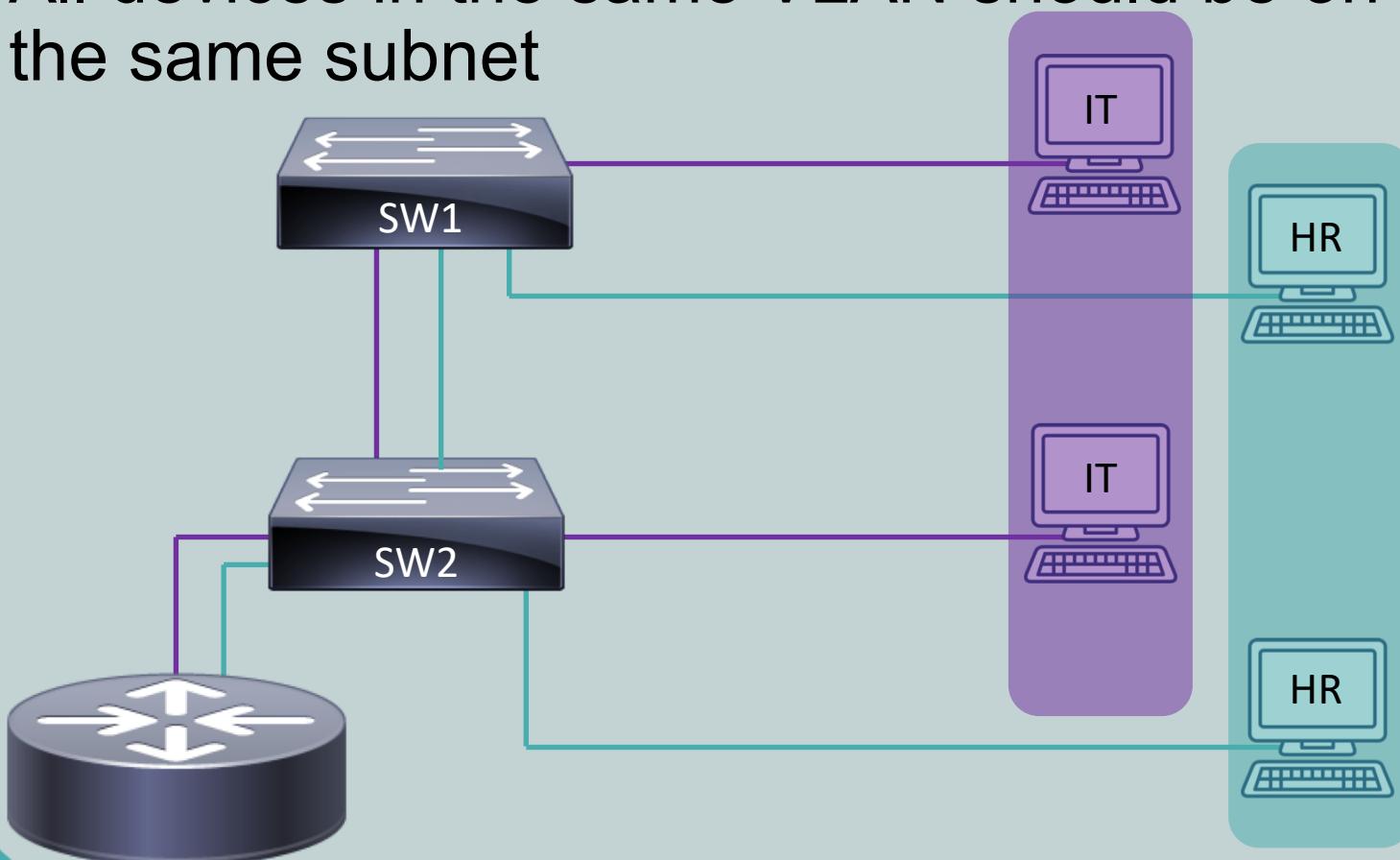


Medium Dependent  
Interface Crossover  
(MDIX)



# VLAN Configuration (Data Link Layer)

- Traffic must be routed between VLANs
- All devices in the same VLAN should be on the same subnet





# Troubleshooting (Layer 3)

CompTIA Network+ (N10-007)

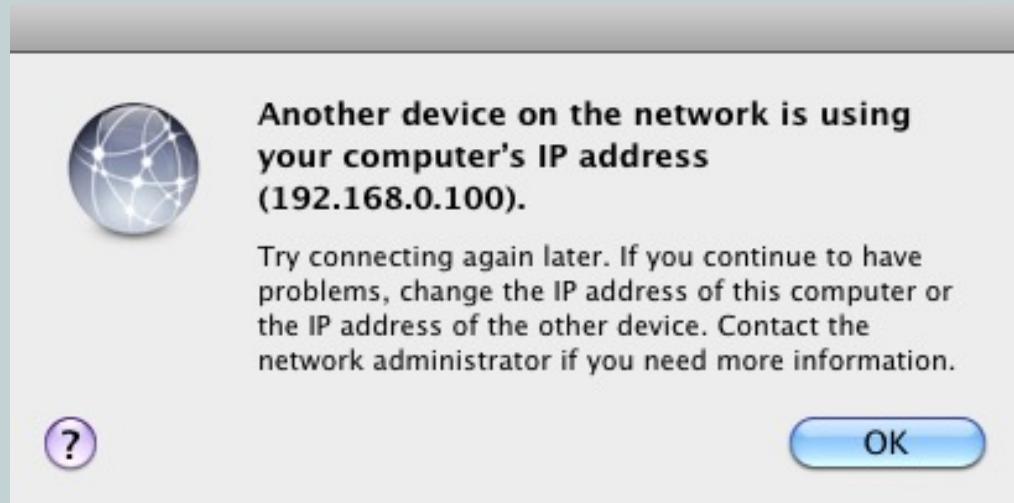
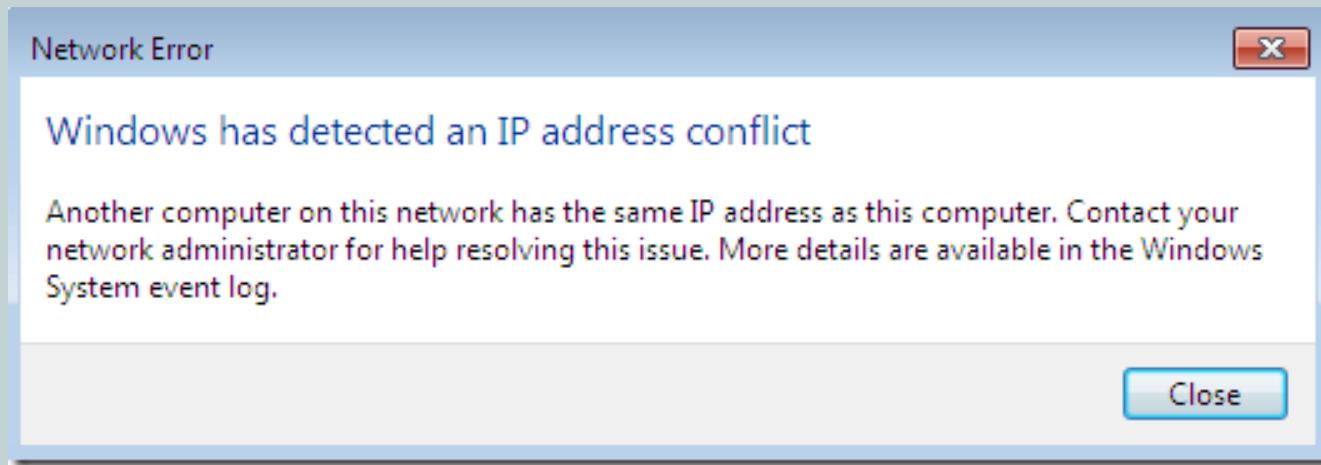
# Network Layer

- Understanding the Layer 3 routing is crucial to troubleshooting many LAN and WAN issues with routing, subnetting, and services like DNS
- Common Issues:
  - Duplicate IP address
  - Incorrect default gateway
  - Incorrect DNS configuration
  - Mismatched MTU



# Duplicate IP Address (Network Layer)

- Two hosts with same IP address can cause unpredictable behavior in the network



# Incorrect Default Gateway (Network Layer)

- Host will be unable to communicate with devices that are outside of the local subnet

Wi-Fi

Wi-Fi    TCP/IP    DNS    WINS    802.1X    Proxies    Hardware

Configure IPv4: Manually

IPv4 Address: 192.168.1.200

Subnet Mask: 255.255.255.0

Router: 10.0.0.1

Wi-Fi

Wi-Fi    TCP/IP    DNS    WINS    802.1X    Proxies    Hardware

Configure IPv4: Manually

IPv4 Address: 10.0.1.200

Subnet Mask: 255.255.255.0

Router: 10.0.0.1



# Incorrect Default Gateway (Network Layer)

- Host will be unable to communicate with devices that are outside of the local subnet

Wi-Fi

Wi-Fi TCP/IP DNS WINS 802.1X Proxies Hardware

Configure IPv4: Manually

IPv4 Address: 192.168.1.200

Subnet Mask: 255.255.255.0

Router: 10.0.0.1

192.168.1.1

Wi-Fi

Wi-Fi TCP/IP DNS WINS 802.1X Proxies Hardware

Configure IPv4: Manually

IPv4 Address: 10.0.1.200

Subnet Mask: 255.255.255.0

Router: 10.0.0.1



# Incorrect Default Gateway (Network Layer)

- Host will be unable to communicate with devices that are outside of the local subnet

