**Discovery 3: Troubleshoot VLAN and Trunk Issues**

**Introduction**

This discovery will guide you through a scenario involving VLAN configuration, Layer 2 connectivity, and IP connectivity. The topology diagram is intentionally vague and there is no connectivity table. Imagine you are on your first day at a new job as a network engineer. You are not yet familiar with the network of your organization. A member of the security team comes to you because the intrusion prevention system has flagged malicious traffic from the IP address 10.10.10.182. You are asked to help in isolating this system and removing it from the network.

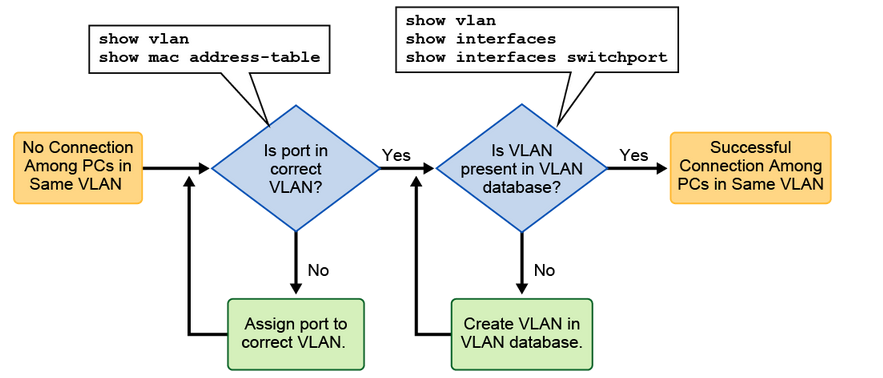
This discovery will also guide you through the IP connectivity issue between two hosts.

Your configuration tasks are as follows:

* Troubleshoot VLAN Issues
* Troubleshoot Trunk Issues

**Task 1: Troubleshoot VLAN Issues**

The following figure shows the flow for troubleshooting VLANs.



To troubleshoot VLAN issues when you have no connection between PCs that belong to the same VLAN, follow these high-level steps:

Use the show vlan command to check whether the port belongs to the expected VLAN. If the port is assigned to the wrong VLAN, use the switchport access vlan command to correct the VLAN membership. Use the show mac address-table command to check which addresses were learned on a particular port of the switch and to which VLAN that port is assigned. If the VLAN to which the port is assigned is deleted, the port becomes inactive. Use the show vlan or show interfaces switchport command to verify that the VLAN is present in the VLAN database.Also note that you can shut the VLAN using shutdown command, so you may need to verify that the VLAN is not disabled using the show vlan command.

MAC Address Table Verification

To display the MAC address table, use the show mac address-table command in privileged EXEC mode as shown in the following example. This command displays the MAC address table for the switch. You can define specific views by using the optional keywords and arguments. The example shows MAC addresses that were learned on the G0/1 interface. As you can see, MAC address 000c.296a.a21c was learned on the interface G0/1 in VLAN 10. If this number is not the expected VLAN number, change the port VLAN membership using the switchport access vlan command.

SW1# show mac address-table interface G0/1

**Mac Address Table**

**-------------------------------------------**

**Vlan Mac Address Type Ports**

**---- ----------- -------- -----**

**10 000c.296a.a21c DYNAMIC Fa0/1**

**10 000f.34f9.9181 DYNAMIC Fa0/1**

**Total Mac Addresses for this criterion: 2**

**Learning Point: Troubleshooting Missing VLANs**

Each port on a switch belongs to a VLAN. If the VLAN to which the port belongs is deleted, the port becomes inactive. All ports belonging to the VLAN that was deleted are unable to communicate with the rest of the network.

As shown in the following example, use the command show interface interface switchport to check whether the port is inactive. If the port is inactive, it will not be functional until you create the missing VLAN using the vlan vlan\_id command or until you assign the port to a valid VLAN.

