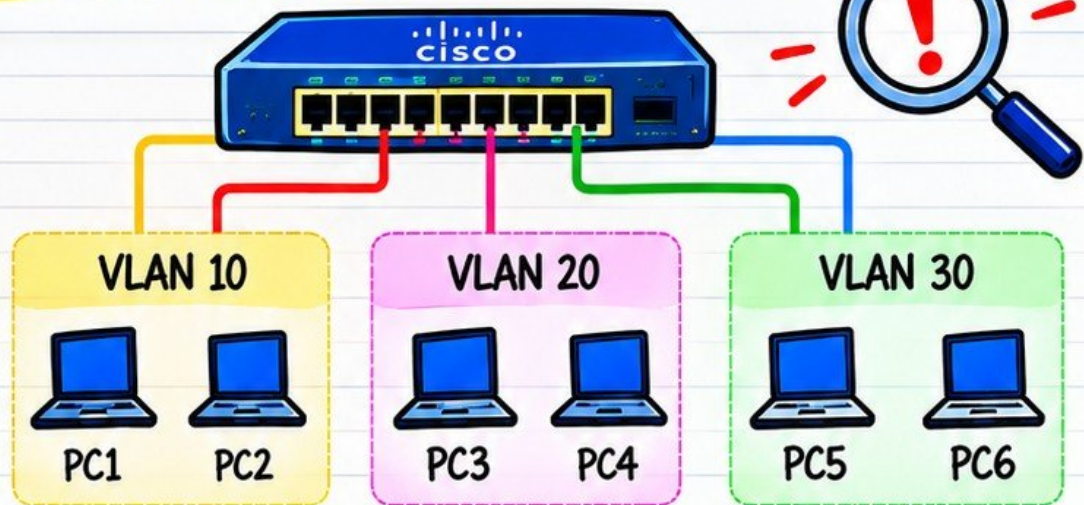
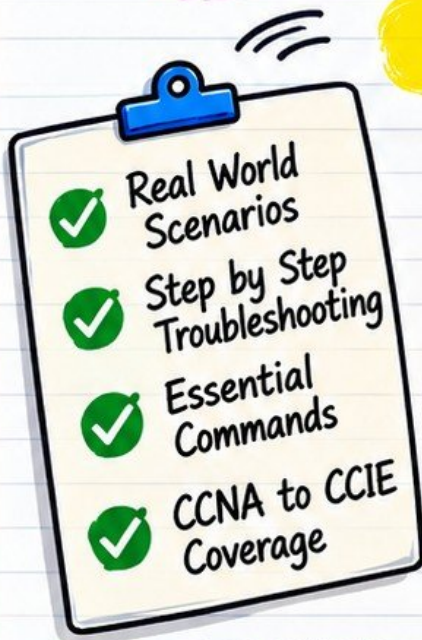


Troubleshooting VLAN Issues

with Commands and Scenarios

CCNA to CCIE Level



VLAN
Not Working

Trunk
Issues

Inter-VLAN
Issues

Access Port
Issues

STP / Native
VLAN Issues

When users face VLAN related issues, follow a systematic troubleshooting approach instead of checking random commands. This helps you to find the root cause quickly.

1 Common VLAN Issues

- ❗ PC not getting IP in a VLAN
- ❗ VLAN not working on access port
- ❗ VLAN not allowed on trunk
- ❗ Inter-VLAN communication not working
- ❗ VLAN missing on switch
- ❗ VLAN not propagating in VTP
- ❗ Trunk down or blocking on STP
- ❗ Users in same VLAN cannot communicate

2 Troubleshooting Workflow

Step 1 Identify the problem and affected VLAN

Get details from user
(Which VLAN, which device,
what is not working)