Wi-Fi

TCP/IP DNS WINS 802.1X Proxies Hardware

Configure IPv4: Manually

IPv4 Address: 192.168.1.200

Subnet Mask: 255.255.255.0

Router: 10.0.0.1

192.168.1.1

Wi-Fi

TCP/IP DNS WINS 802.1X Proxies Hardware

Configure IPv4: Manually

IPv4 Address: 10.0.1.200

Subnet Mask: 255.255.255.0

Router: 10.0.0.1

10.0.1.1



# Incorrect DNS Configuration (Network Layer)

- Host will be unable to browse the Internet using domain names

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . . . : fios-router.home
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-70-92-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c42a:e633:dbe5:1438%3(Preferred)
IPv4 Address. . . . . : 10.0.2.15(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, January 24, 1882 5:17:50 AM
Lease Expires . . . . . : Saturday, March 3, 2018 8:46:08 AM
Default Gateway . . . . . : 10.0.2.2
DHCP Server . . . . . : 10.0.2.2
DHCPv6 IAID . . . . . : 34078759
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-7F-CA-39-08-00-27-70-92-1D
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled
```



# Mismatched MTU (Network Layer)

- Maximum Transmission Units (MTU) defines the largest packet size the router's interface will forward
- If MTU is too small, packets will be dropped
  - Default is usually 1500 bytes
- This is a common issue with VPN tunneling in Site to Site since packets are “wrapped” with an additional header...