**SW1# show interfaces FastEthernet0/1 switchport**

**Name: Fa0/1**

**Switchport: Enabled**

**Administrative Mode: static access**

**Operational Mode: static access**

**Administrative Trunking Encapsulation: dot1q**

**Operational Trunking Encapsulation: native**

**Negotiation of Trunking: Off**

**Access Mode VLAN: 10 (Inactive)**

**Trunking Native Mode VLAN: 1 (default)**

**Administrative Native VLAN tagging: enabled**

**Voice VLAN: none**

**Activity**

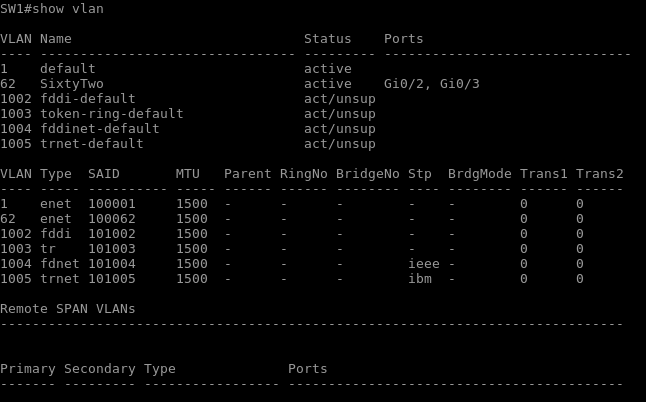
Your task in this discovery is to find the system using the IP address 10.10.10.182 and to disconnect it from the network. You might assume that VLANs are configured by a logical pattern.

Complete the following steps:

**Step 1:** Access the console of SW1 and display the VLAN configuration to show how incorrect that assumption is.

On the SW1 switch, enter the following command:

SW1# show vlan



This disorganized set of VLANs demonstrates why it can be beneficial to set a standard. For example, you can have the VLAN ID match the third octet of the IP network running on that VLAN.

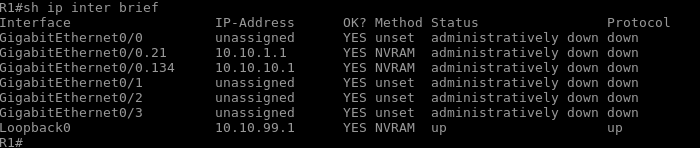
**Step 2:** To determine which VLAN supports the network to which 10.10.10.182 belongs, access the console of R1 and display the brief summary status of its IP interfaces.

**Note**

When the display output pauses with the "--More--" prompt, you can use the space bar to display the next page of the output.

On the R1 router, enter the following command:

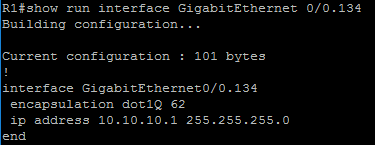
R1# show ip interface brief



**Step 3:** The IP address of GigabitEthernet0/0.134 is 10.10.10.1. If you configure it with a 24-bit subnet mask, it would be on the same subnet as 10.10.10.182.

On the R1 router, enter the following command:

R1# show run interface GigabitEthernet0/0.134

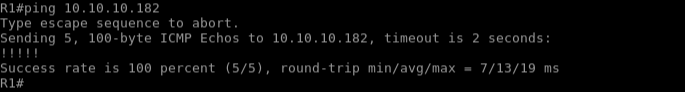


The mask is indeed 24 bits. This interface is on the same subnet as 10.10.10.182.

**Step 4:** The security team member gave you the IP address. Determine the system MAC address by first pinging it from R1 and then finding the entry in the R1 ARP cache.

On the R1 router, enter the following command:

R1# ping 10.10.10.182



R1# show ip arp 10.10.10.182



The system that you are looking for has the MAC address 5000.0003.0000

**Note**

The MAC address in your output can be different. Further in the lab, refer to the MAC address determined in your output.

