Cisco Networking Lab: VLAN and Trunking Configuration

Objective: To configure VLANs on two interconnected switches (SW1 and SW2), assign ports to these VLANs, establish an 802.1Q trunk link between the switches, and verify end-to-end connectivity between devices in the same VLAN.

1. Topology and IP Addressing

The lab uses the following topology for two switches (SW1 and SW2) connected via Ethernet interfaces, with two PCs connected to each switch.

Device	Device IP	Device Interface	SW Interface	VLAN
PC1	192.168.1.100	Eth0/0	SW1 Fa0/1	1
PC2	192.168.20.101	Eth0/0	SW1 Fa0/2	20
PC3	192.168.1.110	Eth0/0	SW2 Fa0/1	1
PC4	192.168.20.110	Eth0/0	SW2 Fa0/2	20

Trunk Link:

- SW1 interface: Gig0/1
- SW2 interface: Gig0/2

2. Phase 1: Basic VLAN Configuration

The goal of this phase is to create VLAN 20 and assign PC2 and PC4 to it. PC1 and PC3 remain in the default VLAN 1.

Step 1. Create VLAN 20 on both switches.

Device	Command
SW1	SW1(config)# vlan 20
	SW1(config-vlan)# exit

SW2	SW2(config)# vlan 20
	SW2(config-vlan)# exit

Step 2. Configure Access Ports for VLAN 20.

Configure the ports connected to PC2 (on SW1) and PC4 (on SW2) as access ports in VLAN 20.

Device	Command
SW1 (for PC2)	SW1(config)# interface FastEthernet 0/2
	SW1(config-if)# switchport mode access
	SW1(config-if)# switchport access vlan 20
SW2 (for PC4)	SW2(config)# interface FastEthernet 0/2
	SW2(config-if)# switchport mode access
	SW2(config-if)# switchport access vlan 20

Step 3. Verify VLAN Membership on SW1.

Use the show vlan command to confirm the configuration.

```
SW1# show vlan
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Et0/0, Et0/1, Et0/3, Et1/0
... (other ports in VLAN 1)
20 IT active Et0/2  <-- VERIFY Et0/2 is here
...
```

3. Phase 2: Connectivity Testing (Before Trunk)

At this point, the link between SW1 and SW2 (Gig0/1 to Gig0/2) is still a default access link in VLAN 1.

Step 4. Test Connectivity within VLAN 1 (Expected Success).

PC1 and PC3 are in VLAN 1, and the link between the switches is in VLAN 1.

Device	Command	Expected Result
PC1	PC1# ping 192.168.1.110	**Success.** (Success rate is 60 percent or higher)

Step 5. Test Connectivity within VLAN 20 (Expected Failure).

PC2 and PC4 are in VLAN 20, but the link between SW1 and SW2 only carries VLAN 1 traffic.

Device	Command	Expected Result
PC2	PC2# ping 192.168.20.110	**Failure.** (Success rate is 0 percent)

The failure is expected because VLAN 20 traffic is dropped at the inter-switch link since it is not configured to carry tagged VLAN 20 frames.

4. Phase 3: Trunk Configuration and Final Verification

Step 6. Configure the Inter-Switch Link as a Trunk.

Configure the link between SW1 (Gig0/1) and SW2 (Gig0/2) to carry both VLAN 1 and VLAN 20 traffic using 802.1Q encapsulation.

Device	Command
SW1 (interface Gig0/1)	SW1(config)# interface Gig0/1
	SW1(config-if)# switchport mode trunk
	SW1(config-if)# switchport trunk allowed vlan 1,20
SW2 (interface Gig0/2)	SW2(config)# interface Gig0/2
	SW2(config-if)# switchport mode trunk
	SW2(config-if)# switchport trunk allowed

	vlan 1,20
	SW2(config-if)# switchport mode trunk

Step 7. Verify Trunk Status on SW1.

Use the show interfaces trunk command to confirm the trunk is active and allowing the correct VLANs.

```
SW1# show interfaces trunk
Port   Mode      Encapsulation  Status      Native vlan
Gig0/1  on         802.1q         trunking    1
Port   Vlans allowed on trunk
Gig0/1  1,20  <-- VERIFY ONLY 1 and 20 ARE ALLOWED
...
```

Step 8. Test Connectivity within VLAN 20 (Expected Success).

The trunk link is now active and carrying both VLAN 1 and VLAN 20 traffic.

Device	Command	Expected Result
PC2	PC2# ping 192.168.20.110	**Success.** (Success rate is 60 percent or higher)

5. Troubleshooting Reference Commands

Use these commands to diagnose issues if any of the verification or ping tests fail.

Command	Purpose	When to Use	Troubleshooting Checklist
show vlan brief	Quick check of all VLANs and port assignments.	If PC is unable to reach the gateway or another PC in the same VLAN on the same switch.	Is the PC's port listed under the correct VLAN (1 or 20)? Is the VLAN active?
show interfaces [interface-id]	Detailed port status (mode, VLAN	If connectivity fails or a trunk won't	Is the port in access mode?

switchport	assignment, trunking details).	form.	Does the *Access Mode VLAN* match the PC's intended VLAN? Is the trunk port configured as trunk mode and using 802.1Q?
show interfaces trunk	Displays all trunk ports and their allowed VLANs.	If the VLAN 20 ping fails after configuring the trunk.	Are both ends of the link (Gig0/1 on SW1 and Gig0/2 on SW2) showing trunking status? Does the **Vlans allowed on trunk** list include 1,20 on both switches?
show mac address-table	Verifies the switch is learning the PC's MAC address.	If a ping fails, confirm the switch is seeing traffic from the source.	Is the source PC's MAC address being learned on the correct interface and in the correct VLAN?
show cdp neighbors	Checks the physical connectivity between switches.	If the link between SW1 and SW2 is down (show ip int brief shows down).	Confirms the switches are seeing each other's device IDs and local/remote interfaces.
show ip interface brief	Checks physical and protocol status of all interfaces.	General link check.	Are the PC access ports and the trunk ports showing status and protocol as **up**?

Common Troubleshooting Scenarios:

1. **VLAN 20 Ping Fails (Step 5) - Expected:** The link is not a trunk. **Fix:** Configure the trunk (Step 6).
2. **VLAN 20 Ping Fails (Step 8) - Unexpected:**

- ○ **Check 1:** Is the access port (Et0/2 on SW1/SW2) assigned to VLAN 20? (show vlan brief).
- ○ **Check 2:** Is the inter-switch link actually trunking? (show interfaces trunk).
- ○ **Check 3:** Are VLANs 1 and 20 explicitly allowed on the trunk? (switchport trunk allowed vlan 1,20).

3. **PC1/PC3 Ping Fails (Step 4):** Check the **IP addresses** of PC1 (192.168.1.100) and PC3 (192.168.1.110) to ensure they are correct, and verify the physical link status.