```
ciscoasa(config)# mtu ?  
configure mode commands/options:  
Current available interface(s):  
  Inside  Name of interface Vlan1  
  outside Name of interface Vlan2  
ciscoasa(config)# mtu outside ?  
configure mode commands/options:  
  <64-65535>  MTU bytes  
ciscoasa(config)# mtu outside
```



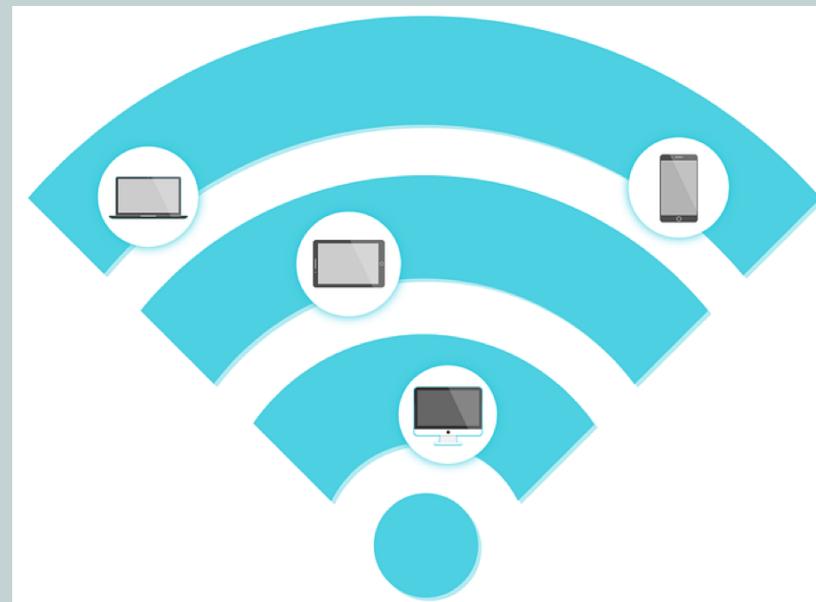


# Troubleshooting (Wireless)

CompTIA Network+ (N10-007)

# Wireless Troubleshooting

- Troubleshooting wireless networks can require a variety of skill sets
  - Layer 1, 2, and 3 issues can occur
  - Radio frequency (RF) conflicts
  - Placement of Access Points
  - Signal strength issues



# Radio Frequency Issues (Wireless)

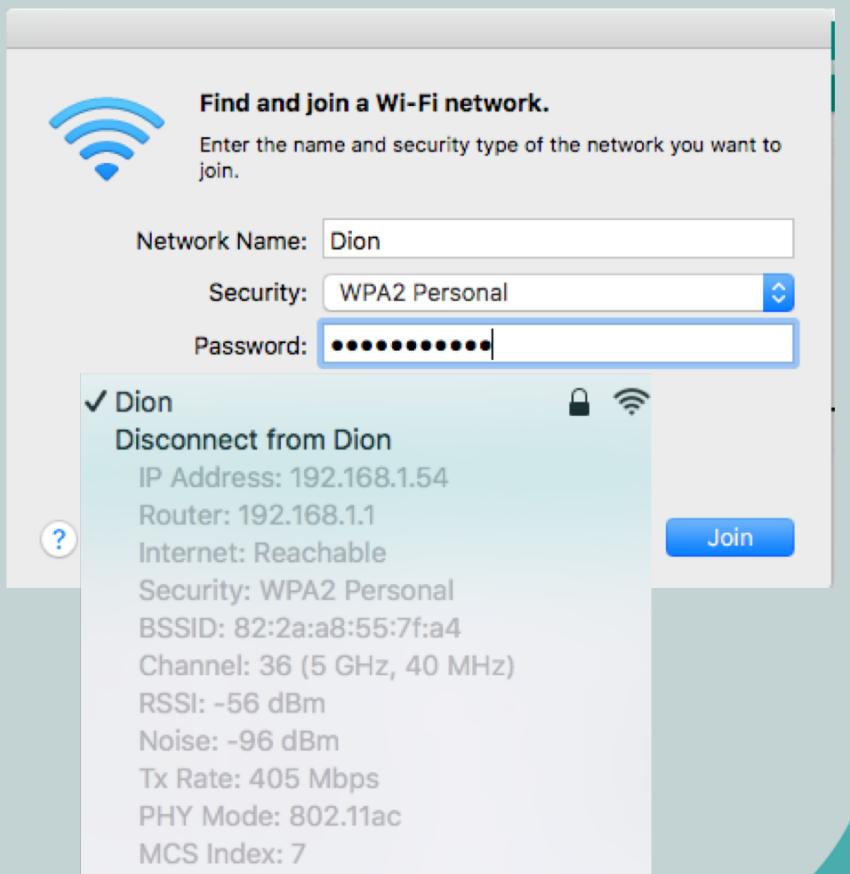
- Radio frequency interference (RFI) from cordless phones, baby monitors, microwaves, and other wireless networks