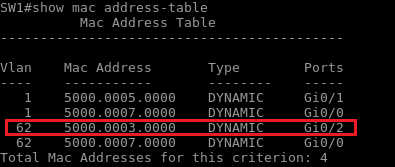
**Step 5:** Access the console of SW1 and view its MAC address table to find the port that is connecting to 5000.0003.0000, or whatever your MAC address is.

**Note**

You must search for the MAC address that you discovered in the previous step.

On the SW1 switch, enter the following command:

SW1# show mac address-table



Interface GigabitEthernet0/2 is where the offending system is connected.

Since there were few addresses in the MAC address table, it was easy to select the appropriate entry. If there are thousands of entries in the table, you would want to filter down the output. Try displaying the MAC address table using the include filter to only include addresses that have 5000.0003, or whatever the last 4 digits of your MAC address are, as part of their address.

SW1# show mac address-table | include 5000.0003



In a larger environment, you might find that the port with the offending MAC address is actually a link to another switch. In this case, you would have to go to that switch and view its MAC address table. It might again be on a link to a third switch. You would have to continue the process until you reached a switch with the address on an end-host port.

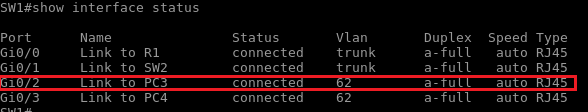
**Step 6:** Display the interface status summary on SW1 to observe the status of GigabitEthernet0/2.

**Note**

One thing that was sensibly configured in this environment is the description on the switch ports. PC3 is the offending system.

On the SW1 switch, enter the following command:

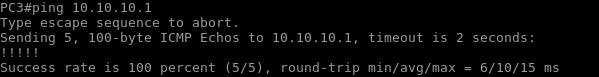
SW1# show interface status



**Step 7:** Using ping from PC3, verify that the offending system, PC3, has access to the network. Attempt to ping R1 (10.10.10.1) from PC3. Ping should be successful.

On PC3, enter the following command:

PC3# ping 10.10.10.1



**Step 8:** Disable interface GigabitEthernet0/2 on SW1.

On the SW1 switch, enter the following commands:

SW1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

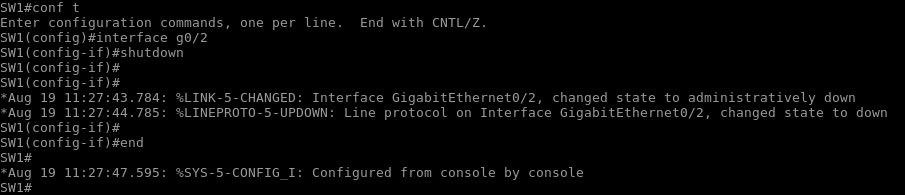
SW1(config)# interface GigabitEthernet0/2

SW1(config-if)# shutdown

SW1(config-if)#

SW1(config-if)# end

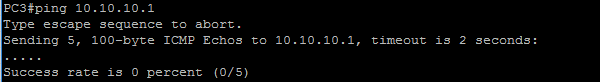
SW1#



**Step 9:** The offending system is PC3. Access the console of PC3 and verify that it has been isolated from the network. Attempt to ping R1 (10.10.10.1). The attempt should fail.

On PC3, enter the following command:

PC3# ping 10.10.10.1

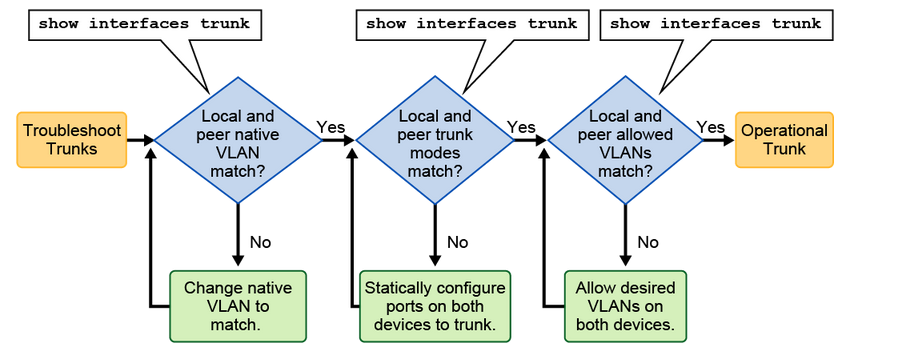


**Task 2: Troubleshoot Trunk Issues**

**Activity**

**Troubleshooting Trunks**

The figure shows the flow for troubleshooting trunks.