Step 2 Check physical connectivity

Verify cable, interface status,
link up/down

Step 3 Verify VLAN configuration

Check if VLAN exists,
correctly assigned to ports

Step 4 Check trunk and allowed VLANs

Verify trunk status and
allowed VLAN list

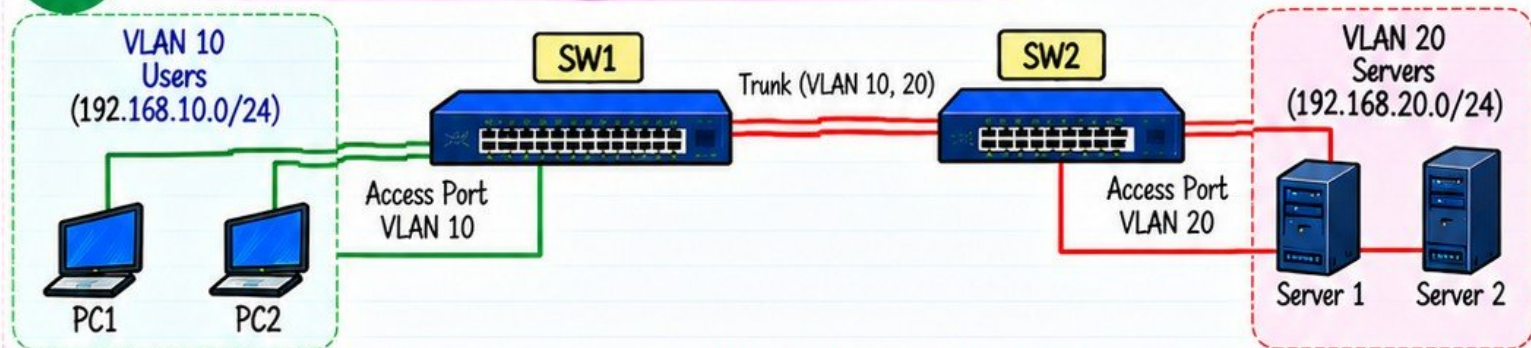
Step 5 Check Layer 2 and STP status

Make sure port is not blocked
and VLAN is forwarding

Step 6 Check end device / DHCP / IP

Verify DHCP, IP, gateway
and VLAN on the host

3 Sample Network Topology for Troubleshooting



4 Key Commands for Initial Checks

✓ Check VLAN Database

Switch# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1
10	Users	active	Fa0/2
20	Servers	active	Fa0/3

Verify if the VLAN exists and is in active state.

✓ Check Interface Status

Switch# **show interfaces status**

Port	Name	Status	VLAN
Fa0/1		connected	10
Fa0/2		connected	10
Fa0/24 (trunk)		connected	trunk

Verify if access ports are in correct VLAN and trunk port is up.

✓ Check Trunk Details

Switch# **show interfaces trunk**

Port	Mode	Encapsulation	Status
Fa0/24	on	802.1q	trunking
Port Vlans allowed on trunk			
Fa0/24	10,20		

Verify if required VLANs are allowed on the trunk.

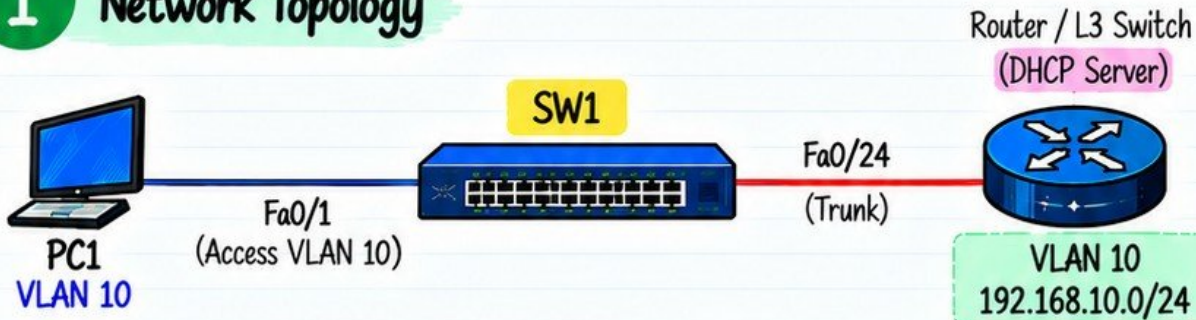
Scenario 1

PC Not Getting IP in VLAN

3/10
Swipe Next

User is connected to VLAN 10 but not getting IP address from DHCP.
Let's troubleshoot this step by step using real commands.

1 Network Topology



Expected Result:

- ✓ PC should get IP in 192.168.10.0/24 from DHCP.