- Solution
  - Pick an unused channel in the 2.4 Ghz spectrum
  - Upgrade the network to 5 Ghz spectrum
  - Determine the best placement of your WAP



# Misconfiguration of Devices (Wireless)

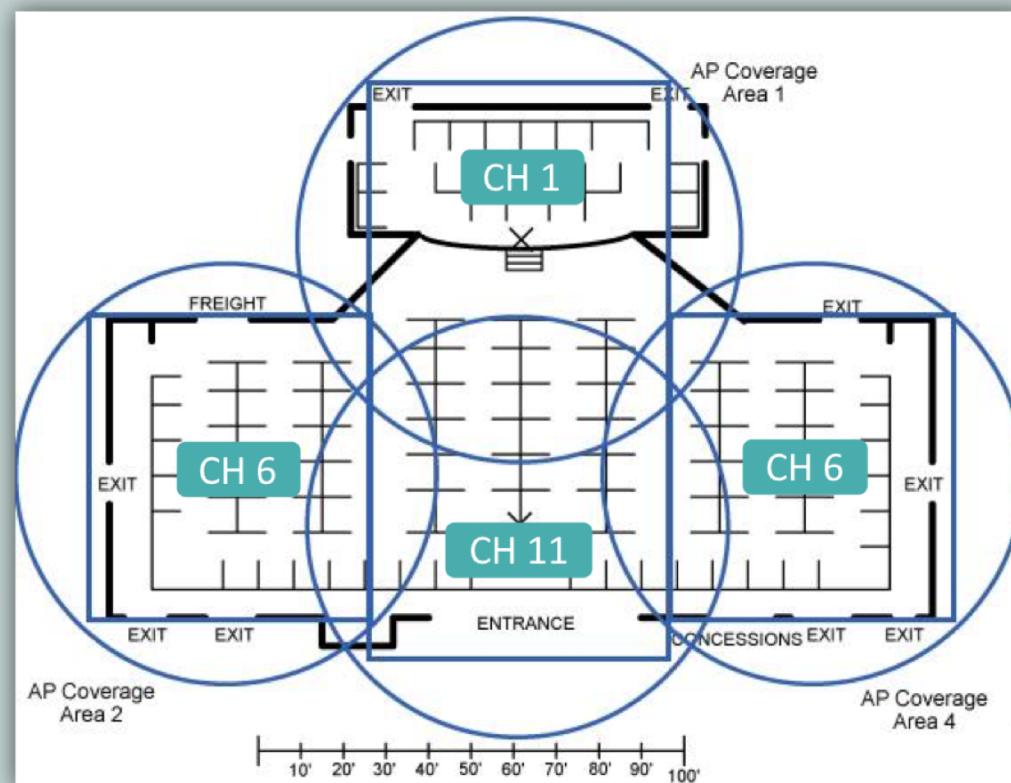
- Variety of wireless settings must match between the client and the access point for communication to be successful

- Solution
  - Verify SSID
  - Verify channel
  - Verify encryption



# Incorrect Placement of AP (Wireless)

- Coverage areas should overlap but not with the same channel numbers
  - 2.4 GHz should use Channels 1, 6, 11
  - 5 Ghz need 2 cells between channel overlap



# Weak Signal Strength (Wireless)

- Received Signal Strength Indicator (RSSI) is too low due to physical objects interfering with the wireless signal or antenna too far from the WAP
