CCNA 200-301 v1.1

MODULE 2 — NETWORK ACCESS

Complete Hands-on Training Labs

Topology • Configuration • Verification • Troubleshooting

NETWORK GUIDE ACADEMY

Instructor / Student Lab Guide

Scope: This guide covers the current CCNA v1.1 Network Access objectives 2.1 through 2.9. The final capstone integrates VLANs, trunks, EtherChannel, Rapid PVST+, device management and wireless infrastructure in one campus scenario. Supplementary PAgP EtherChannel and classic PVST+ STP foundation labs are also included for broader operational practice.

Module 2 Lab Map

- 2.1 VLANs spanning multiple switches — access ports, data/voice VLANs, default VLAN and connectivity
- 2.2 Interswitch connectivity — trunk ports, 802.1Q, native VLAN and allowed VLAN control
- 2.3 Layer 2 discovery — CDP and LLDP
- 2.4 EtherChannel — Layer 2/Layer 3 LACP plus a supplementary PAgP negotiation lab
- 2.5 STP and Rapid PVST+ — classic PVST+ root/port election, Rapid PVST+, PortFast, Root Guard, Loop Guard, BPDU Filter and BPDU Guard
- 2.6 Wireless architectures and AP modes — autonomous, controller-based, cloud-managed, local/FlexConnect/monitor/sniffer/bridge
- 2.7 WLAN infrastructure — AP/WLC physical connectivity, access/trunk ports and LAG
- 2.8 Network device management — console, Telnet, SSH, HTTP/HTTPS, TACACS+/RADIUS and cloud-managed concepts
- 2.9 Wireless LAN GUI interpretation — WLAN creation fields, security, QoS and advanced settings
- Integrated capstone — router-on-a-stick, VLANs, LACP, Rapid PVST+, SSH and wireless infrastructure

How to use the detailed device configurations

Each lab uses one configuration path only. Commands are not repeated in an abbreviated section and then repeated again later. The device-by-device configuration shown in the Lab execution section is the single source of truth for that lab.

Verification output is representative Cisco IOS/IOS XE output. MAC addresses, interface hardware strings, counters, timers, software versions and some command formatting can vary by platform. Focus on the fields identified under What to verify.

Follow the lab in order: topology and addressing plan → Device 1 complete configuration → remaining device configurations → verification command and expected output → What to verify → end-to-end test → troubleshooting/fault exercise. Do not re-enter a configuration unless the lab explicitly tells you to change it for a fault or mode-comparison test.

Recommended Lab Platforms

Cisco Packet Tracer for VLAN, trunking, STP, EtherChannel, basic wireless and management-access practice.

Cisco Modeling Labs (CML), EVE-NG or GNS3 with compatible IOS/IOS XE images for more realistic CLI behavior.

Physical Catalyst switches / IOS XE routers when available. Interface names may differ; adapt Gi/Fa/Te numbering to your platform.

For WLC tasks, use a supported controller simulator, Catalyst 9800 lab, Packet Tracer wireless components, or instructor screenshots for interpretation.

Standard Verification Workflow

1. Confirm physical/interface state before checking higher-layer configuration.
2. Validate VLAN and trunk state; then check STP/EtherChannel state where applicable.
3. Check management IP, default gateway/routing and neighbor discovery.
4. Run reachability tests (ping/SSH/GUI association).
5. Use show commands to prove the expected state, not only a successful ping.
6. Introduce one fault, predict the symptom, verify the fault, correct it, and re-run the same verification.

Lab 2.1 — VLANs Across Multiple Switches — Data and Voice VLANs

CCNA objective: Configure and verify VLANs (normal range) spanning multiple switches; access ports (data and voice), default VLAN and connectivity.

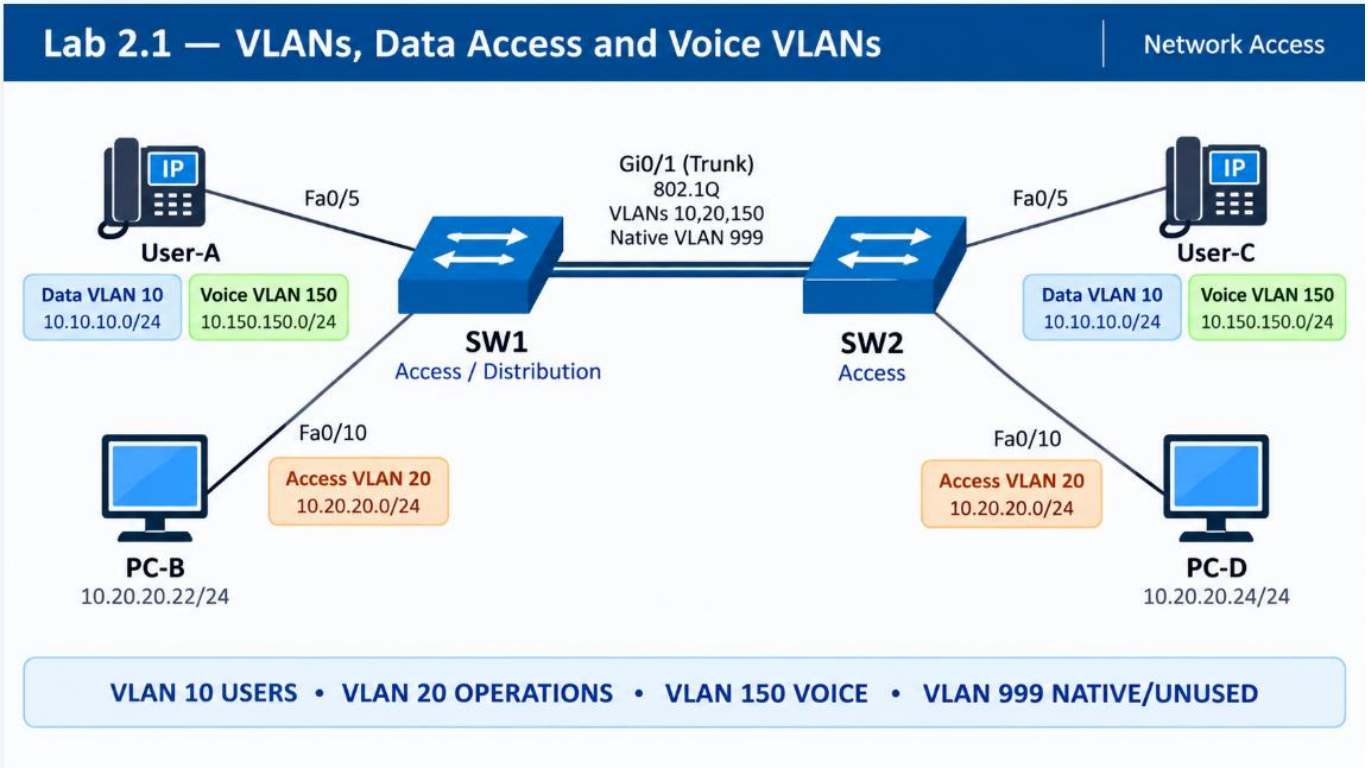


Figure 2.1: VLANs Across Multiple Switches — Data and Voice VLANs reference topology

Lab objectives

- Create normal-range VLANs on two switches.
- Move user ports out of VLAN 1 and assign access VLANs.
- Configure a data VLAN and a voice VLAN on the same switchport.
- Verify VLAN membership, access mode, voice VLAN behavior and end-to-end Layer 2 reachability.
- Recognize common VLAN misconfiguration symptoms.

Addressing and VLAN plan

Item	Value	Purpose
VLAN 10	USERS	User data
VLAN 20	OPERATIONS	Operations data
VLAN 150	VOICE	IP phones
VLAN 999	NATIVE-BLACKHOLE	Native / unused
PC-A / PC-C	10.10.10.11 / .33	VLAN 10
PC-B / PC-D	10.20.20.22 / .24	VLAN 20

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device configuration and verification

SW1 - Complete lab configuration

```
enable
configure terminal
hostname SW1
!
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 150
 name VOICE
vlan 999
 name NATIVE-BLACKHOLE
!
interface FastEthernet0/5
 description USER-A_PHONE_AND_PC
 switchport mode access
 switchport access vlan 10
 switchport voice vlan 150
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/10
 description PC-B_OPERATIONS
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW2
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 no shutdown
end
write memory
```

SW2 - Complete lab configuration

```
enable
configure terminal
hostname SW2
!
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 150
```

```
 name VOICE
vlan 999
 name NATIVE-BLACKHOLE
!
interface FastEthernet0/5
 description USER-C_PHONE_AND_PC
 switchport mode access
 switchport access vlan 10
 switchport voice vlan 150
 spanning-tree portfast
 no shutdown
!
interface FastEthernet0/10
 description PC-D_OPERATIONS
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 no shutdown
end
write memory
```

End-device addressing

- PC-A: 10.10.10.11/24, connected through the data side of the phone on SW1 Fa0/5. Default gateway is not required for this Layer 2-only lab.
- PC-C: 10.10.10.33/24, connected through the data side of the phone on SW2 Fa0/5.
- PC-B: 10.20.20.22/24 on SW1 Fa0/10.
- PC-D: 10.20.20.24/24 on SW2 Fa0/10.
- Cisco IP phones use voice VLAN 150. The switch advertises the voice VLAN to supported phones; the attached PC remains in data VLAN 10.

Verification 1 - VLAN membership

```
SW1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
10   USERS                            active    Fa0/5
20   OPERATIONS                       active    Fa0/10
150  VOICE                            active
999  NATIVE-BLACKHOLE                 active
```

What to verify

- VLANs 10, 20, 150 and 999 exist and are active.

- Fa0/5 appears under VLAN 10 because VLAN 10 is the data access VLAN; the voice VLAN is verified with the switchport command, not by expecting Fa0/5 under VLAN 150 in show vlan brief.
- Fa0/10 appears under VLAN 20.

Verification 2 - Data and voice access port

```
SW1# show interfaces fa0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Access Mode VLAN: 10 (USERS)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 150 (VOICE)
```

What to verify

- Administrative Mode and Operational Mode are static access.
- Access Mode VLAN is 10.
- Voice VLAN is 150.

Verification 3 - Inter-switch trunk

```
SW1# show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Gi0/1       on           802.1q         trunking      999

Port        Vlans allowed on trunk
Gi0/1       10,20,150,999

Port        Vlans allowed and active in management domain
Gi0/1       10,20,150,999

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       10,20,150,999
```

What to verify

- Gi0/1 is trunking with 802.1Q.
- Native VLAN is 999 on both SW1 and SW2.
- VLANs 10, 20 and 150 are allowed and active across the trunk.

Verification 4 - MAC learning and Layer 2 reachability

```
SW1# show mac address-table dynamic vlan 10
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0050.7966.6801    DYNAMIC     Fa0/5
  10    0050.7966.6803    DYNAMIC     Gi0/1

PC-A> ping 10.10.10.33
Reply from 10.10.10.33: bytes=32 time<1ms TTL=128
```

```
Reply from 10.10.10.33: bytes=32 time<1ms TTL=128
Reply from 10.10.10.33: bytes=32 time<1ms TTL=128
Reply from 10.10.10.33: bytes=32 time<1ms TTL=128
```

What to verify

- The local VLAN 10 endpoint is learned on Fa0/5 and the remote VLAN 10 endpoint is learned through Gi0/1.
- PC-A reaches PC-C because both are in VLAN 10 and VLAN 10 is carried across the trunk.
- Repeat the same test between PC-B and PC-D for VLAN 20.

Troubleshooting drills

1. Put PC-B port in VLAN 10 by mistake. Predict which hosts it can reach, then verify with "**show vlan brief**".

2. Delete VLAN 20 from SW2 and observe how the access port appears/inactivates depending on platform. Re-create the VLAN.

3. Remove the voice VLAN command from SW1 Fa0/5 and verify the switchport operational data again.

Lab 2.2 — Interswitch Connectivity — 802.1Q Trunks and Native VLAN

CCNA objective: Configure and verify interswitch connectivity: trunk ports, 802.1Q and native VLAN.