2 Possible Causes

- ! Port not in correct VLAN
- ! VLAN not created
- ! VLAN not allowed on trunk
- ! DHCP not working or not reachable
- ! Switch-Router connectivity issue
- ! STP blocking the port
- ! IP helper-address missing (if DHCP server is in different VLAN)

3 Step 1: Verify PC and Port VLAN

Switch# show interfaces fa0/1 switchport

```
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Access Mode VLAN: 10
Trunking Native Mode VLAN: 1
Trunking VLANs Enabled: None
Trunking VLANs Active: None
```

Make sure port is in correct VLAN (Access VLAN 10)

Switch# show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/24
10	Users	active	Fa0/1
20	Servers	active	-

Verify VLAN is created and in active state.

4 Step 2: Verify VLAN on Trunk

Switch# show interfaces fa0/24 trunk

```
Port    Mode    Encapsulation  Status  Native vlan
Fa0/24  on      802.1q         trunking  1
```

Port Vlan allowed on trunk

```
Fa0/24  1,10,20
```

Port Vlan in spanning tree forwarding state

```
Fa0/24  1,10,20
```

Make sure VLAN 10 is allowed on trunk and is in forwarding state.

5 Step 3: Check DHCP Reachability

Switch# ping 192.168.10.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/3 ms
```

Switch# show ip dhcp snooping binding

MacAddress	IpAddress	Lease(sec)	Type	VLAN
aabb.ccdd.eeff	192.168.10.50	7200	dhcp	10

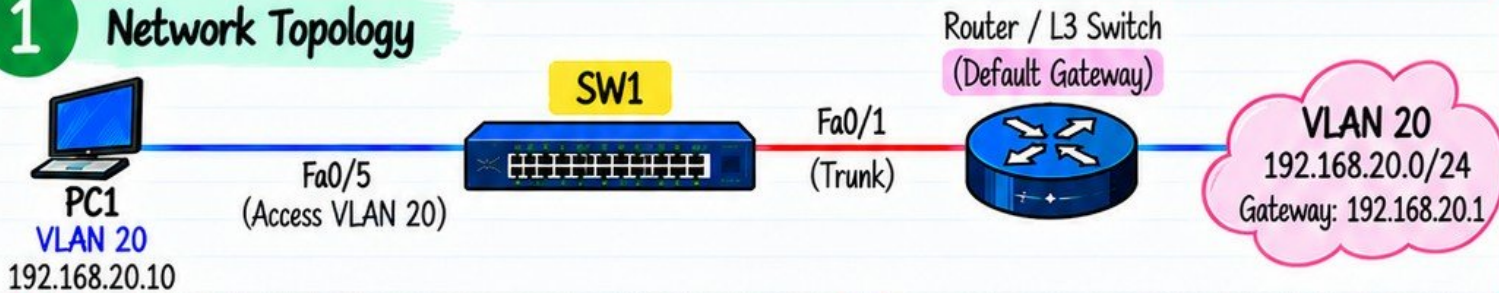
Verify switch can reach DHCP server and DHCP snooping shows bindings (if enabled).



VLAN Not Working on Access Port

PC is connected to VLAN 20 but not getting connectivity.
Let's troubleshoot and fix this step by step.

1 Network Topology



2 Step 1: Check Port Configuration

Switch# show interfaces fa0/5 switchport

```
Name: Fa0/5
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Access Mode VLAN: 20
Trunking Native Mode VLAN: 1
Trunking VLANs Enabled: None
Trunking VLANs Active: None
```

Expected Result:

✓ Access port should be in VLAN 20

✓ Verify that the access port is in correct VLAN (20).
If VLAN is different, update the configuration.

3 Step 2: Check VLAN Status

Switch# show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/24, Gi0/1
10	Users	active	Fa0/1, Fa0/2
20	Servers	active	Fa0/5
30	Management	active	-



Expected Result:

✓ VLAN 20 should be in active state and port Fa0/5 should appear in VLAN 20.

4 Step 3: Verify Physical Link

Switch# show interfaces fa0/5 status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/5	--	connected	20	a-full	100	10/100BaseTX

✓ Status should be connected (not err-disabled or notconnect).
✓ Check for duplex/speed mismatch if needed.

5 Step 4: Test Connectivity from PC

C:\> ping 192.168.20.1

```
Pinging 192.168.20.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

✗ If ping fails, continuing with next steps to find the root cause.