- Solution
  - Use a signal booster
  - Add additional WAPs
  - Use external antenna



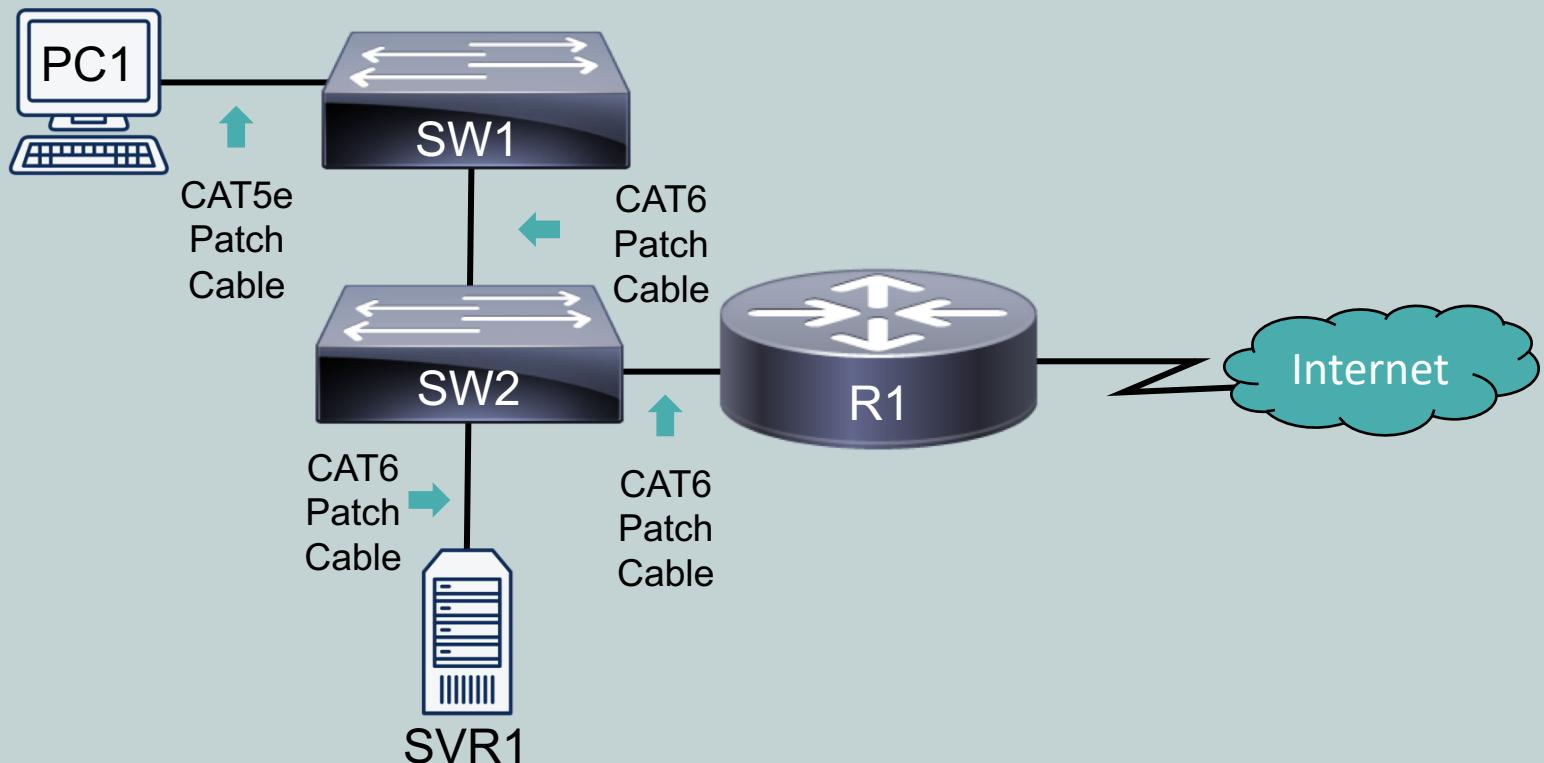


# Troubleshooting Problems

CompTIA Network+ (N10-007)

# Problem #1

*PC1 cannot talk to SVR1, the switches used are older and don't support MDIX.*

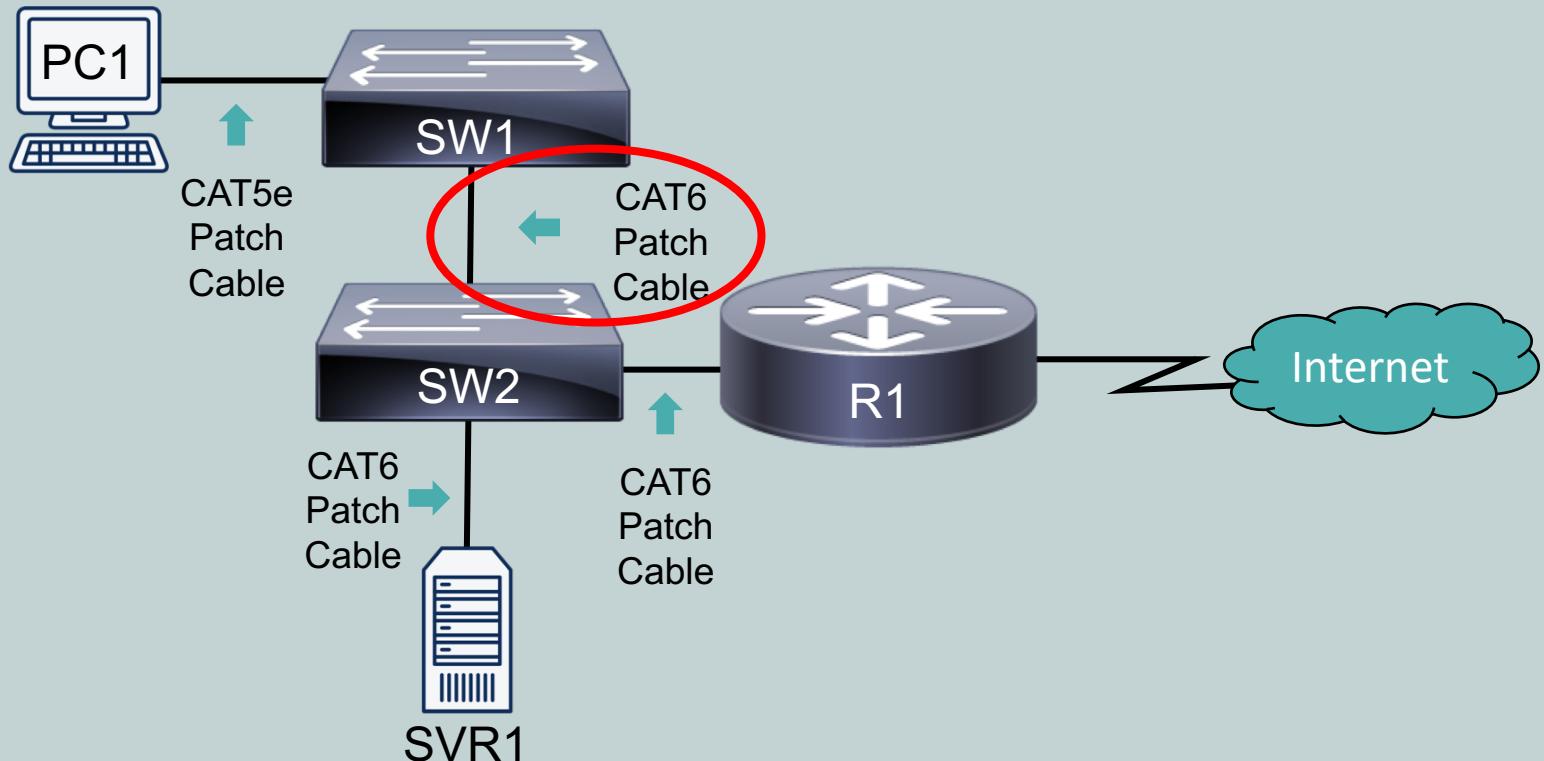


*Why can't the client reach the server?*



# Problem #1

*PC1 cannot talk to SVR1, the switches in use are older and don't support MDIX.*

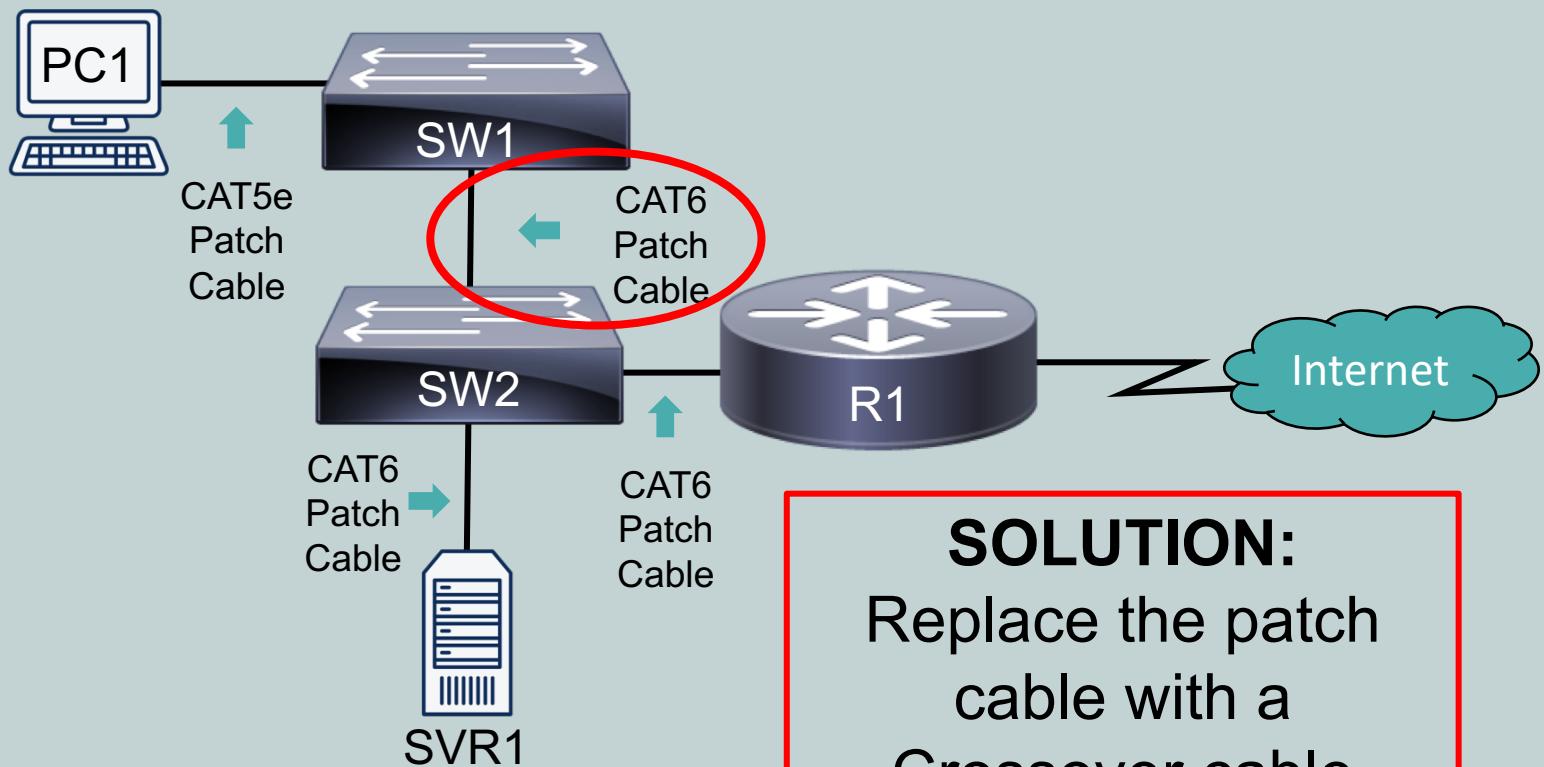


*Why can't the client reach the server?*



# Problem #1

*PC1 cannot talk to SVR1, the switches in use are older and don't support MDIX.*



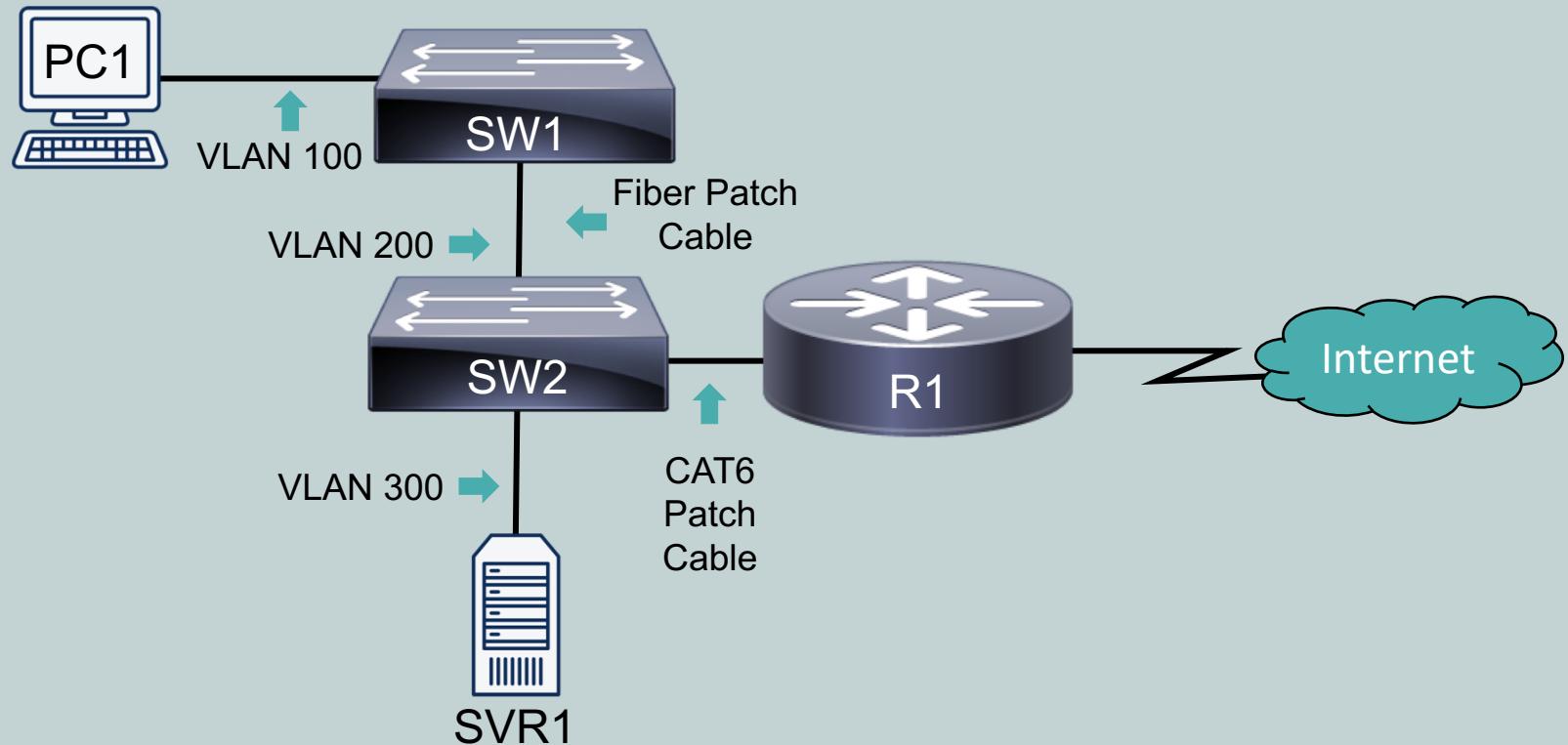
**SOLUTION:**  
Replace the patch cable with a Crossover cable