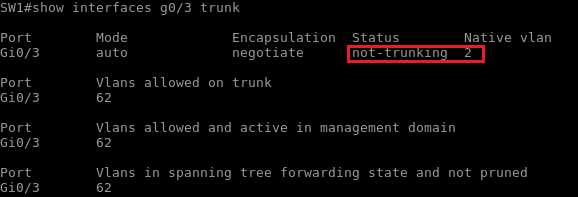
To troubleshoot trunk issues when the trunk is not established, follow these high-level steps:

* Use the show interfaces trunk command to check whether the local and peer native VLANs match. If the native VLAN does not match on both sides, VLAN leaking occurs.
* Use the show interfaces trunk command to check whether a trunk has been established between switches. You should statically configure trunk links whenever possible. However, Cisco Catalyst switch ports by default run DTP, which tries to negotiate a trunk link.
* Use the show interface trunk command to check whether the desired VLANs have been allowed on both the sides of the trunk link.

Verify Trunk Establishment

To display the status of the trunk and native VLAN that is used on a trunk link and to verify trunk establishment, use the show interface trunk command in privileged EXEC mode. The following example shows that the native VLAN on one side of the trunk link was changed to VLAN 2. If one end of the trunk is configured as native VLAN 1 and the other end is configured as native VLAN 2, a frame that is sent from VLAN 1 on one side is received by VLAN 2 on the other. VLAN 1 "leaks" into the VLAN 2 segment. This behavior would never be required, and connectivity issues occur in the network if a native VLAN mismatch exists. Change the native VLAN to the same VLAN on both sides of the VLAN to avoid this behavior.

SW1# show interfaces G0/3 trunk





Cisco Discovery Protocol notifies you of a native VLAN mismatch on a trunk link with this message.

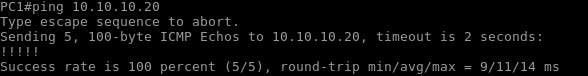
You should statically configure trunk links whenever possible. Cisco Catalyst switch ports by default run DTP. DTP can determine the operational trunking mode and protocol on a switch port when it is connected to another device that is also capable of dynamic trunk negotiation. Remember that if both ends of a trunk are set to dynamic auto trunk mode, a trunk will not be established. The example shows the status of the link as "not-trunking."

Complete the following steps:

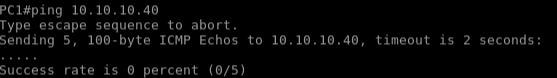
**Step 1:** User that is using PC1 is reporting that PC1 can reach PC2 (10.10.10.20), but cannot reach PC4 (10.10.10.40). Help the user find the issue and resolve it. Using the ping command, access PC1 and verify IP connectivity to PC2 and PC4 to exclude an IP connectivity issue.

On PC1, enter the following commands:

PC1# ping 10.10.10.20



PC1# ping 10.10.10.40



You should find that there is an IP connectivity issue between PC1 and PC4.

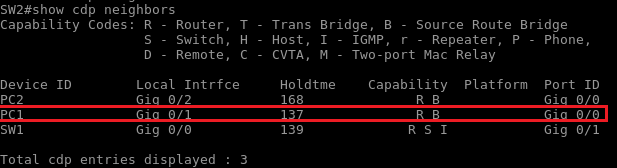
**Step 2:** Access the SW2 switch and check which VLAN is set on the interface that PC1 is connected to. However, first you need to use Cisco Discovery Protocol to verify which port PC1 is connected to.