6 Step 5: Common Causes & Fix

Possible Cause	Solution
Port in wrong VLAN	Use: <code>switchport access vlan 20</code>
VLAN not created	Use: <code>vlan 20</code> and verify
Port in shutdown state	Use: <code>no shutdown</code>
Cable / NIC issue	Check physical connectivity
PC IP in wrong subnet	Assign correct IP (192.168.20.x)
VLAN not allowed on trunk (affects gateway reachability)	Add VLAN 20 on trunk: <code>switchport trunk allowed vlan add 20</code>

Pro Tip:

Always check from Layer 1 to Layer 3
physically → VLAN → trunk → gateway → IP configuration.

Users in Same VLAN Cannot Communicate

PC1 and PC2 are in same VLAN but cannot ping each other.
Let's troubleshoot step by step to find the root cause.

1 Network Topology



Expected Result:

- ✓ PC1 and PC2 should be able to ping each other as they are in the same VLAN (Layer 2 communication).

2 Possible Causes

- ! Different VLAN assignment on ports
- ! Interfaces in err-disabled state
- ! Port security blocking the MAC address
- ! STP blocking the port
- ! DHCP or IP configuration issue
- ! ACL or security feature blocking traffic
- ! VLAN not active in the VLAN database

3 Step 1: Verify VLAN on Both Ports

Switch# show interfaces fa0/1 switchport

```

Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Access Mode VLAN: 10
Trunking Native Mode VLAN: 1
Trunking VLANs Enabled: None
Trunking VLANs Active: None
  
```

Both ports should be in the same VLAN and in access mode.

Switch# show vlan brief

VLAN	Name	Status	Ports
1	default	active	-
10	Users	active	Fa0/1, Fa0/2
20	Servers	active	-

4 Step 2: Check Port Status

Switch# show interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	--	connected	10	a-full	100	10/100BaseTX
Fa0/2	--	connected	10	a-full	100	10/100BaseTX

- ✓ Both ports should be in connected state and not err-disabled.

5 Step 3: Check Port Security

Switch# show port-security interface fa0/1

```

Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
  
```

✗ If violation mode is shutdown and unknown MAC is connected, port will be blocked.

6 Step 4: Check STP Status

Switch# show spanning-tree vlan 10

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Altn	BLK	19	128.2	P2p

- ✗ If port is in blocking state, it will not forward traffic.

7 Step 5: Test Connectivity

PC1> ping 192.168.10.20

```

Pinging 192.168.10.20 with 32 bytes:
Reply from 192.168.10.20: bytes=32 time<1ms
Reply from 192.168.10.20: bytes=32 time<1ms
Reply from 192.168.10.20: bytes=32 time<1ms
Reply from 192.168.10.20: bytes=32 time<1ms
  
```

- ✓ If ping works after fix, issue is resolved.

Pro Tips:

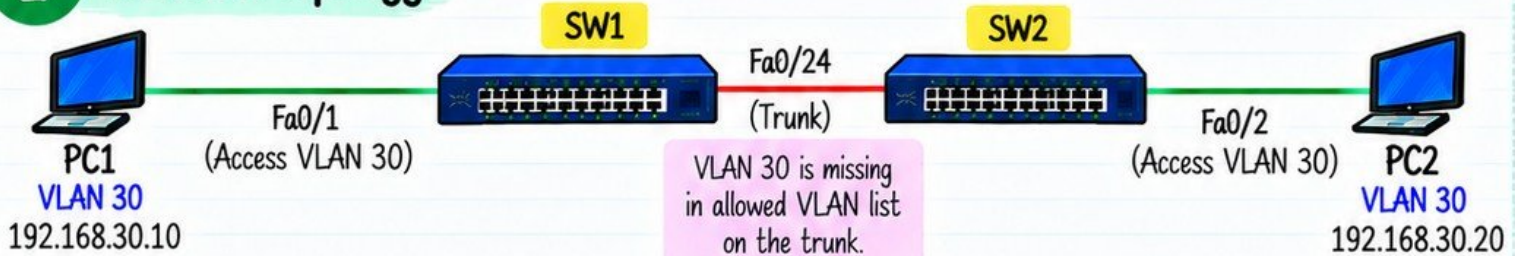
- ✓ Verify same VLAN
- ✓ Check port status
- ✓ Check STP
- ✓ Check port security
- ✓ Verify IP settings
- ✓ Check for ACLs
- ✓ Verify physical cable

Scenario 4

VLAN Not Allowed on Trunk

VLAN 30 is created and assigned to access ports, but devices in VLAN 30 cannot communicate because the VLAN is not allowed on the trunk.