*Why can't the client reach the server?*



## Problem #2

*PC1 is unable to reach SVR1. You have verified communication between SW1 and SW2.*

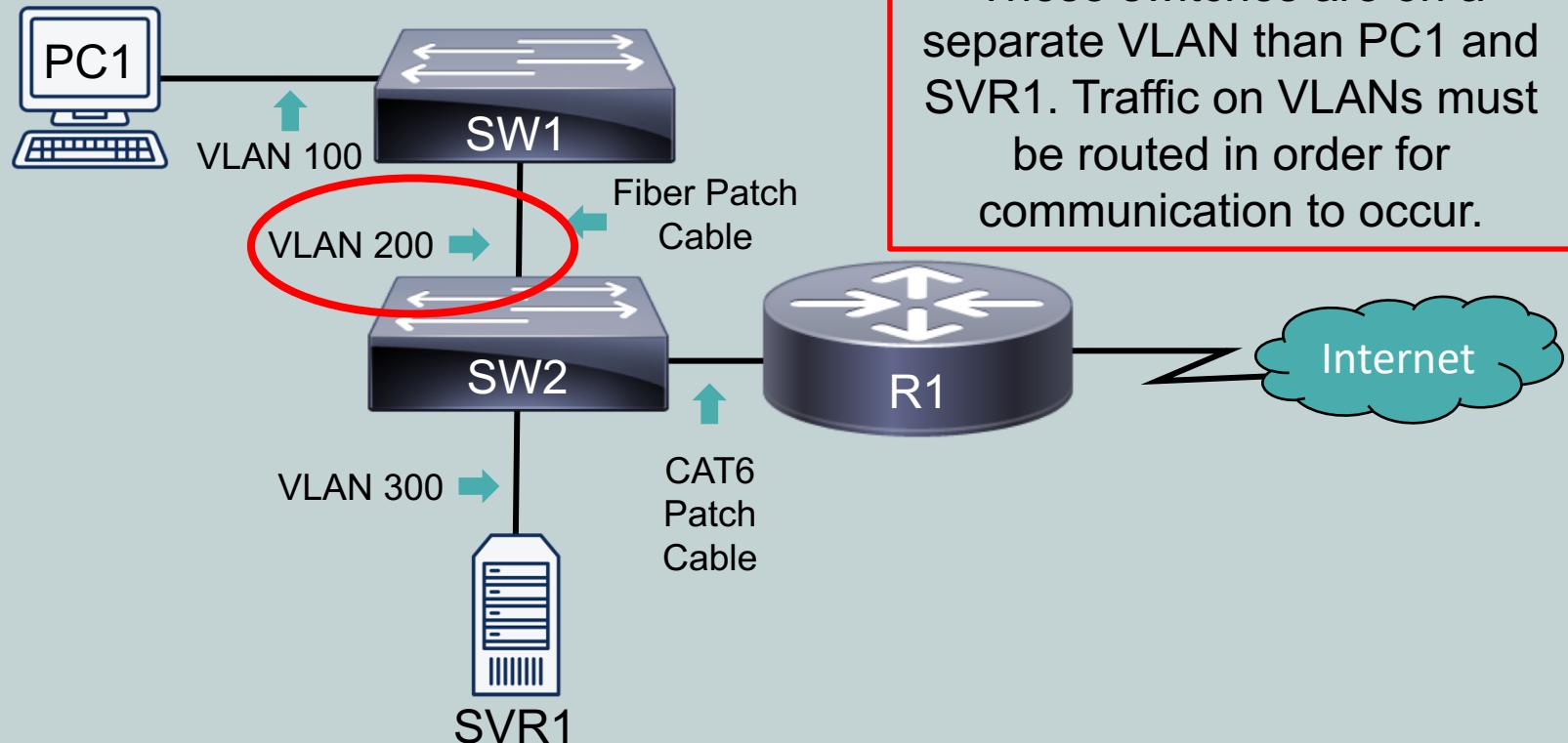


*Why can't the client reach the server?*



## Problem #2

*PC1 is unable to reach SVR1. You have verified communication between SW1 and SW2.*



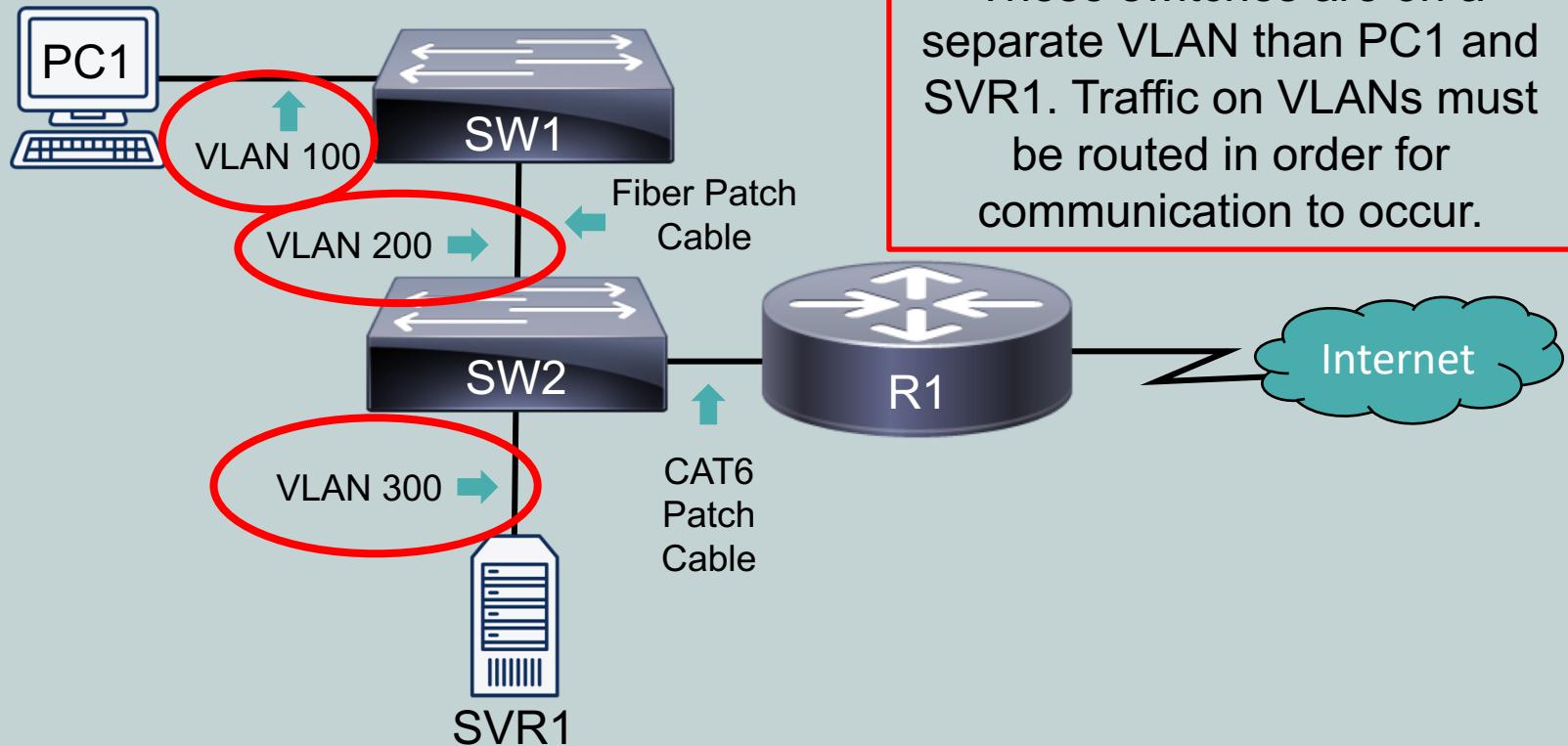
These switches are on a separate VLAN than PC1 and SVR1. Traffic on VLANs must be routed in order for communication to occur.

*Why can't the client reach the server?*



## Problem #2

*PC1 is unable to reach SVR1. You have verified communication between SW1 and SW2.*

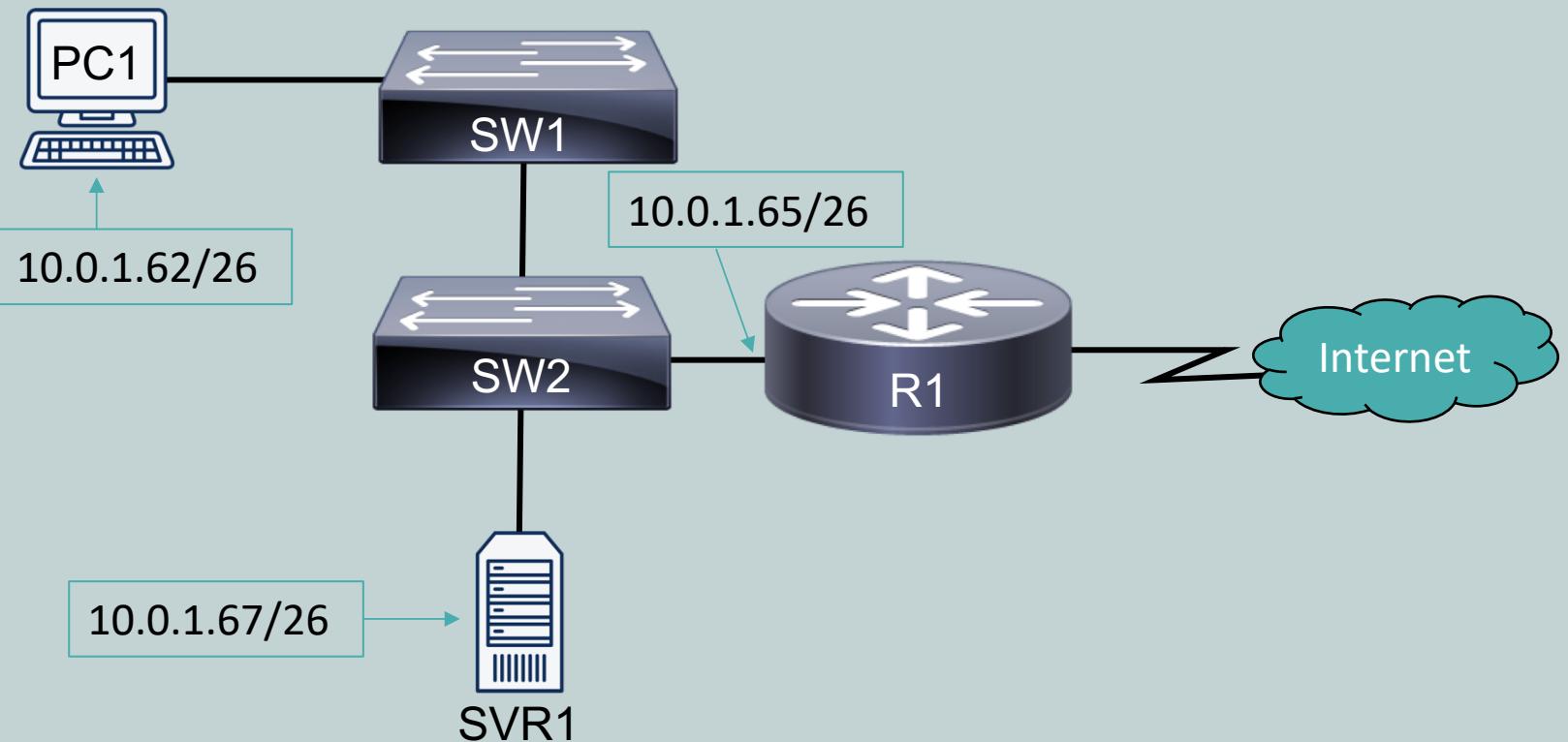


*Why can't the client reach the server?*



## Problem #3

*PC1 is unable to reach SVR1. You have verified communication between SW1 and SW2.*