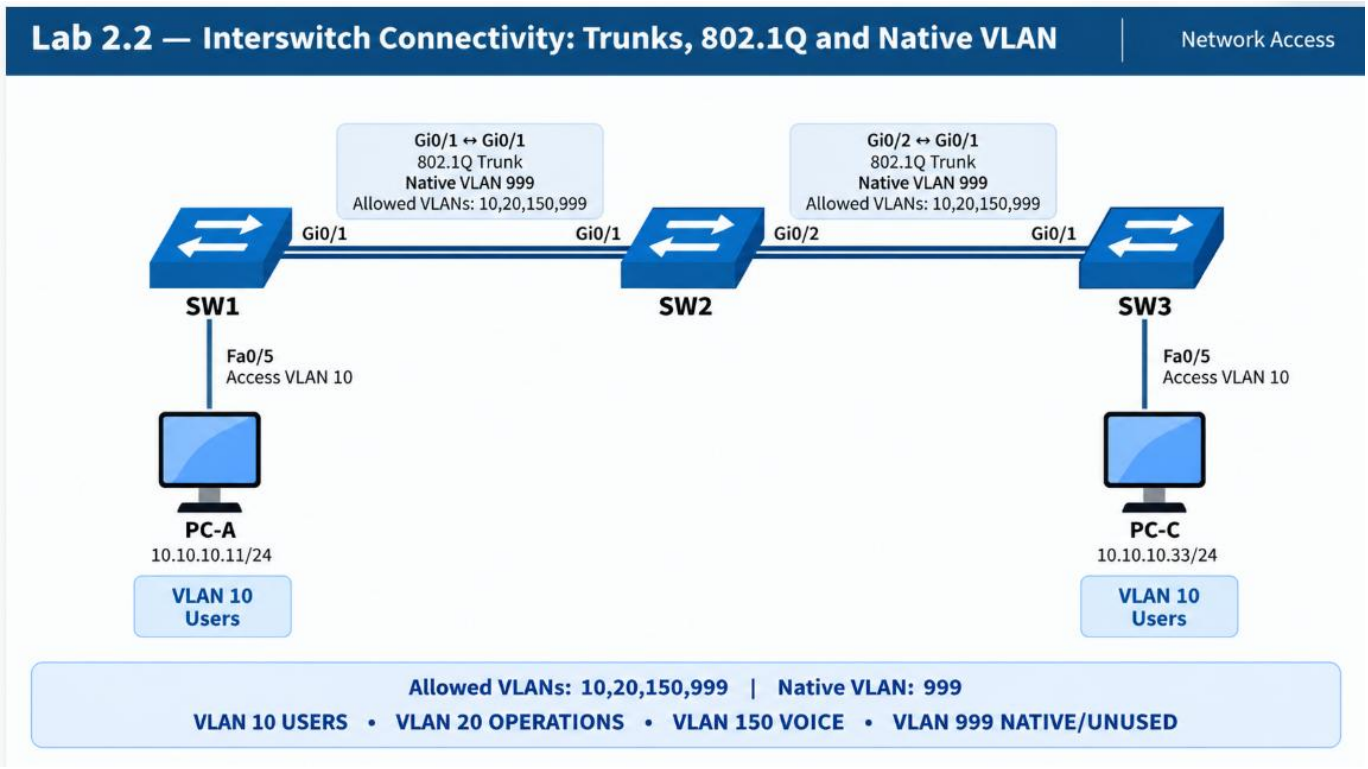


Figure 2.2: Interswitch Connectivity — 802.1Q Trunks and Native VLAN reference topology

Lab objectives

- Build static 802.1Q trunks between three switches.
- Set VLAN 999 as the native VLAN on both ends of every trunk.
- Restrict allowed VLANs and verify the active forwarding list.
- Troubleshoot trunk mode, native VLAN and allowed-VLAN mismatches.

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device configuration and verification

SW1 - Complete lab configuration

```
enable
configure terminal
hostname SW1
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 150
 name VOICE
vlan 999
 name NATIVE-BLACKHOLE
```

```
!
interface FastEthernet0/5
 description PC-A_VLAN10
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW2_GI0_1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 no shutdown
end
write memory
```

SW2 - Complete lab configuration

```
enable
configure terminal
hostname SW2
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 150
 name VOICE
vlan 999
 name NATIVE-BLACKHOLE
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW1_GI0_1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 no shutdown
!
interface GigabitEthernet0/2
 description TRUNK_TO_SW3_GI0_1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 no shutdown
end
write memory
```

SW3 - Complete lab configuration

```
enable
configure terminal
hostname SW3
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 150
```

```
 name VOICE
vlan 999
 name NATIVE-BLACKHOLE
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW2_GI0_2
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 no shutdown
!
interface FastEthernet0/5
 description PC-C_VLAN10
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 no shutdown
end
write memory
```

End-device addressing

- PC-A: 10.10.10.11/24 on SW1 Fa0/5.
- PC-C: 10.10.10.33/24 on SW3 Fa0/5.

Verification 1 - SW2 must see both trunks

```
SW2# show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Gi0/1       on           802.1q         trunking      999
Gi0/2       on           802.1q         trunking      999

Port        Vlans allowed on trunk
Gi0/1       10,20,150,999
Gi0/2       10,20,150,999

Port        Vlans allowed and active in management domain
Gi0/1       10,20,150,999
Gi0/2       10,20,150,999
```

What to verify

- Both Gi0/1 and Gi0/2 are in trunking state.
- Native VLAN 999 is identical on both trunks.
- The allowed VLAN list is exactly 10,20,150,999.

Verification 2 - Detailed trunk switchport state

```
SW2# show interfaces gi0/2 switchport
Name: Gi0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Trunking Native Mode VLAN: 999 (NATIVE-BLACKHOLE)
Trunking VLANs Enabled: 10,20,150,999
```

What to verify

- Administrative and operational modes are trunk.
- 802.1Q is the operational encapsulation where the platform displays this field.
- Native VLAN 999 and the allowed VLAN list match the peer.

Verification 3 - End-to-end VLAN 10 forwarding

```
SW1# show mac address-table dynamic vlan 10
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0050.7966.6801    DYNAMIC     Fa0/5
  10    0050.7966.6803    DYNAMIC     Gi0/1

PC-A> ping 10.10.10.33
Reply from 10.10.10.33: bytes=32 time<1ms TTL=128
```

What to verify

- SW1 learns the remote PC-C MAC through Gi0/1; SW3 learns the remote PC-A MAC through Gi0/1.
- The ping succeeds only when VLAN 10 is created and forwarding over both trunks.

Fault injection

1. Remove VLAN 10 from SW2 Gi0/2 allowed list. PC-A and PC-C should lose Layer 2 connectivity even though the trunk remains up.

2. Set SW3 Gi0/1 native VLAN to 1. Observe native-VLAN mismatch messaging/neighbor information where supported.

3. Change one side to access mode and use `show interfaces trunk` to identify the missing trunk.

Lab 2.3 — Layer 2 Discovery — CDP and LLDP

CCNA objective: Configure and verify Layer 2 discovery protocols: Cisco Discovery Protocol and LLDP.

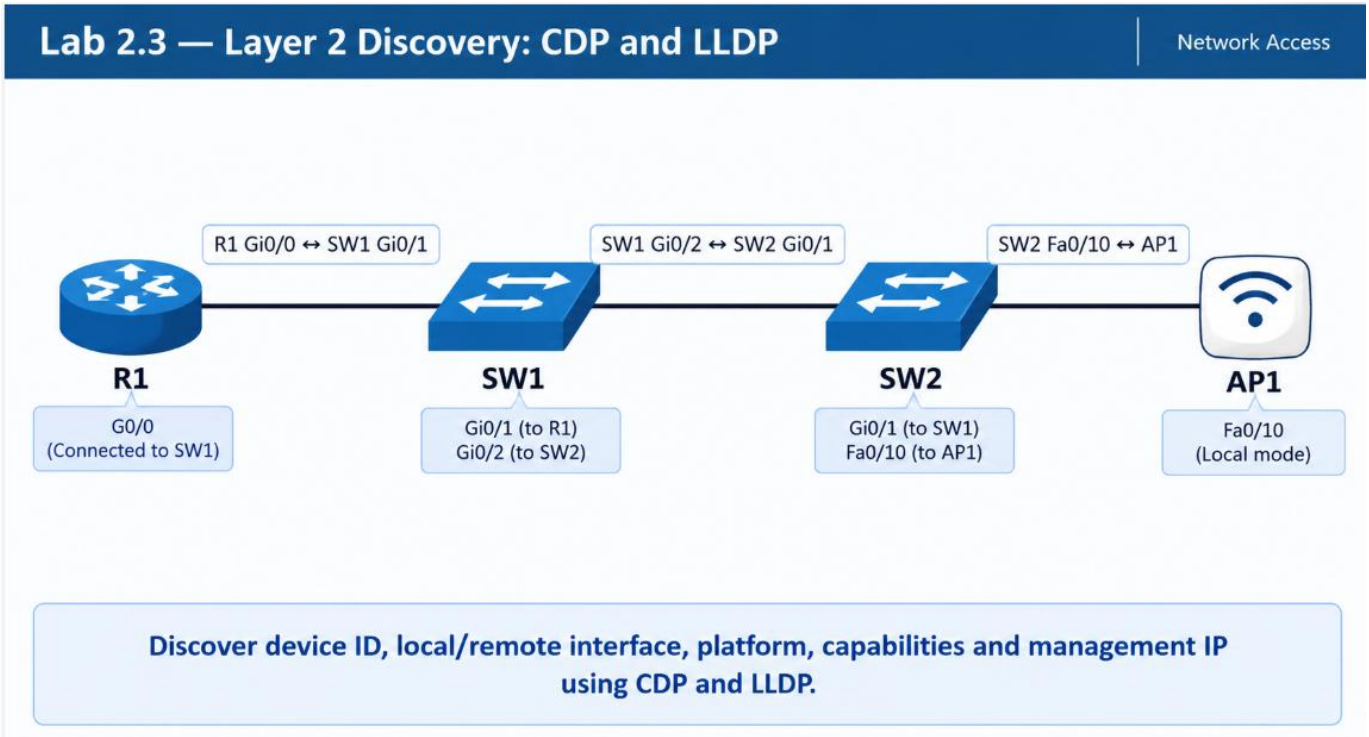


Figure 2.3: Layer 2 Discovery — CDP and LLDP reference topology

Lab objectives

- Use CDP to discover directly connected Cisco neighbors.
- Enable LLDP globally and per interface, then compare the information learned.
- Verify local and remote interface names, platform/capabilities and management addresses.
- Disable discovery selectively where policy requires it.

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device configuration and verification

R1 - Discovery configuration

```
enable
configure terminal
hostname R1
cdp run
lldp run
!
interface GigabitEthernet0/0
 description TO_SW1_GI0_1
 no shutdown
 lldp transmit
 lldp receive
end
```

SW1 - Discovery configuration

```
enable
configure terminal
hostname SW1
cdp run
lldp run
!
interface GigabitEthernet0/1
 description TO_R1_GI0_0
 no shutdown
 cdp enable
 lldp transmit
 lldp receive
!
interface GigabitEthernet0/2
 description TO_SW2_GI0_1
 no shutdown
 cdp enable
 lldp transmit
 lldp receive
!
interface FastEthernet0/24
 description DISCOVERY_DISABLED_TEST_PORT
 no cdp enable
 no lldp transmit
 no lldp receive
end
```

SW2 - Discovery configuration

```
enable
configure terminal
hostname SW2
cdp run
lldp run
!
interface GigabitEthernet0/1
 description TO_SW1_GI0_2
 no shutdown
 cdp enable
 lldp transmit
 lldp receive
!
interface FastEthernet0/10
 description TO_AP1
 no shutdown
 lldp transmit
 lldp receive
end
```

Verification 1 - CDP neighbors from SW1

```
SW1# show cdp neighbors
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R1               Gig 0/1          153        R S I       ISR       Gig 0/0
SW2              Gig 0/2          164        S I         C2960     Gig 0/1
```

What to verify

- R1 is discovered on local Gi0/1 and reports remote Gi0/0.
- SW2 is discovered on local Gi0/2 and reports remote Gi0/1.
- Device ID, local interface, remote Port ID and capability/platform fields match the physical cabling.

Verification 2 - CDP detail

```
SW1# show cdp neighbors detail
-------------------------
Device ID: R1
Entry address(es):
  IP address: 10.0.0.1
Platform: Cisco ISR,  Capabilities: Router Switch IGMP
Interface: GigabitEthernet0/1,  Port ID (outgoing port): GigabitEthernet0/0
Holdtime : 153 sec
```

What to verify

- The management/IP address, platform, capabilities and remote port are plausible for R1.
- A wrong remote port usually indicates incorrect cabling or that a different physical link is being inspected.

Verification 3 - LLDP neighbors from SW1

```
SW1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (W) WLAN Access Point

Device ID           Local Intf     Hold-time  Capability      Port ID
R1                  Gi0/1          120        R               Gi0/0
SW2                 Gi0/2          120        B               Gi0/1
```

What to verify

- The same directly connected neighbors can appear in both CDP and LLDP databases when both protocols are enabled.
- LLDP is vendor-neutral and is the preferred discovery mechanism for non-Cisco neighbors.

Verification 4 - Disabled discovery test port

```
SW1# show cdp interface fa0/24
% CDP is not enabled on interface FastEthernet0/24

SW1# show lldp interface fa0/24
Tx: disabled
Rx: disabled
```

- What to verify
- CDP is disabled only on Fa0/24 while remaining globally enabled.
- LLDP transmit and receive are disabled on the selected test port.