1 Network Topology



2 Verify VLAN Exists

Switch# show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2
10	Users	active	-
20	Servers	active	-
30	Voice	active	-

✓ VLAN 30 is created and active on the switch.

3 Check Trunk Allowed VLANs

Switch# show interfaces trunk

Port	Mode	Encapsulation	Status
Fa0/24	on	802.1q	trunking

Port	Vlans allowed on trunk
Fa0/24	1,10,20

✗ VLAN 30 is not in the allowed VLAN list, so traffic is not passing.

4 Fix: Add VLAN to Trunk

Switch(config)# interface fa0/24

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan
1,10,20,30
Switch(config-if)# end
```

✓ Added VLAN 30 to the trunk allowed list.

5 Verify After Fix

Switch# show interfaces trunk

Port	Mode	Encapsulation	Status
Fa0/24	on	802.1q	trunking

Port	Vlans allowed on trunk
Fa0/24	1,10,20,30

✓ VLAN 30 is now allowed on the trunk.

6 Test Connectivity

PC1> ping 192.168.30.20

```
Pinging 192.168.30.20 with 32 bytes of data:
Reply from 192.168.30.20: bytes=32 time<1ms
Reply from 192.168.30.20: bytes=32 time<1ms
Reply from 192.168.30.20: bytes=32 time<1ms
Reply from 192.168.30.20: bytes=32 time<1ms
Ping statistics for 192.168.30.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

✓ PC1 and PC2 can now communicate successfully.

7 Key Takeaways

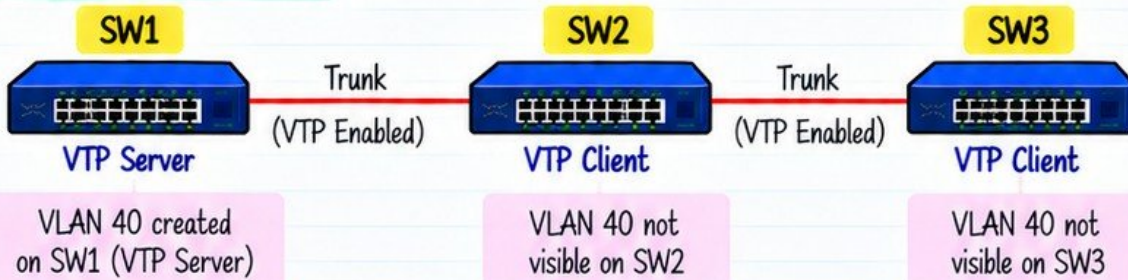
- ✓ Always verify VLAN is created and active.
- ✓ Check trunk mode and allowed VLAN list.
- ✓ If VLAN is missing, add it to the trunk.
- ✓ Use show interfaces trunk to verify.
- ✓ After fixing, test connectivity from end devices.

Pro Tip:
In production networks, consider using "switchport trunk allowed vlan add <vlan-id>" instead of replacing the list.

VLAN Not Propagating in VTP

VLAN is created on VTP server but it is not visible on other VTP clients.
Let's troubleshoot and fix this step by step.

1 Network Topology



Expected Result:

- ✓ VLAN 40 should be automatically propagated to all VTP clients (SW2 and SW3).

2 Possible Causes

- ! VTP mode mismatch (server/client/transparent)
- ! VTP domain name mismatch
- ! VTP version mismatch (V1/V2/V3)
- ! Trunk link not working or VTP not allowed
- ! Pruning enabled on VTP (VLAN filtered)
- ! Higher VTP revision number on client
- ! VLAN database in client is corrupt

3 Step 1: Verify VTP Status on All Switches

Switch# show vtp status

```
VTP Version : 2
Configuration Revision : 15
Maximum VLANs supported locally : 1005
Number of existing VLANs : 10
VTP Operating Mode : Server
VTP Domain Name : TECHNETWORKK
VTP Pruning Mode : Disabled
```

Verify same domain name, same VTP version and correct VTP mode on all switches.

4 Step 2: Verify Trunk and VTP Allowed

Switch# show interfaces trunk

```
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1
```

Vlans allowed on trunk

```
Fa0/1 1-1005
```

- ✓ Make sure the trunk is up and VLAN 40 is allowed on the trunk.