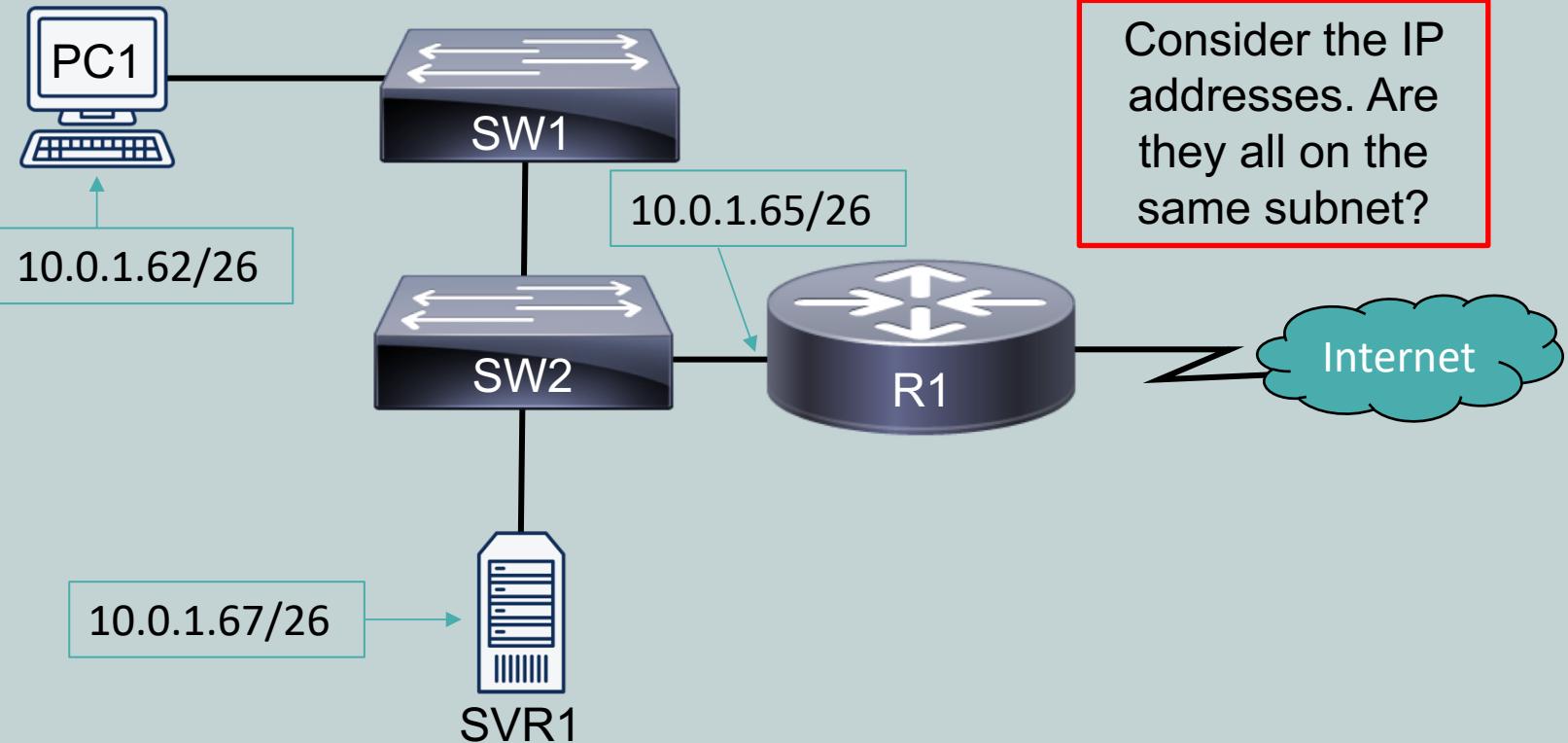


*Why can't the client reach the server?*



# Problem #3

*PC1 is unable to reach SVR1. You have verified communication between SW1 and SW2.*

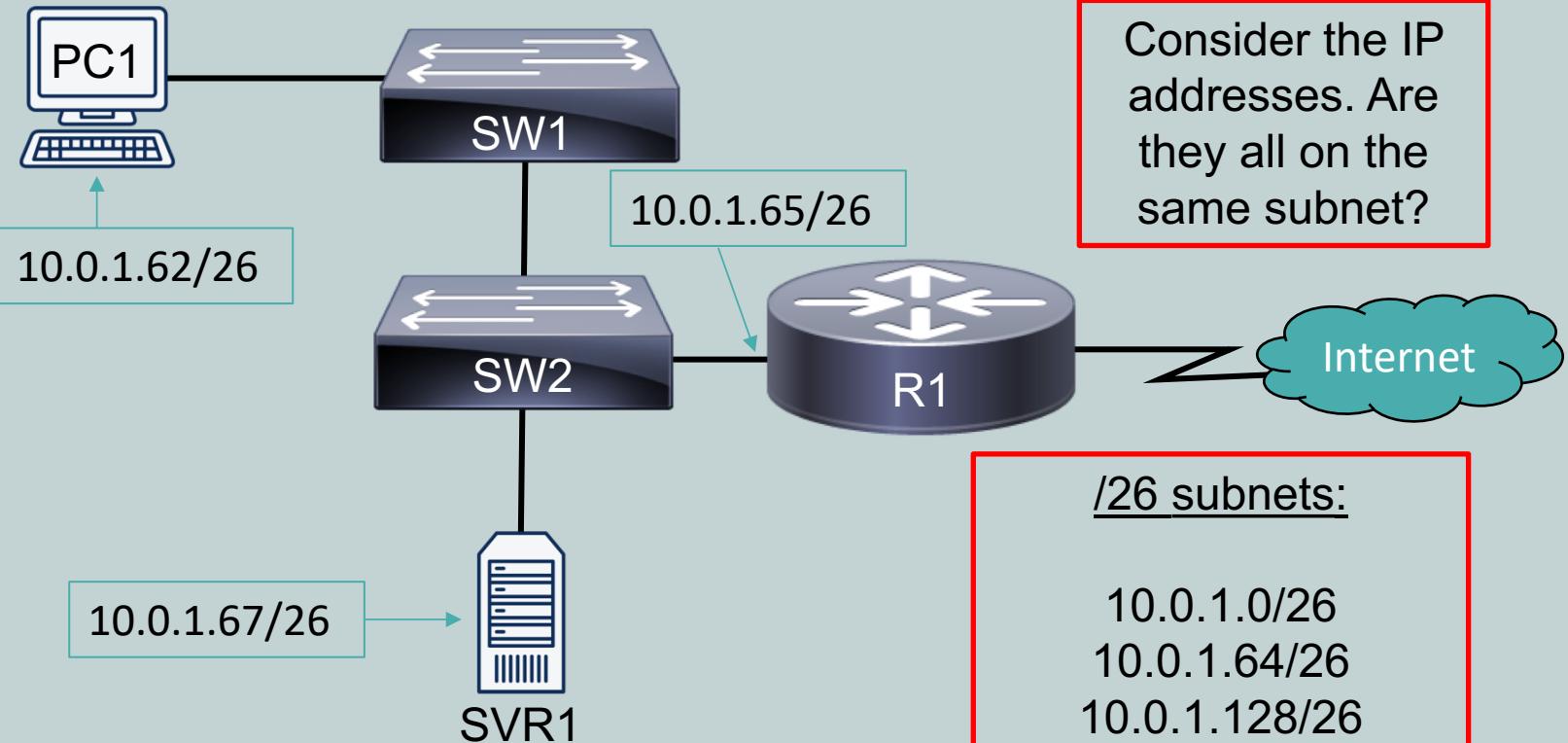


*Why can't the client reach the server?*



# Problem #3

*PC1 is unable to reach SVR1. You have verified communication between SW1 and SW2.*



Consider the IP addresses. Are they all on the same subnet?

/26 subnets:

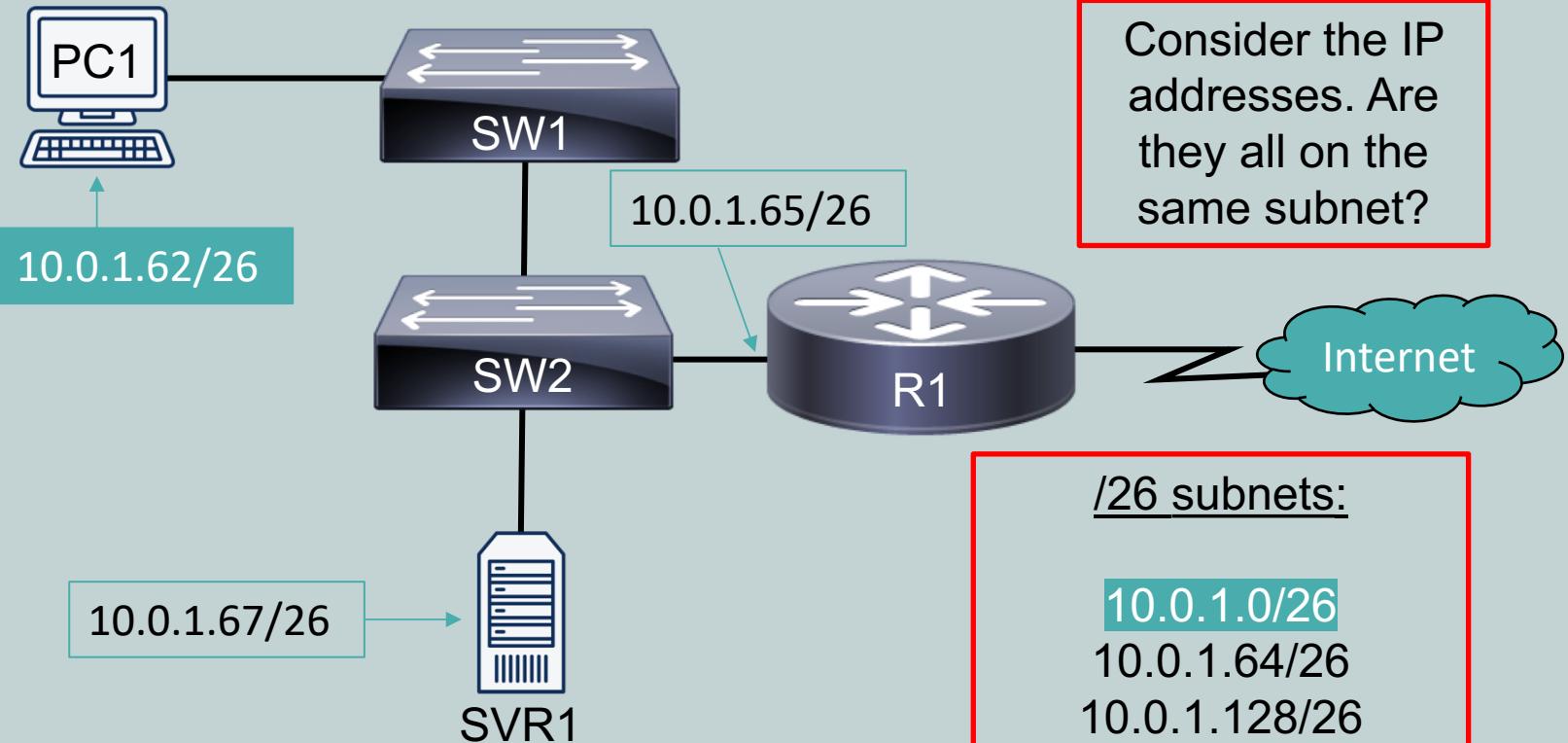
- 10.0.1.0/26
- 10.0.1.64/26
- 10.0.1.128/26
- 10.0.1.192/26

*Why can't the client reach the server?*



# Problem #3

*PC1 is unable to reach SVR1. You have verified communication between SW1 and SW2.*

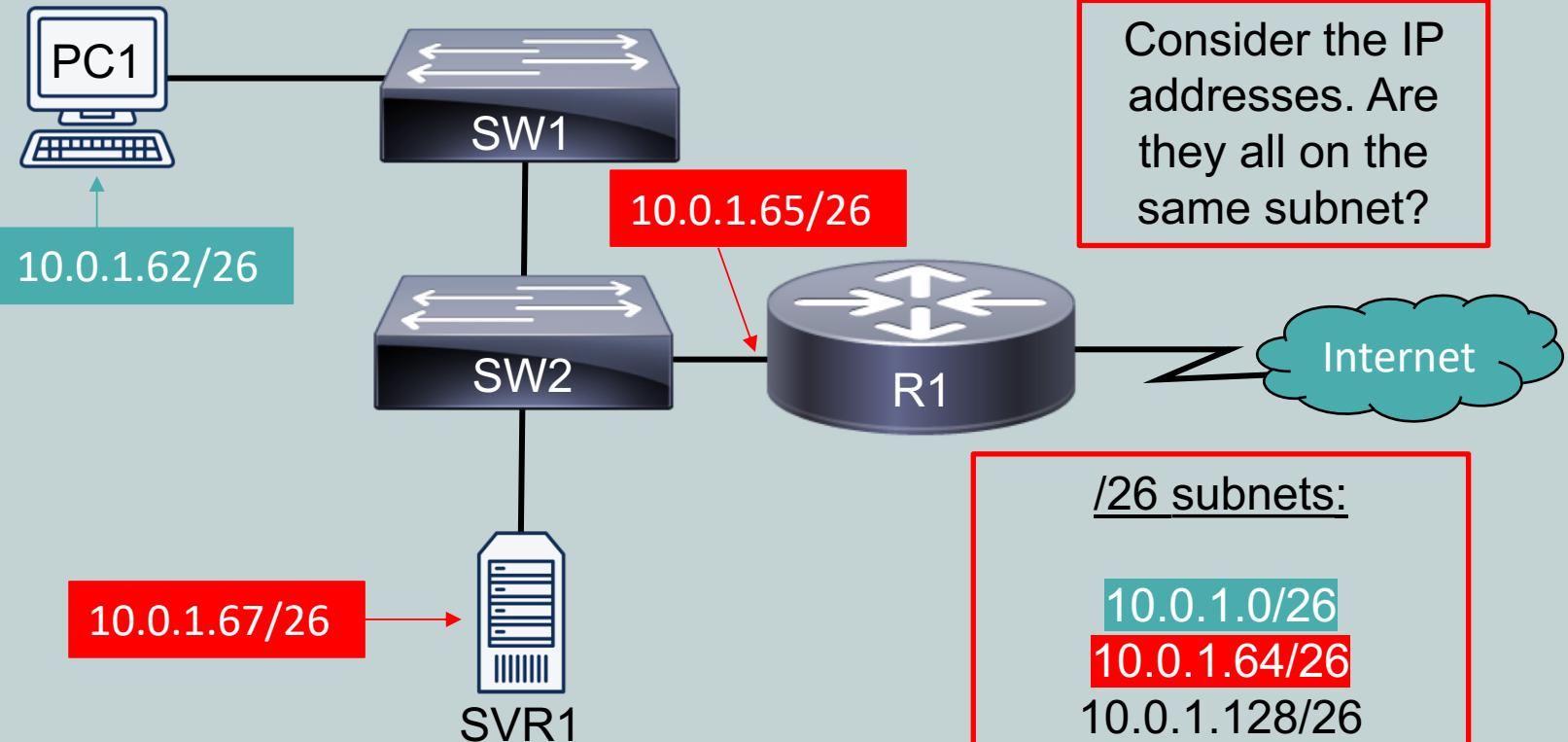


*Why can't the client reach the server?*