Verification questions

1. From SW1, what is the Device ID and remote port for R1?

2. From SW1, what is the Device ID and remote port for SW2?

3. Which protocol provides the most useful detail for a non-Cisco neighbor in your lab?

4. If both CDP and LLDP are enabled, can the same physical neighbor appear in both neighbor databases?

Training focus: Discovery protocols are local-link mechanisms. They do not prove routed reachability; use them to validate physical/logical adjacency and cabling before troubleshooting higher layers.

Lab 2.4 — EtherChannel — Layer 2 and Layer 3 LACP

CCNA objective: Configure and verify Layer 2/Layer 3 EtherChannel using LACP.

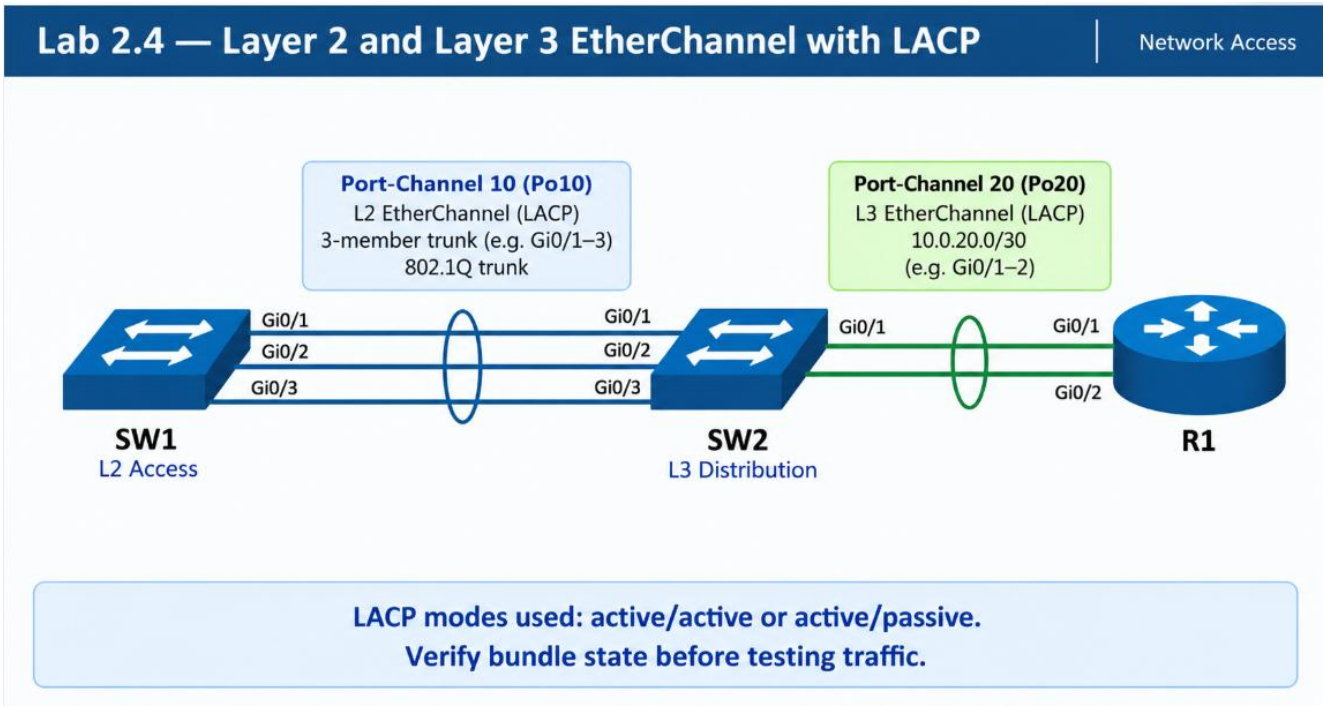


Figure 2.4: EtherChannel — Layer 2 and Layer 3 LACP reference topology

Lab objectives

- Bundle three physical links into a Layer 2 Port-Channel trunk.
- Build a routed Layer 3 Port-Channel where the platform supports routed switchports.
- Use LACP active/passive modes.
- Verify member consistency, bundle protocol and forwarding state.
- Recognize suspended/standalone members caused by mismatch.

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device configuration and verification

SW1 - Layer 2 LACP Port-Channel10

```
enable
configure terminal
hostname SW1
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 150
 name VOICE
vlan 999
 name NATIVE-BLACKHOLE
!
interface range GigabitEthernet0/1 - 3
```

```
 description LACP_MEMBER_TO_SW2
 switchport mode trunk
switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 channel-group 10 mode active
 no shutdown
!
interface Port-channel10
 description LACP_TRUNK_TO_SW2
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 no shutdown
end
write memory
```

SW2 - Layer 2 Port-Channel10 and Layer 3 Port-Channel20

```
enable
configure terminal
hostname SW2
ip routing
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 150
 name VOICE
vlan 999
 name NATIVE-BLACKHOLE
!
interface range GigabitEthernet0/1 - 3
 description LACP_MEMBER_TO_SW1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 channel-group 10 mode passive
 no shutdown
!
interface Port-channel10
 description LACP_TRUNK_TO_SW1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,150,999
 no shutdown
!
interface range GigabitEthernet1/0/47 - 48
 description L3_LACP_MEMBER_TO_R1
 no switchport
 channel-group 20 mode active
 no shutdown
!
interface Port-channel20
 description L3_LACP_TO_R1
 no switchport
 ip address 10.0.20.1 255.255.255.252
```

```
 no shutdown
end
write memory
```

R1 - Layer 3 LACP peer for Port-Channel20

Use this configuration only on a router/platform that supports EtherChannel on the selected routed interfaces. If your Packet Tracer router does not support it, use a platform with routed EtherChannel capability for this part of the lab.

```
enable
configure terminal
hostname R1
!
interface range GigabitEthernet0/0 - 1
 description L3_LACP_MEMBER_TO_SW2
 channel-group 20 mode active
 no shutdown
!
interface Port-channel20
 description L3_LACP_TO_SW2
 ip address 10.0.20.2 255.255.255.252
 no shutdown
end
write memory
```

Verification 1 - Layer 2 LACP bundle

```
SW1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
10     Po10(SU)       LACP       Gi0/1(P) Gi0/2(P) Gi0/3(P)
```

What to verify

- Po10 shows S for Layer 2 and U for in use.
- All three physical members show P, meaning bundled in the Port-Channel.
- No member shows I (stand-alone) or s (suspended).

Verification 2 - LACP neighbor negotiation

```
SW1# show lacp neighbor
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs

Channel group 10 neighbors
Partner's information:
Port      System ID          Port Number  Age   Flags
Gi0/1     32768,0011.2233.4455  1        18s   SA
Gi0/2     32768,0011.2233.4455  2        18s   SA
Gi0/3     32768,0011.2233.4455  3        17s   SA
```

What to verify

- A partner entry exists for every member interface.
- The partner System ID is consistent across the members because they terminate on the same peer switch.

Verification 3 - Port-Channel trunk state

```
SW1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po10        on           802.1q         trunking      999

Port        Vlans allowed on trunk
Po10        10,20,150,999
```

What to verify

- The logical interface Po10, not the individual physical members, is the operational trunk shown for forwarding.
- Native and allowed VLAN settings match SW2.

Verification 4 - Layer 3 Port-Channel20

```
SW2# show ip interface brief | include Port-channel20
Port-channel20          10.0.20.1      YES manual up                    up

SW2# show etherchannel summary
Group  Port-channel  Protocol    Ports
20     Po20(RU)       LACP       Gi1/0/47(P) Gi1/0/48(P)

SW2# show ip route connected | include 10.0.20
C        10.0.20.0/30 is directly connected, Port-channel20
L        10.0.20.1/32 is directly connected, Port-channel20

SW2# ping 10.0.20.2
!!!!!
Success rate is 100 percent (5/5)
```

What to verify

- Po20 is up/up and shows R for Layer 3 and U for in use.
- Both routed members show P.
- 10.0.20.0/30 is installed as directly connected through Port-channel20.
- Ping to 10.0.20.2 succeeds.

Troubleshooting checks

- If a member is suspended, compare speed, duplex, switchport mode, VLAN/trunk attributes and channel-group settings on every member.
- LACP requires at least one side in active mode; passive/passive will not form an LACP bundle.

Supplementary Lab — PAgP EtherChannel

Training objective: Configure and verify a Cisco PAgP Layer 2 EtherChannel, compare desirable/auto behavior, and troubleshoot a bundle that does not form.

Exam-scope note: LACP is the standards-based EtherChannel protocol emphasized by current CCNA objectives. PAgP is Cisco-proprietary and is included here as additional operational knowledge.

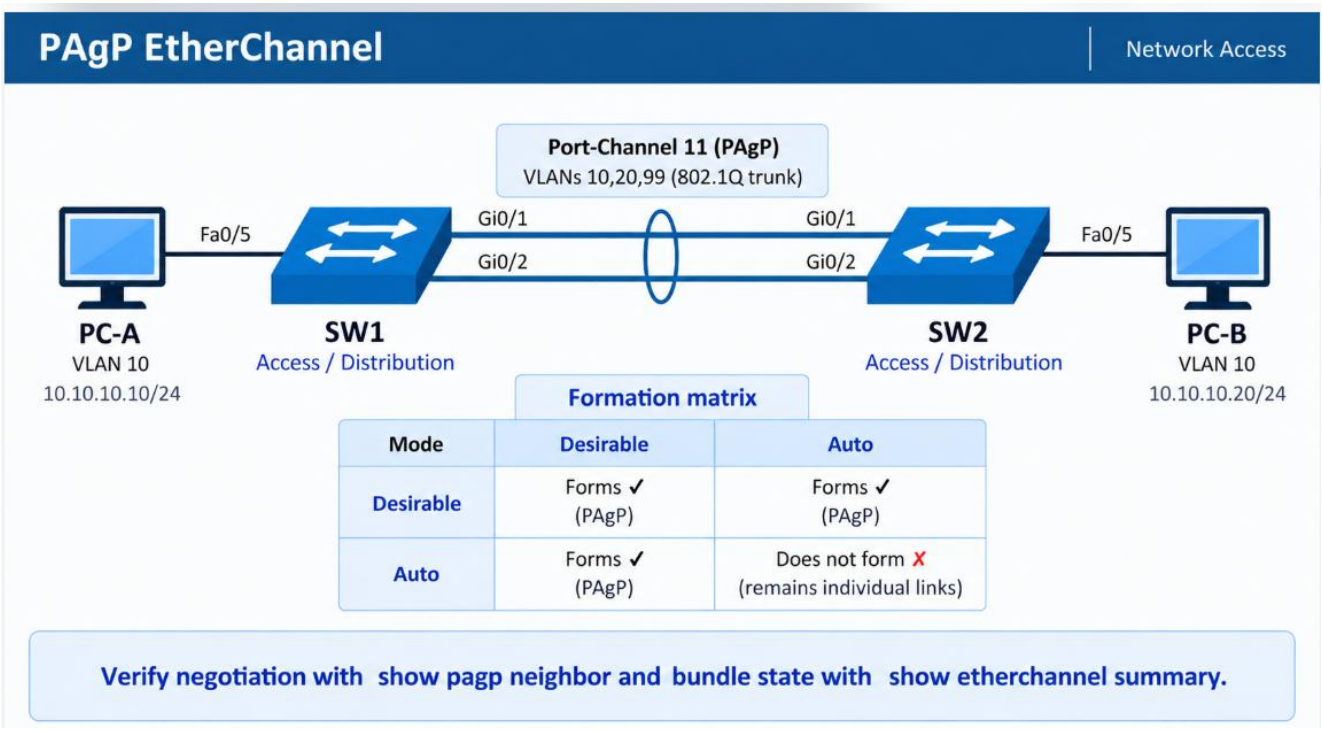


Figure: PAgP EtherChannel reference topology

Lab objectives

- Bundle two physical trunk links into Port-Channel11 using PAgP.
- Verify desirable/auto and desirable/desirable negotiation.
- Demonstrate why auto/auto does not initiate a PAgP bundle.
- Validate VLAN trunk consistency and member-interface state.
- Troubleshoot suspended or standalone members caused by configuration mismatch.

Addressing and VLAN plan

- VLAN 10 — USERS — PC-A 10.10.10.10/24 and PC-B 10.10.10.20/24.
- VLAN 20 — SERVERS — carried across the trunk for validation.
- VLAN 99 — MANAGEMENT / native VLAN in this lab.
- Port-Channel11 members — Gi0/1 and Gi0/2 on both switches.