Note

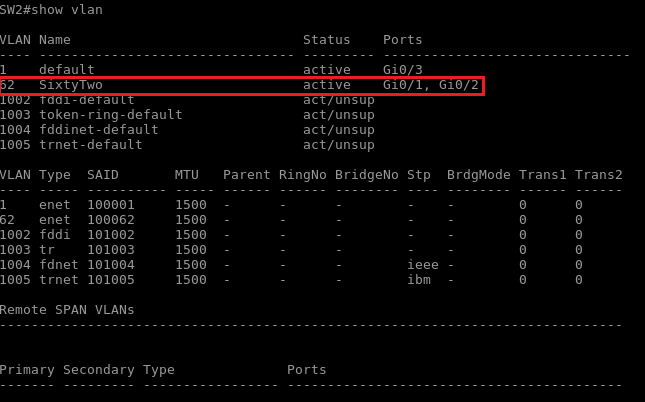
With real PCs, PC would not be seen as the Cisco Discovery Protocol neighbor, so you would need to use the same approach that you used in the first procedure of this discovery.

On the SW2 switch, enter the following commands:

SW2# show cdp neighbors



SW2# show vlan

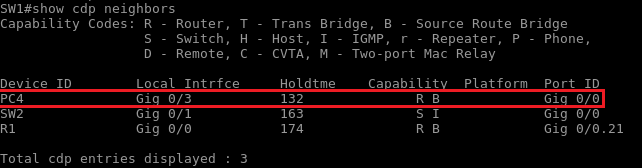


You will find out that PC1 is connected to GigabitEthernet0/1 and that it is placed into active VLAN 62.

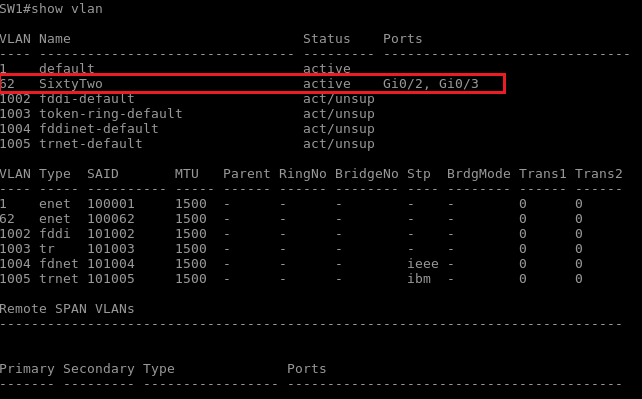
**Step 3:** Access the SW1 switch and check which VLAN is set on the interface that PC4 is connected to. However, first you need to use Cisco Discovery Protocol to verify which port PC4 is connected to.

On the SW1 switch, enter the following commands:

SW1# show cdp neighbors



SW1# show vlan



You will find out that both PC1 and PC4 are in the same VLAN.

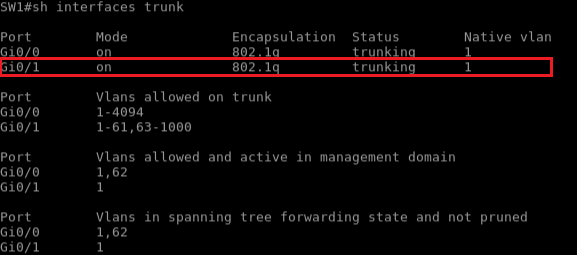
**Step 4:** While troubleshooting, you first noticed the following message on the SW1 console:



This message indicates that SW1 and SW2 have different native VLANs configured.  
  