# Problem #3

*PC1 is unable to reach SVR1. You have verified communication between SW1 and SW2.*

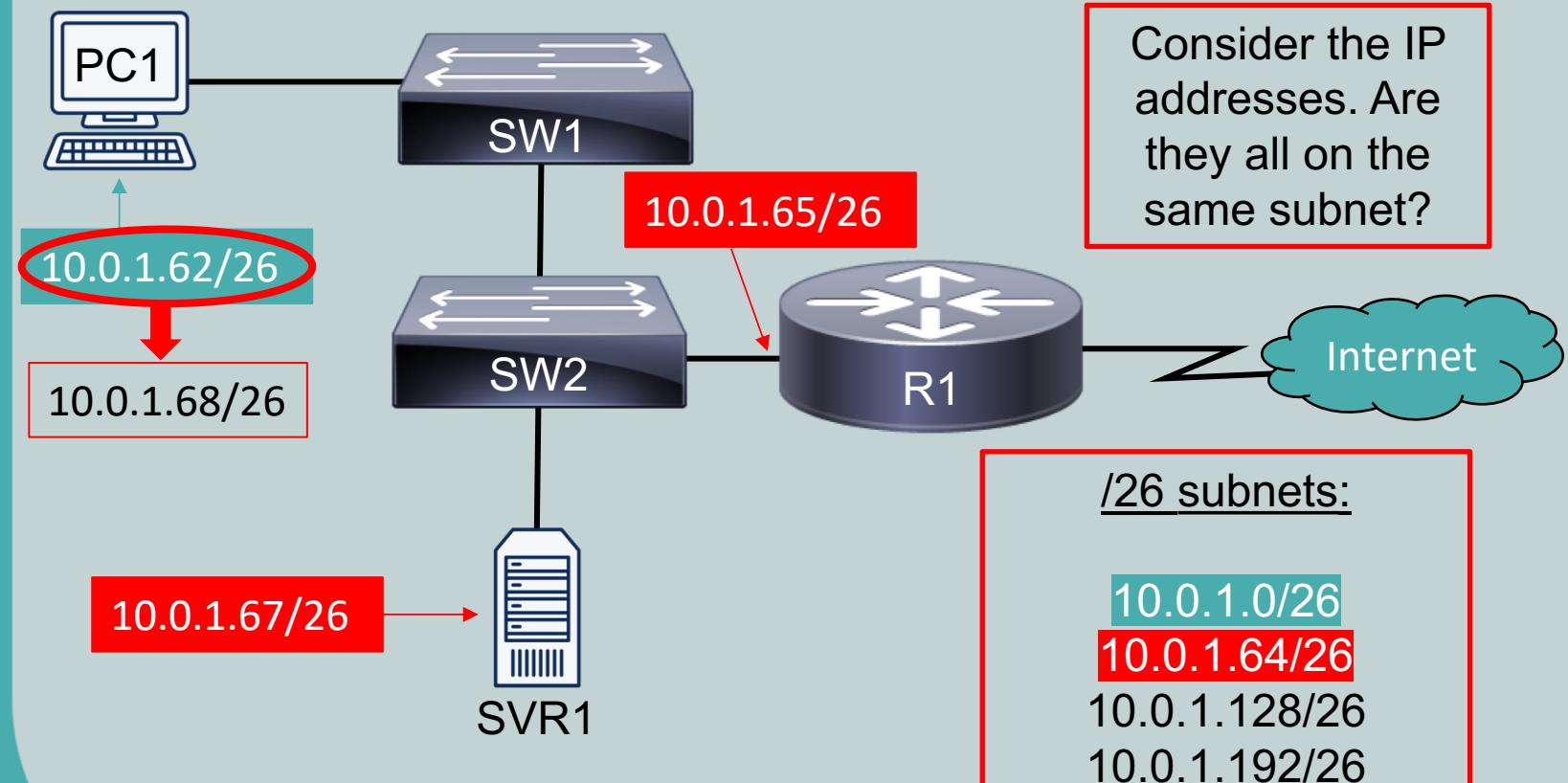


*Why can't the client reach the server?*



# Problem #3

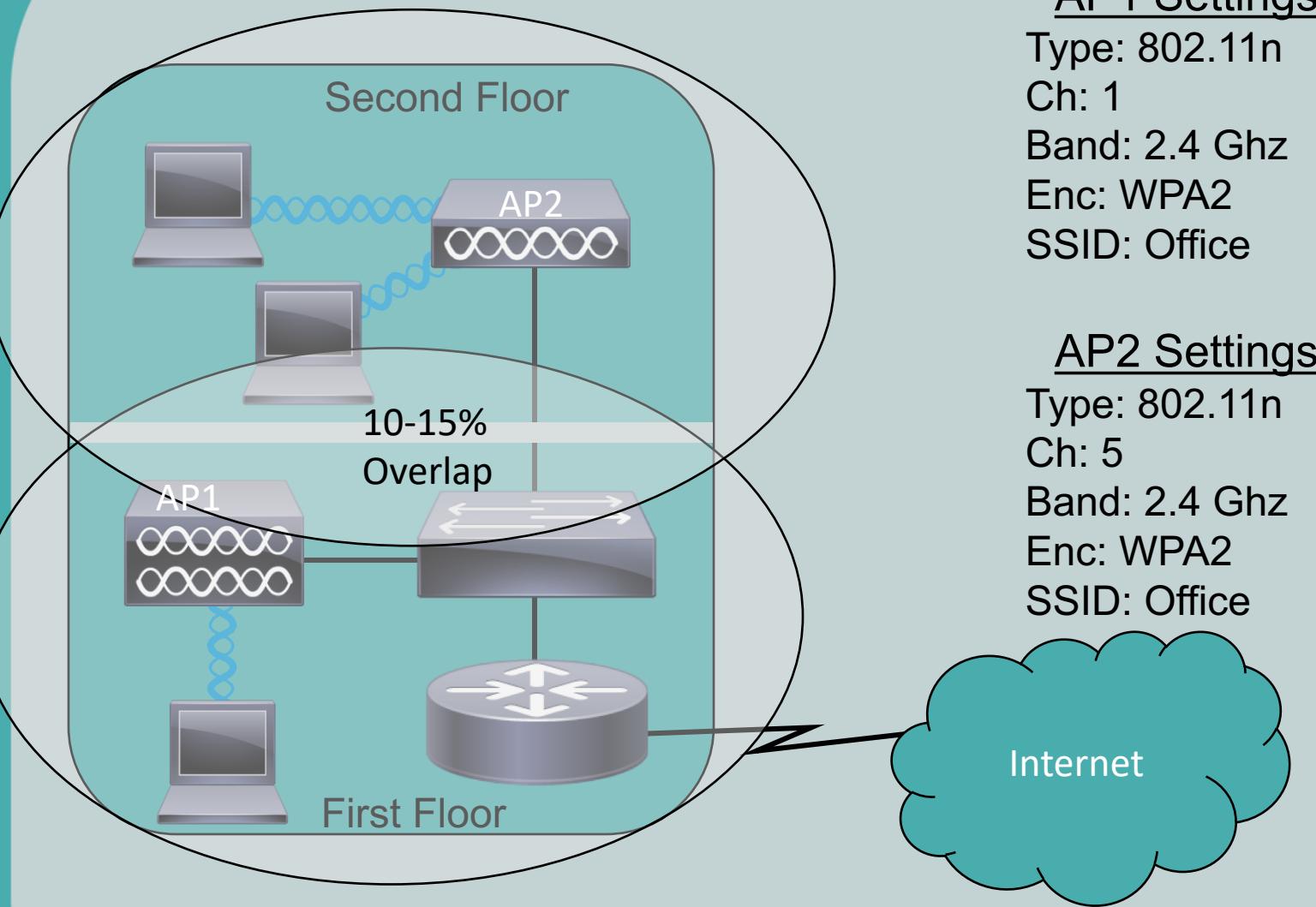
*PC1 is unable to reach SVR1. You have verified communication between SW1 and SW2.*



*Why can't the client reach the server?*



# Problem #4



## AP1 Settings

Type: 802.11n  
Ch: 1  
Band: 2.4 Ghz  
Enc: WPA2  
SSID: Office

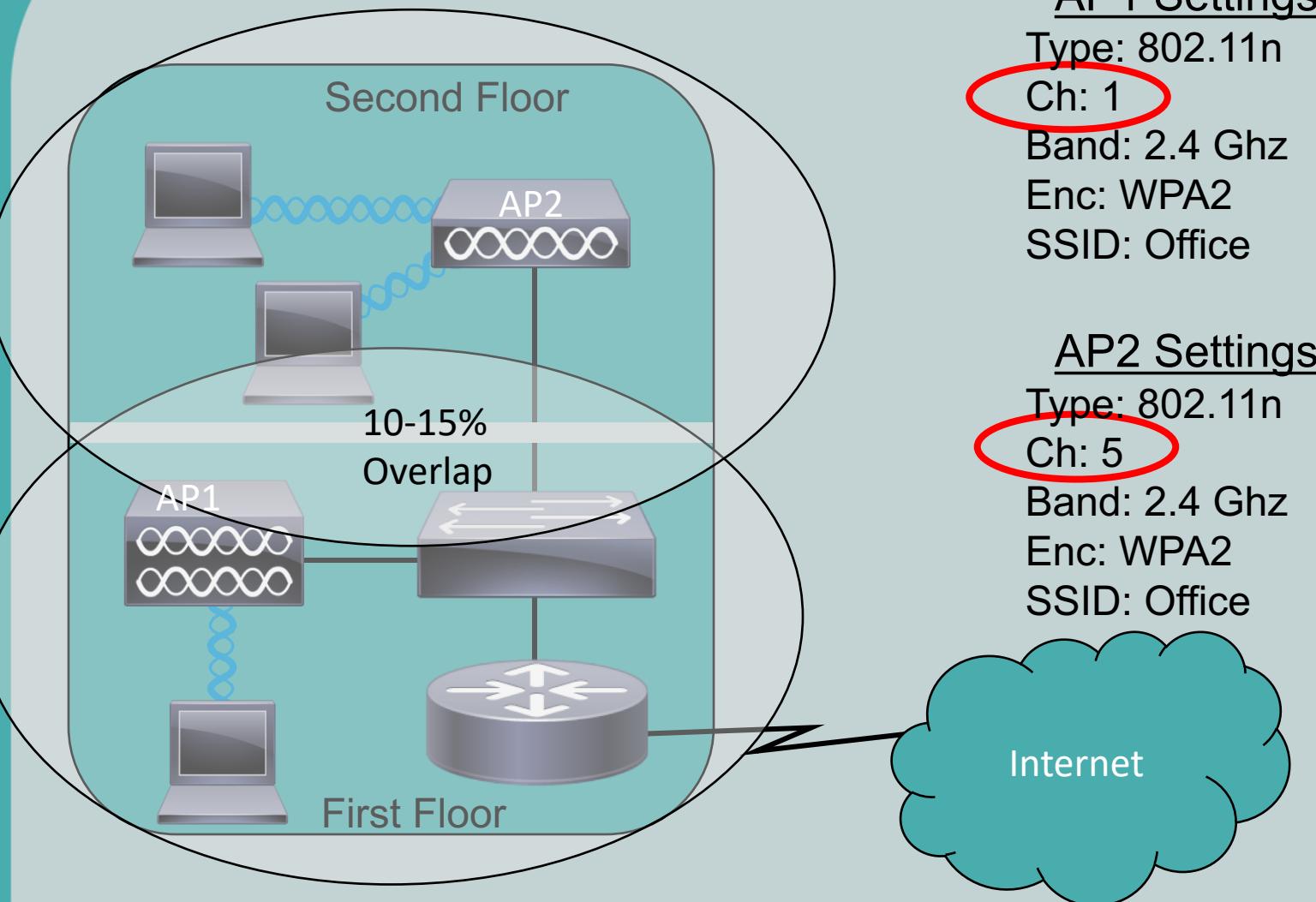
## AP2 Settings

Type: 802.11n  
Ch: 5  
Band: 2.4 Ghz  
Enc: WPA2  
SSID: Office

Users are complaining that their WiFi service is dropping. What is the design flaw?



# Problem #4



Users are complaining that their WiFi service is dropping. What is the design flaw?