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device configuration and verification

SW1 - PAgP desirable side

```
enable
configure terminal
hostname SW1
vlan 10
 name USERS
vlan 20
 name SERVERS
vlan 99
 name MANAGEMENT
!
interface FastEthernet0/10
 description PC-A_VLAN10
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 no shutdown
!
interface range GigabitEthernet0/1 - 2
 description PAGP_MEMBER_TO_SW2
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,99
 channel-group 11 mode desirable
 no shutdown
!
interface Port-channel11
 description PAGP_TRUNK_TO_SW2
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,99
 no shutdown
end
write memory
```

SW2 - PAgP auto side

```
enable
configure terminal
hostname SW2
vlan 10
 name USERS
vlan 20
 name SERVERS
vlan 99
 name MANAGEMENT
!
interface FastEthernet0/10
 description PC-B_VLAN10
 switchport mode access
```

```
 switchport access vlan 10
 spanning-tree portfast
 no shutdown
!
interface range GigabitEthernet0/1 - 2
 description PAGP_MEMBER_TO_SW1
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,99
 channel-group 11 mode auto
 no shutdown
!
interface Port-channel11
 description PAGP_TRUNK_TO_SW1
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,99
 no shutdown
end
write memory
```

PC addressing

- PC-A: 10.10.10.10/24 on SW1 Fa0/10.
- PC-B: 10.10.10.20/24 on SW2 Fa0/10.

Verification 1 - EtherChannel summary

```
SW1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        S - Layer2      U - in use

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
11     Po11(SU)       PAgP       Gi0/1(P) Gi0/2(P)
```

What to verify

- Po11 shows SU: Layer 2 and in use.
- Protocol is PAgP.
- Gi0/1 and Gi0/2 both show P, proving both links are bundled.

Verification 2 - PAgP neighbor

```
SW1# show pagp neighbor
Flags:  S - Device is sending Slow hello
        C - Device is in Consistent state

Channel group 11 neighbors
Partner              Partner             Partner
Port      Name        Device ID           Port
Gi0/1     SW2         0011.2233.4455      Gi0/1
Gi0/2     SW2         0011.2233.4455      Gi0/2
```

What to verify

- SW2 appears as the PAgP partner on both local member links.
- Both members negotiate with the same partner device.

Verification 3 - Port-Channel trunk

```
SW1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po11        on           802.1q         trunking      99

Port        Vlans allowed on trunk
Po11        10,20,99
```

What to verify

- Po11 is trunking and uses native VLAN 99.
- Allowed VLANs are 10,20,99 on both switches.

Verification 4 - Member interface state

```
SW1# show interfaces gi0/1 etherchannel
Port state    = Up Mstr In-Bndl
Channel group = 11          Mode = Desirable
Port-channel  = Po11        GC   = 0x00010001
Protocol      = PAgP
```

What to verify

- Port state includes In-Bndl.
- Channel group is 11 and protocol is PAgP.

Verification 5 - Data forwarding

```
PC-A> ping 10.10.10.20
Reply from 10.10.10.20: bytes=32 time<1ms TTL=128
Reply from 10.10.10.20: bytes=32 time<1ms TTL=128
```

What to verify

- The hosts in VLAN 10 communicate through Po11.
- After traffic, each switch should learn the remote PC MAC through Po11 rather than an individual member interface.

PAgP mode test - auto/auto expected failure

```
SW1(config)# interface range gi0/1 - 2
SW1(config-if-range)# no channel-group 11
SW1(config-if-range)# channel-group 11 mode auto

SW2(config)# interface range gi0/1 - 2
SW2(config-if-range)# no channel-group 11
SW2(config-if-range)# channel-group 11 mode auto

SW1# show etherchannel summary
Group  Port-channel  Protocol    Ports
11     Po11(SD)       PAgP       Gi0/1(I) Gi0/2(I)
```

What to verify

- Auto/auto does not actively initiate PAgP negotiation.
- The Port-Channel is not in use and members are not bundled. Exact flags can differ by platform.
- Restore SW1 to desirable and SW2 to auto after the test.

Part B — PAgP mode tests

1. Change SW2 member links from "**mode auto**" to "**mode desirable"**. Verify that desirable/desirable still forms the bundle.

2. Remove and recreate the channel using "**mode auto**" on both sides. Verify that auto/auto does not form because neither side actively initiates negotiation.

3. Restore SW1 to desirable and SW2 to auto before continuing.

Troubleshooting drills

1. On SW2 Gi0/2, configure a different allowed-VLAN list. Observe whether the member is suspended or fails bundle consistency checks. Restore the matching list.

2. Change one member to access mode while the other remains a trunk. Verify the EtherChannel failure and identify the incompatible parameter.

3. Place only one physical member into channel-group 11. Compare the EtherChannel summary before and after adding the second member.

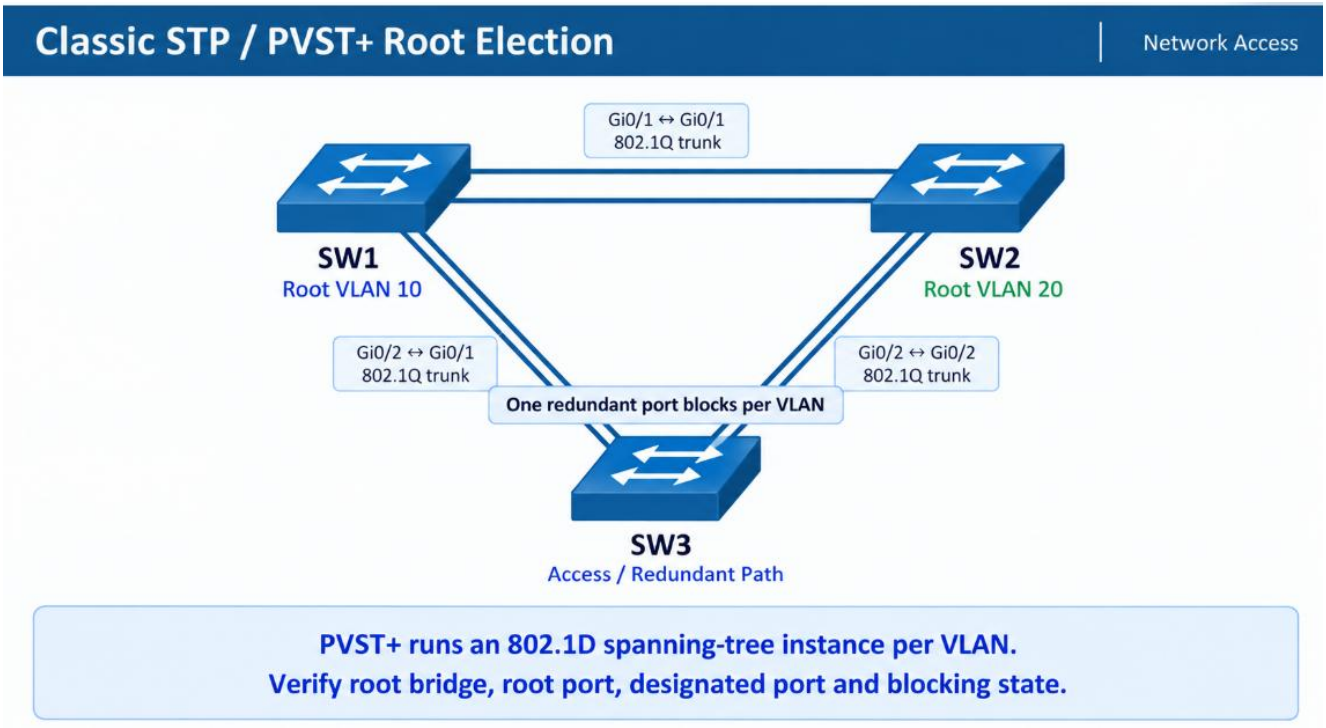
4. Use "**show pagp neighbor**", "**show etherchannel summary"**, and interface configuration side-by-side to identify the root cause before changing configuration.

PAgP quick reference

- **desirable** — actively sends PAgP negotiation messages and attempts to form the channel.
- **auto** — listens for PAgP and forms when the peer is desirable; auto/auto does not form.
- **on** — forces a static EtherChannel and does not use PAgP negotiation; both sides must be configured consistently.
- All member links must match key Layer 2 attributes such as trunk/access mode, native VLAN, allowed VLAN list, speed and duplex where applicable.

Supplementary Lab — Classic STP / PVST+ Root Election and Port Roles

Training objective: Build a three-switch redundant Layer 2 topology, control the root bridge independently per VLAN, identify STP port roles/states, and observe classic 802.1D convergence behavior.



Supplementary Figure: Classic STP / PVST+ root-election reference topology

Lab objectives

- Run PVST+ so VLAN 10 and VLAN 20 have independent spanning-tree instances.
- Make SW1 the root bridge for VLAN 10 and SW2 the root bridge for VLAN 20.
- Identify root ports, designated ports and the redundant blocking port for each VLAN.
- Review classic STP port states: Blocking, Listening, Learning and Forwarding.
- Manipulate path cost and bridge priority to observe deterministic path selection and reconvergence.

What STP is deciding

- **Root bridge** — the switch with the lowest Bridge ID for that VLAN. Bridge ID is based on STP priority plus the VLAN system ID extension and MAC address.
- **Root port** — the non-root switch port with the lowest total path cost toward the root bridge.
- Designated port — the forwarding port selected for a LAN segment based on the superior BPDU for that segment.
- **Blocking port** — a classic STP non-forwarding redundant port that prevents a Layer 2 loop.
- Classic STP convergence uses Blocking → Listening → Learning → Forwarding when a port transitions toward forwarding; timers make this slower than Rapid PVST+.

- **Execution sequence**: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device configuration and verification

SW1 - VLAN 10 root primary / VLAN 20 root secondary

```
enable
configure terminal
hostname SW1
spanning-tree mode pvst
vlan 10
 name USERS
vlan 20
 name OPERATIONS
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW2_GI0_1
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
!
interface GigabitEthernet0/2
 description TRUNK_TO_SW3_GI0_1
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
!
spanning-tree vlan 10 root primary
spanning-tree vlan 20 root secondary
end
write memory
```

SW2 - VLAN 20 root primary / VLAN 10 root secondary

```
enable
configure terminal
hostname SW2
spanning-tree mode pvst
vlan 10
 name USERS
vlan 20
 name OPERATIONS
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW1_GI0_1
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
!
interface GigabitEthernet0/2
 description TRUNK_TO_SW3_GI0_2
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
!
```

```
spanning-tree vlan 20 root primary
spanning-tree vlan 10 root secondary
end
write memory
```

SW3 - Redundant access switch

```
enable
configure terminal
hostname SW3
spanning-tree mode pvst
vlan 10
 name USERS
vlan 20
 name OPERATIONS
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW1_GI0_2
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
!
interface GigabitEthernet0/2
 description TRUNK_TO_SW2_GI0_2
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
end
write memory
```

Verification 1 - VLAN 10 on SW1

```
SW1# show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0010.1111.1111
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0010.1111.1111

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1               Desg FWD 4         128.1    P2p
Gi0/2               Desg FWD 4         128.2    P2p
```

What to verify

- SW1 displays This bridge is the root for VLAN 10.
- The bridge priority reflects root-primary priority plus VLAN 10 system ID extension.
- Both SW1 trunk ports are designated and forwarding because SW1 is the root bridge.

Verification 2 - VLAN 10 on SW3

```
SW3# show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0010.1111.1111
             Cost        4
             Port        1 (GigabitEthernet0/1)

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1               Root FWD 4         128.1    P2p
Gi0/2               Altn BLK 4         128.2    P2p
```

What to verify

- SW3 Gi0/1 is the root port toward SW1 for VLAN 10.
- SW3 Gi0/2 is alternate/blocking for VLAN 10, preventing the Layer 2 loop.

Verification 3 - VLAN 20 on SW2 and SW3

```
SW2# show spanning-tree vlan 20
VLAN0020
  Root ID    Priority    24596
             Address     0020.2222.2222
             This bridge is the root

SW3# show spanning-tree vlan 20
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1               Altn BLK 4         128.1    P2p
Gi0/2               Root FWD 4         128.2    P2p
```

What to verify

- SW2 is root for VLAN 20.
- SW3 uses Gi0/2 as its VLAN 20 root port and blocks the redundant Gi0/1 path for VLAN 20.
- The same physical link can have different roles in different PVST+ VLAN instances.

Verification 4 - STP timers

```
SW1# show spanning-tree vlan 10 detail | include hello|forward|aging
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
```

What to verify

- Classic STP default timers are Hello 2 seconds, Max Age 20 seconds and Forward Delay 15 seconds.