Using the show interface command, check which VLAN is used as native on GigabitEthernet0/1 on SW1 and SW2:

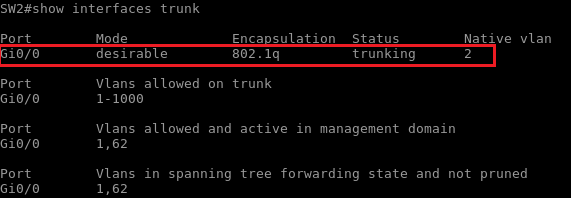
On the SW1 and SW2 switch, enter the following commands:

SW1# show interfaces trunk



On SW2, check which VLAN is used as native on GigabitEthernet0/1:

SW2# show interfaces trunk

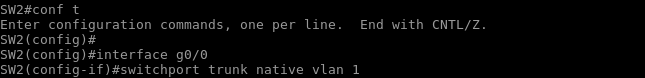


**Step 5:** Change the native VLAN configuration on the SW2 switch.

On the SW2 switch, enter the following commands:

SW2# configure terminal Enter configuration commands, one per line. End with CNTL/Z. SW2(config)# interface GigabitEthernet0/0

SW2(config-if)# switchport trunk native vlan 1



**Note**

Messages to the console stopped.

**Step 6:** Using the ping command, verify if native VLAN was the reason for broken connectivity between PC1 and PC4. Access PC1 and verify IP connectivity to PC4.

On PC1, enter the following command:

PC1# ping 10.10.10.40

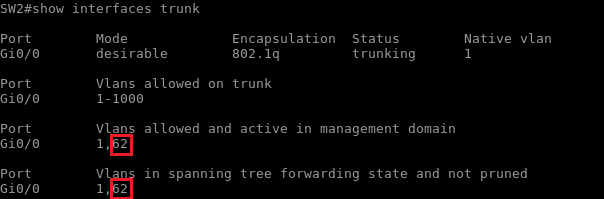


PC1 still has no connectivity to PC4, so you need to investigate further.

**Step 7:** You have determined that PC1 and PC4 are both in VLAN 62. Now, you will verify trunk link between SW1 and SW2. Use the show interfaces command on SW1 and SW2 to perform this verification.

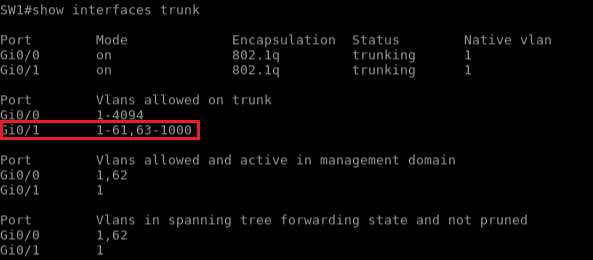
On the SW1 and SW2 switches, enter the following commands:

SW2# show interfaces trunk



VLAN 62 is correctly allowed to the link to SW1

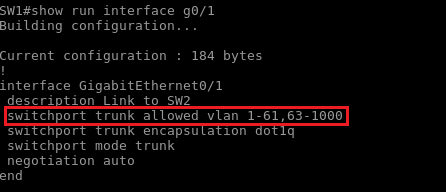
SW1# show interfaces trunk

VLAN 62 is missing from the allowed VLANs on the link toward SW2.

**Step 8:** On SW1, verify the interface GigabitEthernet0/1 configuration. Confirm that VLAN 62 is excluded from the allowed VLAN list.

On the SW1 switch, enter the following command:

SW1# show run interface GigabitEthernet0/1



**Step 9:** On the SW1 interface GigabitEthernet0/1, add VLAN 62 to the trunk.

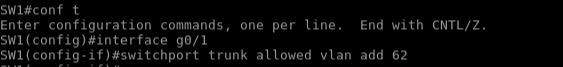
On the SW1 switch, enter the following commands:

SW1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SW1(config)# interface GigabitEthernet0/1

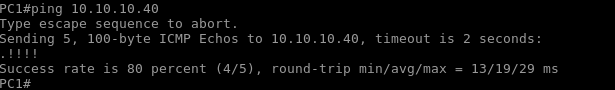
SW1(config-if)# switchport trunk allowed vlan add 62



**Step 10:** Using the ping command on PC1, verify that the IP connectivity issue to PC4 is resolved. Ping should be successful.

On PC1, enter the following commands:

PC1# ping 10.10.10.40



**Note**

It may take a while for the ping to work.