5 Step 3: Check VLAN on Client Switch

Switch# show vlan brief

```
VLAN Name Status Ports
1 default active -
10 Users active Fa0/2
20 Servers active -
40 (Not Present)
```

VLAN 40 is not present on client switches.

6 Step 4: Verify VTP Revision Number

Switch# show vtp status

```
Configuration Revision : 15
VTP Operating Mode : Client
VTP Domain Name : TECHNETWORKK
```

- ✗ If client has higher revision number than server, it will not accept updates from the server.

7 Step 5: Fix the Issue

- ✓ Configure same VTP domain name on all switches
- ✓ Use same VTP version (V1/V2/V3)
- ✓ Configure correct VTP mode (server/client)
- ✓ Ensure trunk is up and VLAN is allowed
- ✓ If revision number is higher, reset VTP on client (e.g., delete vlan.dat and reload)

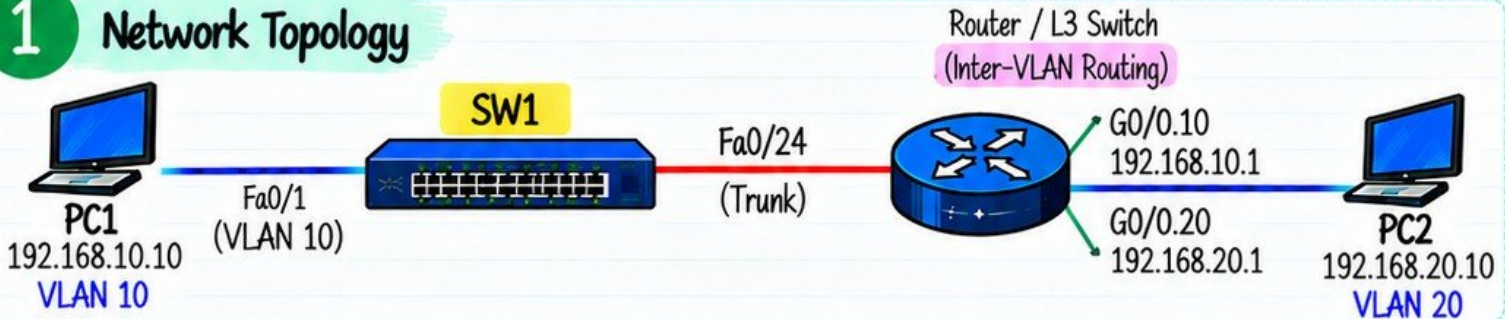
Pro Tip:

If the client has a higher revision number and is not accepting updates, you can force it to accept by deleting the vlan.dat file and reloading the switch (in lab or planned maintenance window).

Inter-VLAN Communication Issue

PC in VLAN 10 can ping PC in VLAN 20 but cannot ping the Gateway or other VLANs. Let's troubleshoot this step by step.

1 Network Topology



2 Possible Causes

- ! SVI / Subinterface is down
- ! VLAN not allowed on trunk
- ! Incorrect IP on SVI/Subinterface
- ! Routing not enabled (ip routing)
- ! ACL blocking inter-VLAN traffic
- ! Wrong default gateway on PC
- ! HSRP/VRRP not working (redundancy)
- ! Routing missing between VLANs

3 Step 1: Verify SVI/Subinterface Status

Switch# show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan10	192.168.10.1	YES	manual	up	up
Vlan20	192.168.20.1	YES	manual	down	down

- ✗ VLAN 20 interface is down, so inter-VLAN routing is not working.

4 Step 2: Verify VLAN and Trunk

Switch# show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/24	on	802.1q	trunking	1

Vlans allowed on trunk

1,10,20

- ✓ VLAN 10 and 20 are allowed on the trunk.

6 Step 4: Check Access-List (ACL)

Switch# show access-lists

```
Extended IP access list BLOCK_INTERVLAN
10 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
20 permit ip any any
```

- ✗ ACL is blocking traffic between VLAN 10 and VLAN 20.

5 Step 3: Verify Routing is Enabled

Switch# show running-config | include ip routing

```
ip routing
```

Note:
For inter-VLAN routing, make sure "ip routing" is enabled on the L3 Switch / Router.