Verification 5 - Path-cost manipulation

```
SW3(config)# interface gi0/1
SW3(config-if)# spanning-tree vlan 10 cost 100

SW3# show spanning-tree vlan 10
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1               Altn BLK 100       128.1    P2p
Gi0/2               Root FWD 4         128.2    P2p
```

What to verify

- Increasing the VLAN 10 cost on the previous root path makes the alternate path more attractive.
- After the observation, remove the manual cost with no spanning-tree vlan 10 cost.

Failure and reconvergence drills

1. Record the current VLAN 10 root port and blocked port on SW3.

2. Shut the current root-port link on SW3. Observe which redundant port moves through the classic STP states toward forwarding.

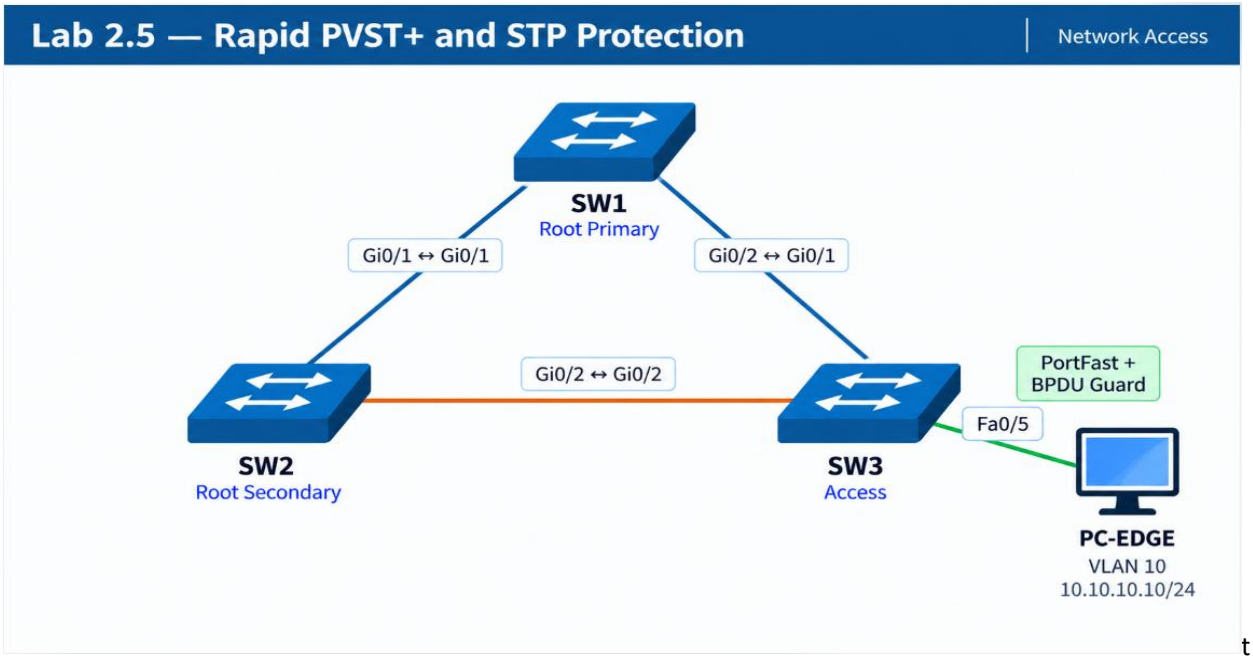
3. Restore the link and verify the original topology stabilizes again.

4. Temporarily lower SW3 bridge priority for VLAN 10 and observe a new root election. Restore SW1 as root primary after the test.

5. Compare the convergence behavior and port-state terminology here with the following Rapid PVST+ lab.

Lab 2.5 — Rapid PVST+ and STP Protection

CCNA objective: Interpret basic operations of Rapid PVST+: root port, root bridge primary/secondary, port roles/states, PortFast, Root Guard, Loop Guard, BPDU Filter and BPDU Guard.



t

Figure 2.5: Rapid PVST+ and STP Protection reference topology

Lab objectives

- Elect SW1 as root primary and SW2 as root secondary for VLANs 10 and 20.
- Identify root, designated and alternate ports.
- Observe forwarding/discarding behavior under Rapid PVST+.
- Protect edge and topology-facing interfaces using the v1.1 protection features.

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device configuration and verification

SW1 - Root primary and topology protection

```
enable
configure terminal
hostname SW1
spanning-tree mode rapid-pvst
vlan 10
 name USERS
vlan 20
 name OPERATIONS
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW2_GI0_1
 switchport mode trunk
```

```
 switchport trunk allowed vlan 10,20
 no shutdown
!
interface GigabitEthernet0/2
 description TRUNK_TO_SW3_GI0_1
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 spanning-tree guard root
 no shutdown
!
spanning-tree vlan 10,20 root primary
spanning-tree loopguard default
end
write memory
```

SW2 - Root secondary

```
enable
configure terminal
hostname SW2
spanning-tree mode rapid-pvst
vlan 10
 name USERS
vlan 20
 name OPERATIONS
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW1_GI0_1
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
!
interface GigabitEthernet0/2
 description TRUNK_TO_SW3_GI0_2
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
!
spanning-tree vlan 10,20 root secondary
spanning-tree loopguard default
end
write memory
```

SW3 - Redundant access switch and edge protections

```
enable
configure terminal
hostname SW3
spanning-tree mode rapid-pvst
vlan 10
 name USERS
vlan 20
 name OPERATIONS
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW1_GI0_2
 switchport mode trunk
```

```
 switchport trunk allowed vlan 10,20
 no shutdown
!
interface GigabitEthernet0/2
 description TRUNK_TO_SW2_GI0_2
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown
!
interface FastEthernet0/5
 description PC_EDGE_VLAN10
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/6
 description INSTRUCTOR_BPDU_FILTER_TEST_ONLY
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpdufilter enable
 shutdown
!
spanning-tree loopguard default
end
write memory
```

Keep Fa0/6 shut until the instructor-controlled BPDU Filter demonstration. BPDU Filter can create loops when misused.

Verification 1 - Root and rapid port roles

```
SW1# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0010.1111.1111
             This bridge is the root

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1               Desg FWD 4         128.1    P2p
Gi0/2               Desg FWD 4         128.2    P2p

SW3# show spanning-tree vlan 10
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1               Root FWD 4         128.1    P2p
Gi0/2               Altn DSC 4         128.2    P2p
Fa0/5               Desg FWD 19        128.5    P2p Edge
```

What to verify

- Protocol is rstp.
- SW1 is root for VLAN 10 and VLAN 20.
- SW3 has one Root FWD port and one Altn DSC port on the redundant uplinks.
- Fa0/5 is shown as an edge/PortFast forwarding port.

Verification 2 - PortFast and BPDU Guard

```
SW3# show spanning-tree interface fa0/5 detail
 Port 5 (FastEthernet0/5) of VLAN0010 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.5.
   The port is in the portfast mode
   Bpdu guard is enabled

SW3# show running-config interface fa0/5
interface FastEthernet0/5
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
```

What to verify

- PortFast is active on the end-host port.
- BPDU Guard is enabled on the same edge port.

Verification 3 - Root Guard

```
SW1# show spanning-tree inconsistentports

Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
VLAN0010             GigabitEthernet0/2     Root Inconsistent

Number of inconsistent ports (segments) in the system : 1
```

What to verify

- This output is expected only during the controlled test when SW3 sends a superior BPDU toward root-guarded SW1 Gi0/2.
- When the superior BPDU condition is removed, the interface should automatically leave root-inconsistent state.

Verification 4 - Loop Guard default

```
SW1# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0010, VLAN0020
EtherChannel misconfig guard            is enabled
Extended system ID                      is enabled
Portfast Default                        is disabled
PortFast BPDU Guard Default             is disabled
PortFast BPDU Filter Default            is disabled
Loopguard Default                       is enabled
```

What to verify

- Switch is in rapid-pvst mode.
- Loopguard Default is enabled.

Failure drills

1. Shut the current root-port link on SW3 and observe reconvergence to the alternate path.

2. Connect a test switch to the BPDU Guard port and observe the protection action. Recover only after confirming the cause.

3. Temporarily alter STP priority on SW3 to try to become root and verify Root Guard behavior on the protected interface.

Lab 2.6 — Cisco Wireless Architectures and AP Modes

CCNA objective: Describe Cisco wireless architectures and AP modes.

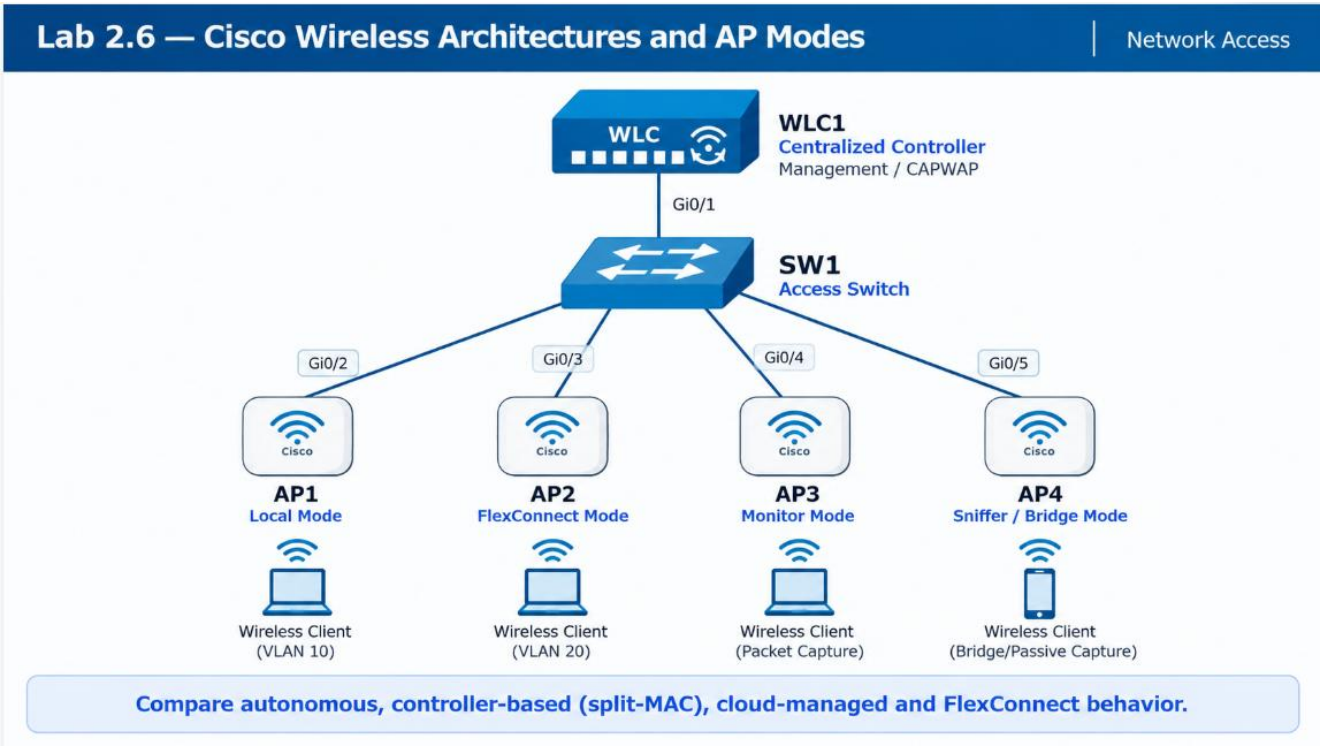


Figure 2.6: Cisco Wireless Architectures and AP Modes reference topology

Lab objectives

- Compare autonomous, controller-based/split-MAC, cloud-managed and remote-site FlexConnect designs.
- Identify practical AP modes and the traffic/operations role of each mode.
- Observe AP-to-WLC management/CAPWAP relationships where the lab platform supports them.

Architecture comparison exercise

- Autonomous AP: configuration and forwarding decisions are largely local to the AP. Suitable for small standalone deployments, but management does not scale as cleanly.
- Controller-based / split-MAC: APs handle time-sensitive radio functions while a WLC centralizes control, policy and WLAN configuration.
- Cloud-managed: management/control is delivered through a cloud service while local data forwarding behavior depends on platform/design.
- FlexConnect: designed for remote sites; an AP is still controller-managed but can locally switch selected WLAN traffic at the branch.Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device observation and verification

This lesson is primarily an interpretation lab rather than a full WLAN deployment lab. AP mode configuration syntax varies by controller platform and software release, so the CCNA task is to identify the architecture and verify the resulting AP state.

WLC1 - Catalyst 9800 verification example

```
WLC1# show ap summary
Number of APs: 4

AP Name   Slots  AP Model        Ethernet MAC   Radio MAC      Location   Country  IP
Address       State
AP1       2      C9xxx           xxxx.xxxx.0001 xxxx.xxxx.1001 default    IN
10.100.100.11   Registered
AP2       2      C9xxx           xxxx.xxxx.0002 xxxx.xxxx.1002 branch     IN
10.100.100.12   Registered
AP3       2      C9xxx           xxxx.xxxx.0003 xxxx.xxxx.1003 default    IN
10.100.100.13   Registered
AP4       2      C9xxx           xxxx.xxxx.0004 xxxx.xxxx.1004 default    IN
10.100.100.14   Registered

WLC1# show wireless stats ap join summary
Number of APs joined : 4
Number of APs not joined : 0
```

What to verify

- All expected APs appear in the controller AP database.
- Each AP is in Registered/joined state before interpreting the configured AP mode.
- The AP management IPs are in the expected management network.

Per-AP inspection example

```
WLC1# show ap name AP1 config general
AP Name                      : AP1
Administrative State         : Enabled
AP Mode                      : Local
AP IPv4 Address              : 10.100.100.11
CAPWAP State                 : Joined

WLC1# show ap name AP2 config general
AP Name                      : AP2
Administrative State         : Enabled
AP Mode                      : FlexConnect
AP IPv4 Address              : 10.100.100.12
CAPWAP State                 : Joined
```

What to verify

- AP1 is in Local mode for normal controller-based client service.
- AP2 is in FlexConnect mode for remote-site operation.
- For AP3/AP4, verify the configured monitoring/sniffer/bridge role supported by the actual lab platform.

Lab 2.7 — WLAN Physical Infrastructure — AP, WLC, Access/Trunk and LAG

CCNA objective: Describe physical infrastructure connections of WLAN components: AP, WLC, access/trunk ports and LAG.

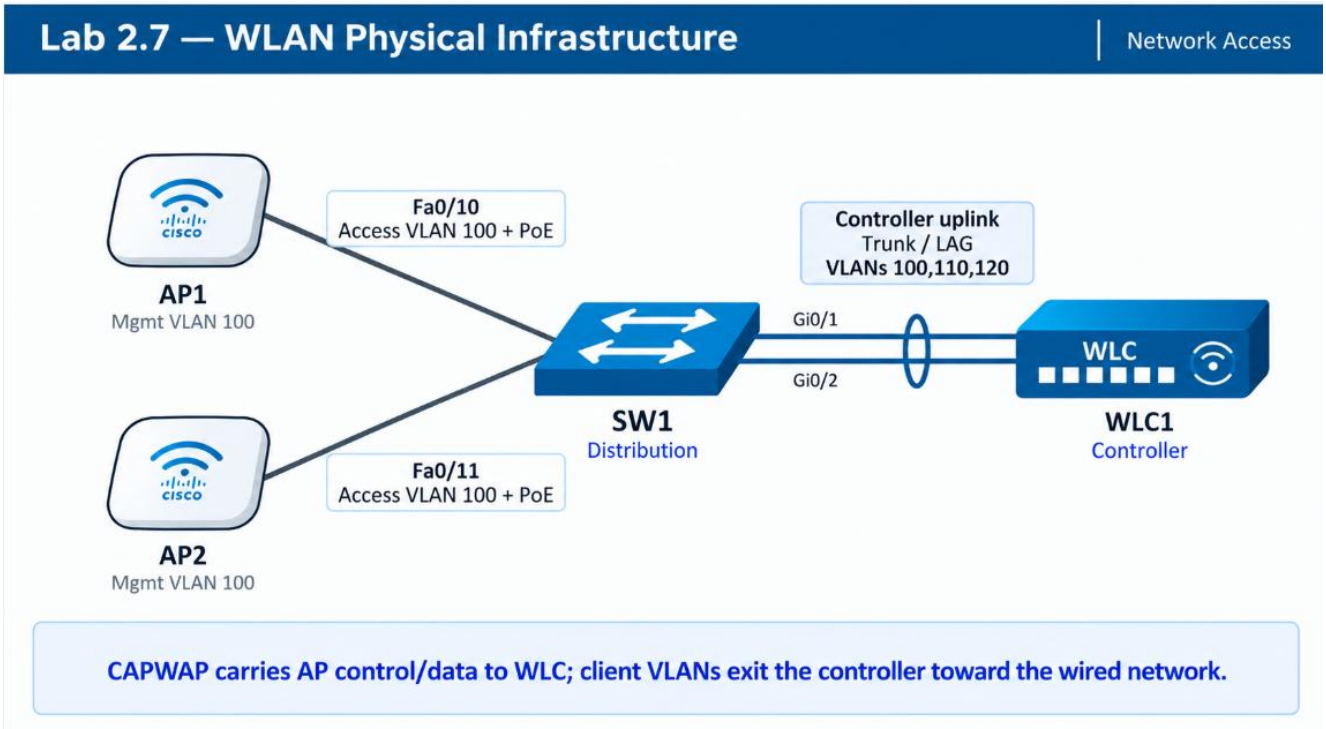


Figure 2.7: WLAN Physical Infrastructure — AP, WLC, Access/Trunk and LAG reference topology

Lab objectives

- Connect lightweight APs to PoE access ports in an AP management VLAN.
- Connect the controller toward the switching infrastructure using a trunk or link aggregation design.
- Map management and client VLANs through the wired network.
- Verify switch-side state before troubleshooting wireless association.

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device configuration and verification

SW1 - AP access ports and WLC trunk

```
enable
configure terminal
hostname SW1
vlan 100
 name AP-MGMT
vlan 110
```

```
 name WLAN-STAFF
vlan 120
 name WLAN-GUEST
!
interface FastEthernet0/10
 description AP1_MGMT_VLAN100_POE
 switchport mode access
 switchport access vlan 100
 spanning-tree portfast
 power inline auto
 no shutdown
!
interface FastEthernet0/11
 description AP2_MGMT_VLAN100_POE
 switchport mode access
 switchport access vlan 100
 spanning-tree portfast
 power inline auto
 no shutdown
!
interface GigabitEthernet0/24
 description WLC1_UPLINK
 switchport mode trunk
 switchport trunk allowed vlan 100,110,120
 no shutdown
end
write memory
```

AP1 / AP2 - Management requirements

- AP1 and AP2 obtain or use management addresses in VLAN 100.
- Each AP must have a valid default gateway and IP reachability to WLC1 for CAPWAP discovery/join.
- No access VLAN 110 or 120 is configured on the AP switchports in this centralized-controller example; client VLANs are carried on the controller-side trunk.

WLC1 - Controller-side expectations

- WLC management is reachable through VLAN 100.
- The controller uplink carries VLANs 100, 110 and 120 toward SW1.
- If using a controller LAG/Port-Channel design, configure the exact controller platform according to its guide and make all switch member interfaces consistent before bundling.

Verification 1 - PoE and interface status

```
SW1# show power inline
Module   Available     Used     Remaining
         (Watts)      (Watts)    (Watts)
------   ---------   --------   ---------
1          370.0        31.0       339.0

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/10    auto   on         15.5    Ieee PD             4     30.0
Fa0/11    auto   on         15.5    Ieee PD             4     30.0
```

```
SW1# show interfaces status
Port      Name               Status       Vlan       Duplex Speed Type
Fa0/10    AP1_MGMT_VLAN100   connected    100        a-full a-100 10/100BaseTX
Fa0/11    AP2_MGMT_VLAN100   connected    100        a-full a-100 10/100BaseTX
Gi0/24    WLC1_UPLINK        connected    trunk      a-full a-1000 10/100/1000BaseTX
```

What to verify

- AP ports are connected and receiving PoE where supported.
- Fa0/10 and Fa0/11 are access VLAN 100.
- The WLC uplink is physically up.

Verification 2 - WLC trunk

```
SW1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gi0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/24      100,110,120

Port        Vlans allowed and active in management domain
Gi0/24      100,110,120
```

What to verify

- Gi0/24 is trunking.
- VLANs 100, 110 and 120 are all allowed and active.

Verification 3 - AP MAC learning

```
SW1# show mac address-table dynamic vlan 100
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
100     00aa.bbcc.0010    DYNAMIC     Fa0/10
100     00aa.bbcc.0011    DYNAMIC     Fa0/11
100     00aa.bbcc.1000    DYNAMIC     Gi0/24
```

What to verify

- AP MAC addresses are learned on the correct access ports in VLAN 100.
- The controller-side VLAN 100 MAC is learned through the WLC trunk.

Verification 4 - Controller sees APs

```
WLC1# show ap summary
AP Name   AP Model   IP Address       State
AP1       C9xxx      10.100.100.11   Registered
AP2       C9xxx      10.100.100.12   Registered
```

What to verify

- Both APs are registered/joined to WLC1.
- If an AP has power but is not joined, troubleshoot VLAN 100 addressing/routing and CAPWAP reachability before investigating WLAN policy.

Lab 2.8 — Network Device Management Access

CCNA objective: Describe network device management access: Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS and cloud managed.

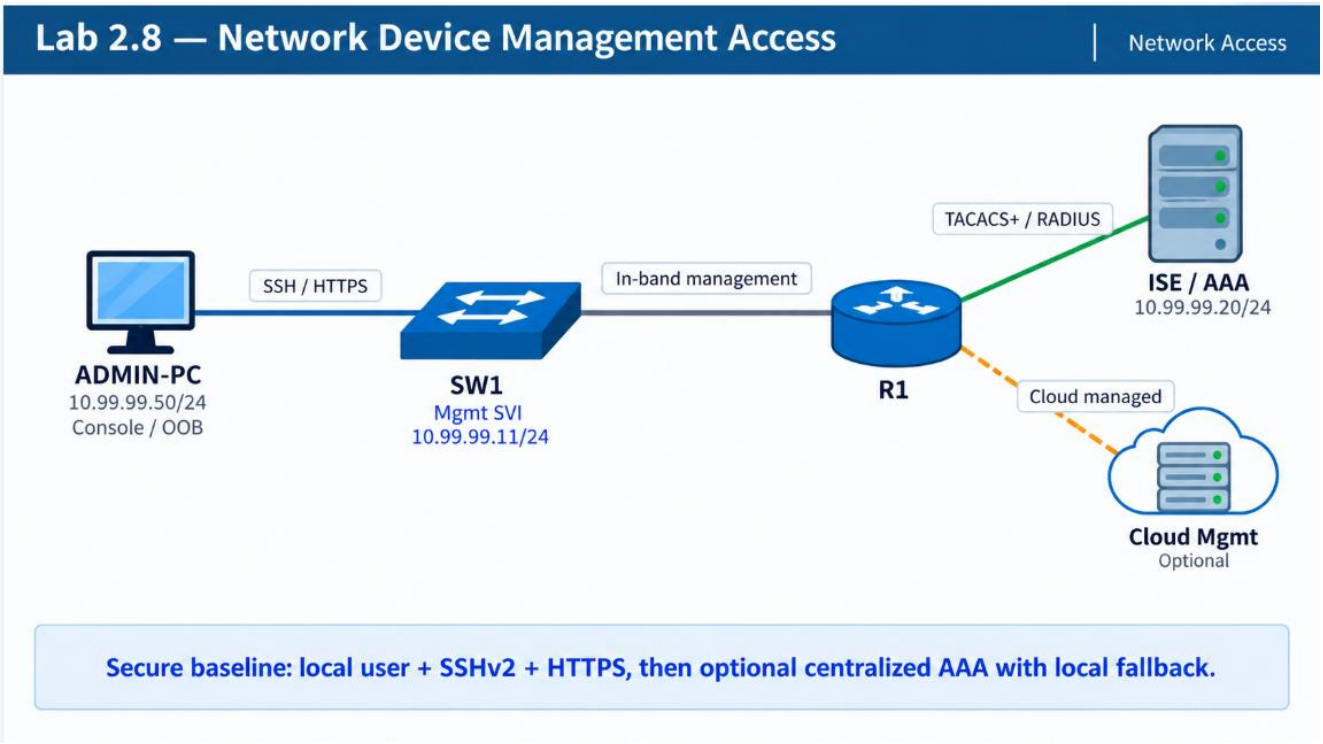


Figure 2.8: Network Device Management Access reference topology

Lab objectives

- Configure a management SVI/default gateway on a Layer 2 switch.
- Secure remote CLI access with SSHv2 and a local user.
- Enable HTTPS and disable the plaintext HTTP server.
- Compare console/OOB, Telnet, SSH, HTTPS, centralized AAA and cloud-managed access.
- Add centralized AAA syntax with local fallback for an advanced lab.