7 Step 5: Verify Default Gateway on PC



PC1 (VLAN 10)
IP Address : 192.168.10.10
Subnet Mask : 255.255.255.0
Default GW : 192.168.10.1



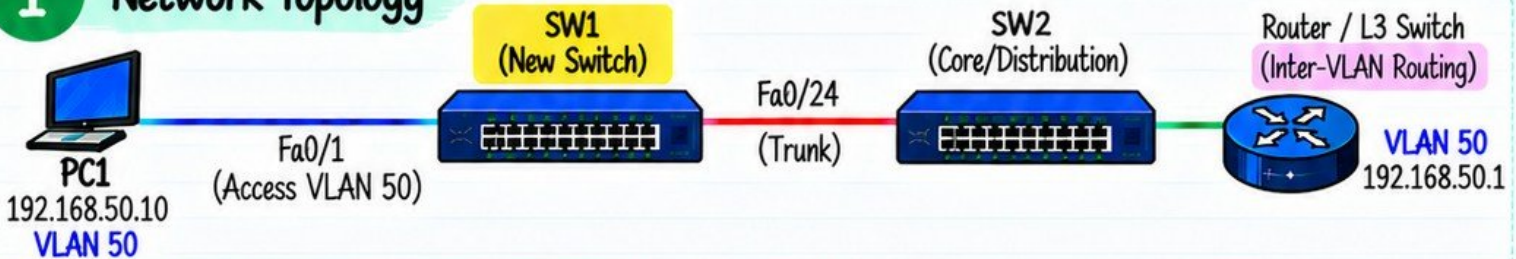
PC2 (VLAN 20)
IP Address : 192.168.20.10
Subnet Mask : 255.255.255.0
Default GW : 192.168.20.1

Pro Tip:
If default gateway is wrong, PC will not be able to reach other VLANs even if routing is working.

VLAN Not Working After Switch Replacement

After replacing a switch, users in VLAN 50 are not getting connectivity because trunk and VLAN configuration is missing on the new switch. Let's troubleshoot and fix this step by step.

1 Network Topology



2 Symptoms

- ! Users in VLAN 50 cannot ping gateway
- ! Other VLANs are working fine
- ! New switch was recently replaced
- ! PC gets APIPA (169.254.x.x) or no response
- ! No entry for VLAN 50 in switch
- ! Trunk link not allowing VLAN 50

3 Step 1: Check VLAN Exists

Switch# show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2
10	Users	active	-
20	Servers	active	-
30	Voice	active	-
50	(Not Present)		

Expected:
VLAN 50 should be present in the VLAN database.

✗ VLAN 50 is missing on the new switch.

4 Step 2: Check Trunk Allowed VLANs

Switch# show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/24	on	802.1q	trunking	1
Vlans allowed on trunk				
1,10,20,30				

✗ VLAN 50 is not allowed on the trunk.

5 Step 3: Check Port Configuration

Switch# show interfaces fa0/1 switchport

Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Access Mode VLAN: 1
Trunking Native Mode VLAN: 1
Trunking VLANs Enabled: None
Trunking VLANs Active: None

Expected:
Access port should be in VLAN 50.

✗ Port is in VLAN 1 instead of VLAN 50.

6 Step 4: Fix the Configuration

```
Switch(config)# vlan 50
Switch(config-vlan)# name HR
Switch(config-vlan)# exit
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 50
Switch(config-if)# exit
Switch(config)# interface fa0/24
Switch(config-if)# switchport trunk allowed vlan add 50
```

7 Step 5: Verify After Fix

Switch# show vlan brief

VLAN	Name	Status	Ports
1	default	active	-
10	Users	active	-
20	Servers	active	-
30	Voice	active	-
50	HR	active	Fa0/1

✓ VLAN 50 is now created and working.

Also Verify:

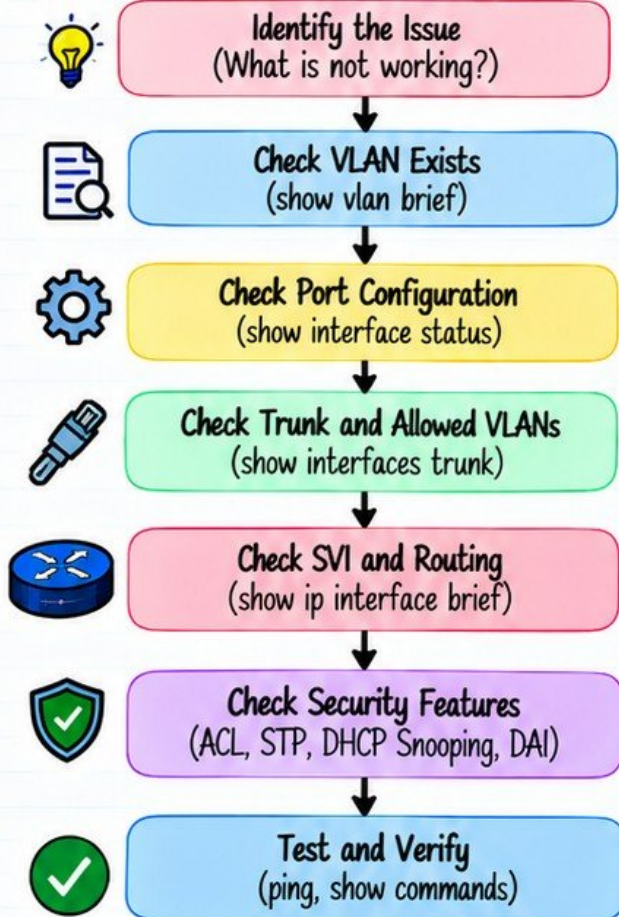
- Ping gateway 192.168.50.1
- Check trunk allowed VLANs
- Verify routing between VLANs

Scenario 8 (Final)

VLAN Troubleshooting Summary

Use this final checklist and command sheet to quickly troubleshoot any VLAN issue from CCNA to CCIE level.

1 VLAN Troubleshooting Flow



2 Important Troubleshooting Commands

Task	Command
Check VLAN list	show vlan brief
Check interface status	show interfaces status
Check trunk details	show interfaces trunk
Check allowed VLANs	show interfaces trunk include Vlan
Check interface config	show running config interface fa0/1
Check SVI status	show ip interfac brief
Check MAC address table	show mac address-table vlan 10
Check STP status	show spanning-tree vlan 10
Check VTP status	show vtp status
Check routing table	show ip route
Check access-list	show access-lists
Debug (if required)	debug spanning-tree events debug vlan

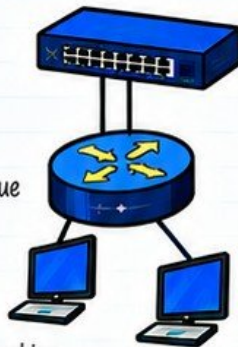
3 Common Root Causes Checklist

- ✓ VLAN not created or not active
- ✓ Access port assigned to wrong VLAN
- ✓ Trunk not allowing the required VLAN
- ✓ VLAN not present on remote switch
- ✓ VTP mode / domain / revision mismatch
- ✓ SVI is down or missing (for inter-VLAN)
- ✓ IP routing not enabled
- ✓ ACL blocking inter-VLAN traffic
- ✓ STP blocking the port
- ✓ Security features (DHCP Snooping, DAI, Port Security)
- ✓ Default gateway issue on end device
- ✓ Incorrect physical or logical topology

Pro Tip:
In real networks, check Layer 2, Layer 3 and security features together. Most VLAN issues are a combination of multiple misconfigurations.

4 Scenario Examples Covered

- ✓ Users in same VLAN cannot communicate
- ✓ VLAN not allowed on trunk
- ✓ Inter-VLAN communication issue
- ✓ VLAN not propagating in VTP
- ✓ SVI down or not configured
- ✓ Wrong default gateway / routing issue
- ✓ ACL blocking inter-VLAN traffic
- ✓ STP blocking the port
- ✓ Port security / DHCP snooping issue
- ✓ New switch replacement VLAN not working



5 Key Takeaways

- ✓ Always verify VLAN is created and active.
- ✓ Check port mode (access/trunk) and allowed VLANs.
- ✓ Verify SVI, routing and default gateway.
- ✓ Check security features (ACL, STP, DHCP Snooping).
- ✓ Use proper show and debug commands.
- ✓ Test from end devices after every change.
- ✓ Follow a structured troubleshooting approach.
- ✓ Most VLAN issues are Layer 2 related.
- ✓ Document the final working configuration.

Remember:
VLAN troubleshooting is one of the most common real-world network issues from CCNA to CCIE level. A systematic approach saves time and helps find the root cause quickly.