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — device-by-device configuration and verification

R1 - Management VLAN default gateway

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 description MGMT_VLAN99_GATEWAY_TO_SW1
 ip address 10.99.99.1 255.255.255.0
 no shutdown
end
write memory
```

SW1 - VLAN 99, SSHv2, HTTPS and TACACS+ with local fallback

```
enable
configure terminal
hostname SW1
vlan 99
 name MANAGEMENT
!
interface Vlan99
 description MANAGEMENT_SVI
 ip address 10.99.99.11 255.255.255.0
 no shutdown
!
interface FastEthernet0/5
 description ADMIN_PC
 switchport mode access
 switchport access vlan 99
 spanning-tree portfast
 no shutdown
!
interface GigabitEthernet0/1
 description MGMT_UPLINK_TO_R1
 switchport mode access
 switchport access vlan 99
 no shutdown
!
ip default-gateway 10.99.99.1
ip domain-name nga.lab
username admin privilege 15 secret Str0ng-Lab-Only!
crypto key generate rsa modulus 2048
ip ssh version 2
!
no ip http server
ip http secure-server
!
aaa new-model
tacacs server ISE1
 address ipv4 10.99.99.20
 key LabSharedKey!
!
aaa group server tacacs+ TAC-GRP
 server name ISE1
!
aaa authentication login VTY_AUTH group TAC-GRP local
!
line vty 0 4
 login authentication VTY_AUTH
 transport input ssh
 exec-timeout 10 0
end
write memory
```

ADMIN-PC and AAA server addressing

- ADMIN-PC: 10.99.99.50/24, default gateway 10.99.99.1.
- ISE/AAA server: 10.99.99.20/24, default gateway 10.99.99.1; configure a matching TACACS+ network-device entry and shared key LabSharedKey! on the server.

Verification 1 - Management SVI and gateway reachability

```
SW1# show ip interface brief | include Vlan99
Vlan99                 10.99.99.11    YES manual up                    up

SW1# ping 10.99.99.1
!!!!!
Success rate is 100 percent (5/5)

SW1# ping 10.99.99.20
!!!!!
Success rate is 100 percent (5/5)
```

What to verify

- Vlan99 is up/up. On a Layer 2 switch, the SVI will not come up unless VLAN 99 exists and at least one Layer 2 port in VLAN 99 is operational.
- SW1 can reach both the default gateway and AAA server before AAA testing.

Verification 2 - SSHv2

```
SW1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SW1.nga.lab

ADMIN-PC> ssh -l admin 10.99.99.11
Password:
SW1> enable
SW1#
```

What to verify

- SSH is enabled and reports version 2.0.
- The admin session reaches SW1 over 10.99.99.11 and authenticates successfully.
- Telnet should not be accepted because VTY transport input is restricted to ssh.

Verification 3 - HTTPS status

```
SW1# show ip http server status
HTTP server status: Disabled
HTTP server port: 80
HTTP server active supplementary listener ports: 0
HTTP secure server status: Enabled
HTTP secure server port: 443
```

What to verify

- Plain HTTP is disabled.
- HTTPS is enabled on TCP/443.

Verification 4 - AAA/TACACS configuration

```
SW1# show running-config | section aaa
 aaa new-model
 aaa authentication login VTY_AUTH group TAC-GRP local

SW1# show running-config | section tacacs
 tacacs server ISE1
  address ipv4 10.99.99.20
  key 7 <encrypted-or-obscured-value>
 aaa group server tacacs+ TAC-GRP
  server name ISE1
```

What to verify

- The VTY authentication method list tries TAC-GRP first and local second.
- The TACACS+ server IP is 10.99.99.20 and the server is a member of TAC-GRP.
- Test local fallback only in a controlled lab by making the TACACS+ service unavailable, then confirming the local admin account still permits SSH login.

Access-method interpretation

- **Console**: local out-of-band access; does not require working IP connectivity.
- **Telnet**: plaintext remote CLI; know it for the exam but prefer SSH in real deployments.
- **SSH**: encrypted remote CLI; standard secure management choice.
- **HTTP/HTTPS**: browser-based WebUI; HTTPS protects the session in transit.
- **TACACS+/RADIUS**: centralized AAA services. TACACS+ is commonly used for administrative device access and RADIUS is widely used for network access and can also support device administration.
- **Cloud managed:** devices are monitored/configured through a cloud management plane depending on product architecture.

Lab 2.9 — Wireless LAN GUI Interpretation

CCNA objective: Interpret wireless LAN GUI configuration for client connectivity: WLAN creation, security settings, QoS profiles and advanced settings.

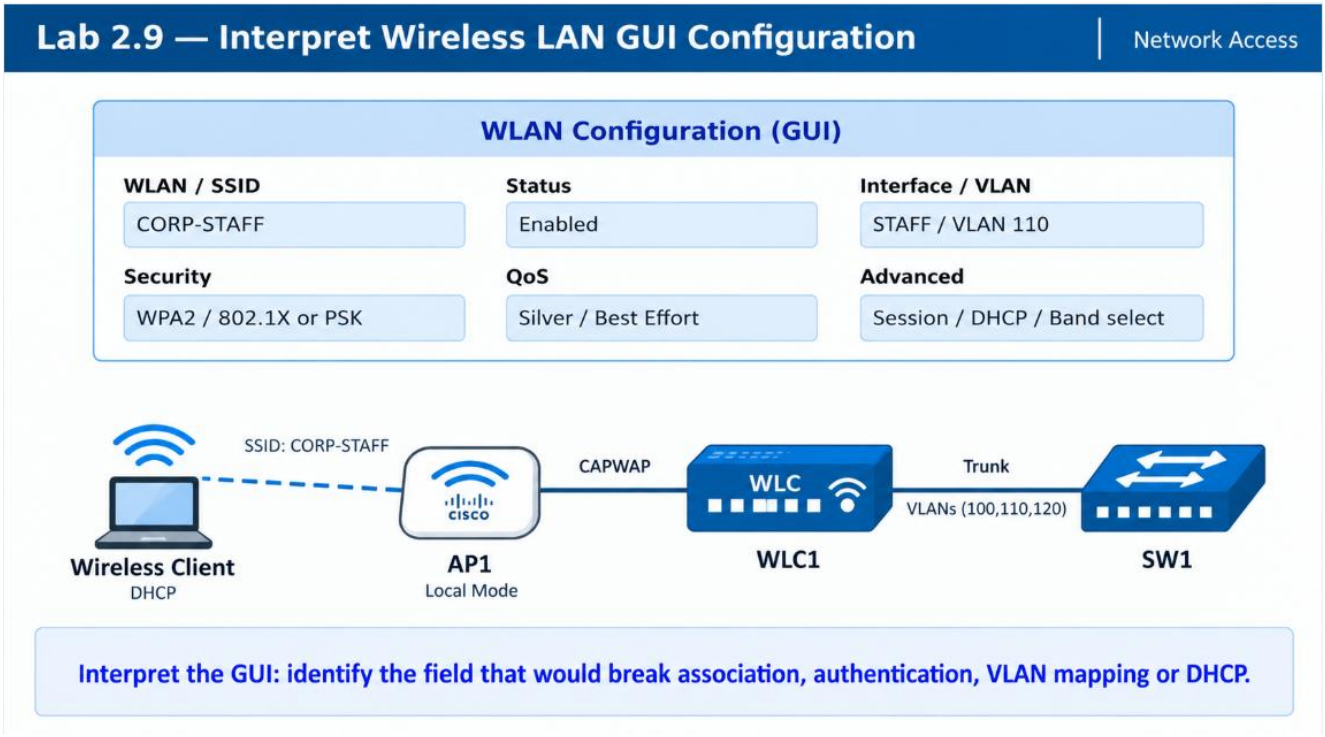


Figure 2.9: Wireless LAN GUI Interpretation reference topology

Lab objectives

- Interpret a WLAN profile rather than relying on memorized click paths.
- Identify which GUI field maps the SSID to the client VLAN/policy.
- Identify security and QoS fields that directly affect client access.
- Use client/AP status to distinguish RF/association, authentication, VLAN and DHCP failures.

GUI field inspection checklist

1. Find the WLAN/SSID name and confirm the WLAN is enabled.

2. Identify the interface, policy profile or VLAN that carries client traffic.

3. Check Layer 2 security: open/WPA2/WPA3, PSK or 802.1X as applicable.

4. Check AAA server selection when enterprise authentication is used.

5. Read the QoS profile/policy and determine the intended traffic treatment.

6. Check advanced options such as session timeout, client exclusion, DHCP requirements, peer-to-peer blocking or band-selection settings.

7. Open client monitoring and note association state, AP, WLAN, IP address, VLAN/policy and signal information.

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — controller/client verification and interpretation

The CCNA objective is to interpret WLAN configuration presented in a GUI. Use controller CLI output as a second view of the same fields so you can prove the GUI setting is actually active.

WLC1 - WLAN summary

```
WLC1# show wlan summary
Number of WLANs: 1

WLAN ID  WLAN Profile Name / SSID          Status  Interface / Policy
-------  --------------------------------  ------  ------------------
10       CORP-STAFF / CORP-STAFF           Enabled STAFF / VLAN 110
```

What to verify

- The CORP-STAFF WLAN is enabled.
- The WLAN maps to the intended policy/interface for VLAN 110.

WLC1 - WLAN detail

```
WLC1# show wlan name CORP-STAFF
WLAN Profile Name     : CORP-STAFF
SSID                  : CORP-STAFF
Status                : Enabled
Security              : WPA2 / 802.1X or PSK
Policy / VLAN         : STAFF / 110
QoS                   : Silver / Best Effort
```

What to verify

- SSID name and enabled status match the GUI.
- Security method matches the design; a client can associate but fail authentication when this field is wrong.
- VLAN/policy mapping is 110; an incorrect mapping commonly causes DHCP or reachability failures after successful association.

Wireless client verification example

```
WLC1# show wireless client summary
Number of Clients: 1

MAC Address      AP Name  WLAN  State        IPv4 Address     VLAN
0011.2233.4455   AP1      10    Run          10.110.110.51    110
```

What to verify

- Client state is Run/connected.
- The client is associated to the expected AP and WLAN.
- The client receives an address from the VLAN 110 subnet.

Interpretation scenarios

Symptom	Most likely GUI area to inspect first
SSID not visible	WLAN status, AP/tag assignment, radio policy
Client associates but fails authentication	Security / AAA settings
Client authenticates but gets no IP	VLAN/policy mapping, DHCP reachability
Voice client receives poor service	QoS profile/policy mapping
Only one AP fails to advertise WLAN	AP policy/tag/group or AP operational state

CCNA focus: Objective 2.9 uses the verb “interpret.” The key skill is reading the relationship among WLAN/SSID, security, QoS, advanced settings and the client VLAN/policy—not memorizing one controller software version’s exact menus.

Lab CAPSTONE — Integrated Campus Access Lab

CCNA objective: Integrates Module 2 switching, STP, LACP, management access and WLAN infrastructure.

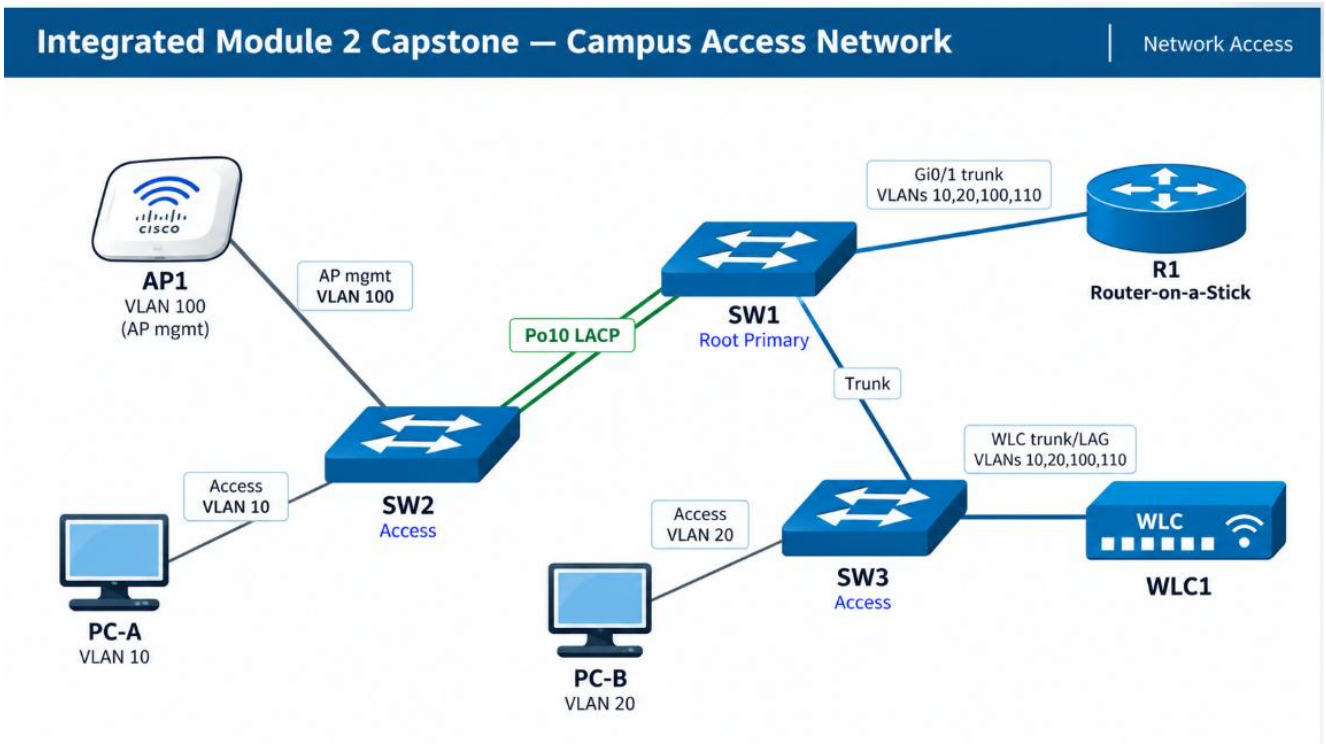


Figure CAPSTONE: Integrated Campus Access Lab reference topology

Scenario

You are building a small enterprise campus. SW1 is the distribution/root switch. SW2 and SW3 are access switches. SW1-to-SW2 uses LACP Port-Channel10. SW1-to-SW3 is an 802.1Q trunk. R1 provides router-on-a-stick inter-VLAN routing. AP1 uses management VLAN 100 and WLC1 carries WLAN client VLAN 110. Secure device management uses VLAN 99 and SSH.

Required VLANs and gateways

VLAN	Name	Gateway
10	USERS	10.10.10.1/24
20	OPERATIONS	10.20.20.1/24
99	MGMT	10.99.99.1/24
100	AP-MGMT	10.100.100.1/24
110	WLAN-STAFF	10.110.110.1/24
999	NATIVE-BLACKHOLE	No user gateway

Execution sequence: configure each device once, then verify the resulting state using the sample output and What to verify criteria.

Lab execution — complete device-by-device configuration

The interface assignments below make the existing capstone topology deterministic: SW1 Gi0/1 to R1 Gi0/0, SW1 Fa0/23-24 to SW2 Fa0/23-24 as Po10, SW1 Gi0/2 to SW3 Gi0/1, PC-A on SW2 Fa0/10, AP1 on SW2 Fa0/11, PC-B on SW3 Fa0/10, and WLC1 on SW3 Gi0/24.

SW1 - Distribution/root switch

```
enable
configure terminal
hostname SW1
spanning-tree mode rapid-pvst
!
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 99
 name MGMT
vlan 100
 name AP-MGMT
vlan 110
 name WLAN-STAFF
vlan 999
 name NATIVE-BLACKHOLE
!
interface GigabitEthernet0/1
 description TRUNK_TO_R1_GI0_0
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,99,100,110,999
 no shutdown
!
interface range FastEthernet0/23 - 24
 description LACP_MEMBER_TO_SW2
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,99,100,110,999
 channel-group 10 mode active
 no shutdown
!
interface Port-channel10
 description LACP_TRUNK_TO_SW2
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,99,100,110,999
 no shutdown
!
interface GigabitEthernet0/2
 description TRUNK_TO_SW3_GI0_1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,99,100,110,999
 no shutdown
!
spanning-tree vlan 10,20,99,100,110 root primary
!
interface Vlan99
 description MANAGEMENT_SVI
 ip address 10.99.99.11 255.255.255.0
 no shutdown
ip default-gateway 10.99.99.1
```

```
!
ip domain-name nga.lab
username admin privilege 15 secret Str0ng-Lab-Only!
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0
end
write memory
```

SW2 - Access switch with PC-A and AP1

```
enable
configure terminal
hostname SW2
spanning-tree mode rapid-pvst
!
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 99
 name MGMT
vlan 100
 name AP-MGMT
vlan 110
 name WLAN-STAFF
vlan 999
 name NATIVE-BLACKHOLE
!
interface range FastEthernet0/23 - 24
 description LACP_MEMBER_TO_SW1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,99,100,110,999
 channel-group 10 mode passive
 no shutdown
!
interface Port-channel10
 description LACP_TRUNK_TO_SW1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,99,100,110,999
 no shutdown
!
interface FastEthernet0/10
 description PC-A_VLAN10
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable
 no shutdown
!
interface FastEthernet0/11
```

```
 description AP1_MGMT_VLAN100
 switchport mode access
 switchport access vlan 100
 spanning-tree portfast
 spanning-tree bpduguard enable
 power inline auto
 no shutdown
!
spanning-tree vlan 10,20,99,100,110 root secondary
!
interface Vlan99
 description MANAGEMENT_SVI
 ip address 10.99.99.12 255.255.255.0
 no shutdown
ip default-gateway 10.99.99.1
!
ip domain-name nga.lab
username admin privilege 15 secret Str0ng-Lab-Only!
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
end
write memory
```

SW3 - Access switch with PC-B and WLC1

```
enable
configure terminal
hostname SW3
spanning-tree mode rapid-pvst
!
vlan 10
 name USERS
vlan 20
 name OPERATIONS
vlan 99
 name MGMT
vlan 100
 name AP-MGMT
vlan 110
 name WLAN-STAFF
vlan 999
 name NATIVE-BLACKHOLE
!
interface GigabitEthernet0/1
 description TRUNK_TO_SW1_GI0_2
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,99,100,110,999
 no shutdown
!
interface FastEthernet0/10
 description PC-B_VLAN20
 switchport mode access
```

```
 switchport access vlan 20
 spanning-tree portfast
 spanning-tree bpduguard enable
 no shutdown
!
interface GigabitEthernet0/24
 description WLC1_TRUNK
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 100,110,999
 no shutdown
!
interface Vlan99
 description MANAGEMENT_SVI
 ip address 10.99.99.13 255.255.255.0
 no shutdown
ip default-gateway 10.99.99.1
!
ip domain-name nga.lab
username admin privilege 15 secret Str0ng-Lab-Only!
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
end
write memory
```

R1 - Router-on-a-stick gateways

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 description TRUNK_TO_SW1_GI0_1
 no ip address
 no shutdown
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.20.20.1 255.255.255.0
!
interface GigabitEthernet0/0.99
 encapsulation dot1Q 99
 ip address 10.99.99.1 255.255.255.0
!
interface GigabitEthernet0/0.100
 encapsulation dot1Q 100
 ip address 10.100.100.1 255.255.255.0
!
interface GigabitEthernet0/0.110
 encapsulation dot1Q 110
```

```
 ip address 10.110.110.1 255.255.255.0
!
interface GigabitEthernet0/0.999
 encapsulation dot1Q 999 native
 no ip address
end
write memory
```

Endpoint and wireless addressing

- PC-A: 10.10.10.10/24, default gateway 10.10.10.1.
- PC-B: 10.20.20.20/24, default gateway 10.20.20.1.
- AP1 management: VLAN 100, for example 10.100.100.10/24 with gateway 10.100.100.1 or DHCP in the same subnet.
- WLC1 management: VLAN 100, for example 10.100.100.20/24 with gateway 10.100.100.1. CORP-STAFF clients map to VLAN 110.

Verification output and what to verify

1. VLAN and trunk verification

```
SW1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gi0/1       on           802.1q         trunking      999
Gi0/2       on           802.1q         trunking      999
Po10        on           802.1q         trunking      999

Port        Vlans allowed on trunk
Gi0/1       10,20,99,100,110,999
Gi0/2       10,20,99,100,110,999
Po10        10,20,99,100,110,999
```

What to verify

- All infrastructure trunks are operational and use native VLAN 999.
- Every required user, management and wireless VLAN is carried end to end.

2. LACP Port-Channel verification

```
SW1# show etherchannel summary
Group  Port-channel  Protocol    Ports
10     Po10(SU)       LACP       Fa0/23(P) Fa0/24(P)
```

What to verify

- Po10 is Layer 2/in use and both members are bundled.
- Shutting one member should leave Po10 operational through the remaining healthy member.

3. STP root verification

```
SW1# show spanning-tree root
                        Root    Hello Max Fwd
Vlan            Root ID         Cost    Time  Age Dly  Root Port
---------------- -------------------- --------- ----- --- ---  ----------------
VLAN0010        24586 0010.1111.1111        0    2   20  15
VLAN0020        24596 0010.1111.1111        0    2   20  15
```

```
VLAN0099        24675 0010.1111.1111      0    2   20  15
VLAN0100        24676 0010.1111.1111      0    2   20  15
VLAN0110        24686 0010.1111.1111      0    2   20  15
```

What to verify

- SW1 is the root bridge for VLANs 10,20,99,100 and 110.
- SW2 is configured as secondary and should not become root while SW1 is healthy.

4. Router-on-a-stick verification

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Gi0/0                  unassigned      YES unset  up                    up
Gi0/0.10               10.10.10.1      YES manual up                    up
Gi0/0.20               10.20.20.1      YES manual up                    up
Gi0/0.99               10.99.99.1      YES manual up                    up
Gi0/0.100              10.100.100.1    YES manual up                    up
Gi0/0.110              10.110.110.1    YES manual up                    up
Gi0/0.999              unassigned      YES unset  up                    up
```

```
R1# show ip route connected
C  10.10.10.0/24 is directly connected, GigabitEthernet0/0.10
C  10.20.20.0/24 is directly connected, GigabitEthernet0/0.20
C  10.99.99.0/24 is directly connected, GigabitEthernet0/0.99
C  10.100.100.0/24 is directly connected, GigabitEthernet0/0.100
C  10.110.110.0/24 is directly connected, GigabitEthernet0/0.110
```

What to verify

- All routed subinterfaces are up/up.
- Each VLAN subnet appears as directly connected through the correct subinterface.

5. End-to-end routing verification

```
PC-A> ping 10.20.20.20
Reply from 10.20.20.20: bytes=32 time<1ms TTL=127
Reply from 10.20.20.20: bytes=32 time<1ms TTL=127

PC-A> tracert 10.20.20.20
  1   <1 ms   <1 ms   <1 ms   10.10.10.1
  2   <1 ms   <1 ms   <1 ms   10.20.20.20
```

What to verify

- PC-A in VLAN 10 reaches PC-B in VLAN 20 through R1.
- The first routed hop is 10.10.10.1, proving the host is using the correct default gateway.

6. Switch management verification

```
SW2# show ip interface brief | include Vlan99
Vlan99                 10.99.99.12    YES manual up                    up
```

```
SW3# show ip interface brief | include Vlan99
Vlan99                 10.99.99.13    YES manual up                    up

SW1# show ip ssh
SSH Enabled - version 2.0
```

What to verify

- All switch management SVIs are up/up in VLAN 99.
- SSH version 2 is enabled and remote management uses VLAN 99.

7. AP/WLC wired-path verification

```
SW2# show interfaces fa0/11 switchport
Administrative Mode: static access
Operational Mode: static access
Access Mode VLAN: 100 (AP-MGMT)

SW3# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gi0/24      on           802.1q         trunking      999

Port        Vlans allowed on trunk
Gi0/24      100,110,999
```

What to verify

- AP1 is on management VLAN 100.
- WLC1 uplink carries management VLAN 100 and WLAN client VLAN 110.
- Only after the wired path is correct should you troubleshoot CAPWAP join, WLAN policy, authentication or DHCP.

Capstone troubleshooting tickets

1. VLAN 20 users cannot reach the gateway, but VLAN 10 works. Locate the Layer 2 or subinterface mismatch.

2. Port-Channel10 shows one member suspended. Find the mismatched switchport parameter.

3. A user connects a small switch to an edge port and the port err-disables. Explain which feature acted and why.

4. AP1 receives power but cannot reach WLC1. Prove VLAN 100 forwarding from the AP switchport toward the gateway/controller.

5. SSH fails but ping to the management SVI succeeds. Check domain/RSA keys, SSH version, VTY authentication and "**transport input**.

Module 2 Verification Command Index

VLAN / access: show vlan brief and show interfaces <int> switchport and show mac address-table

Trunks: show interfaces trunk and show interfaces <int> switchport

Discovery: show cdp neighbors detail and show lldp neighbors detail

EtherChannel: show etherchannel summary, show lacp neighbor, show pagp neighbor and show interfaces port-channel <n>

STP / Rapid PVST+: show spanning-tree vlan <id>, show spanning-tree root, show spanning-tree summary and show spanning-tree inconsistent ports

PoE / AP links: show power inline, show interfaces status and show lldp neighbors detail

Management: show ip interface brief, show ip ssh, show users and show ip http server status

Wireless controller: show wireless summary and show ap summary (Catalyst 9800 examples)

Suggested lab completion standard

- Student can build the topology from a blank file/device state.
- Student can explain why each command is required.
- Student can prove the expected state with show commands.
- Student can isolate at least one injected fault without relying on the instructor.
- Student saves the final running configuration and screenshots/text outputs required by the instructor.