

1. Virtual LANs (VLANs) & Trunking

VLANs logically segment a physical switch into multiple isolated broadcast domains. Devices in different VLANs require a Layer 3 device to communicate.

- **802.1Q:** The industry standard trunking protocol. Inserts a 4-byte tag into the Ethernet frame.
- **Native VLAN:** Untagged traffic on a trunk link. Defaults to VLAN 1. Security best practice is to change this to an unused VLAN.

Essential Commands:

```
SW1(config)# vlan 10
SW1(config-vlan)# name PROD_NET
SW1(config)# interface g0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config)# interface g0/24
SW1(config-if)# switchport mode trunk
```

2. Inter-VLAN Routing

To route traffic between isolated VLANs, you must cross a Layer 3 boundary.

Method	Description
Router-on-a-Stick (ROAS)	Uses router subinterfaces (e.g., g0/0.10) over a single trunk link. Requires 'encapsulation dot1q [vlan_id]' before assigning an IP.
Layer 3 Switching (SVIs)	Uses Switch Virtual Interfaces (interface vlan

Method	Description
	10) on a Multilayer Switch. Much faster. Requires the 'ip routing' global command.

3. Spanning Tree Protocol (STP)

Prevents Layer 2 broadcast storms by logically blocking redundant links. The switch with the lowest Bridge ID (BID) becomes the Root Bridge.

- **Bridge ID (BID):** Priority (Default 32768) + MAC Address.
- **Rapid PVST+ (802.1w):** Cisco's default modern STP. Provides sub-second convergence.
- **PortFast:** Skips listening/learning states. Use ONLY on edge ports connected to end devices (PCs, servers).
- **BPDU Guard:** Disables a PortFast-enabled port if it receives a BPDU, preventing rogue switches from causing loops.

Essential Commands:

```
SW1(config)# spanning-tree mode rapid-pvst
SW1(config)# spanning-tree vlan 10,20 root primary
SW1(config-if)# spanning-tree portfast
SW1(config-if)# spanning-tree bpduguard enable
```

4. EtherChannel (Link Aggregation)

Bundles multiple physical links into a single logical Port-Channel to increase bandwidth and provide redundancy without STP blocking the links.

Protocol	Standard	Modes
LACP	IEEE 802.3ad (Open Standard)	Active / Passive
PAgP	Cisco Proprietary	Desirable / Auto

** Always apply configurations (trunking, allowed VLANs) to the Port-Channel interface, not the physical member interfaces.*

5. Layer 2 Discovery Protocols

- **CDP (Cisco Discovery Protocol):** Cisco proprietary. Enabled by default. Transmits every 60s.
- **LLDP (Link Layer Discovery Protocol):** IEEE 802.1AB standard. Vendor-neutral. Transmits every 30s.

Security Note: Disable CDP/LLDP on untrusted edge ports using `no cdp enable` to prevent reconnaissance, except when connecting to Cisco IP Phones which require CDP for Voice VLAN assignment.

6. Wireless Architectures & Security

Split-MAC Architecture

Divides wireless functions between Lightweight Access Points (LAPs) and a Wireless LAN Controller (WLC).

- **LAP Duties:** Real-time RF tasks, beacons, hardware encryption.
- **WLC Duties:** Authentication, roaming control, RF management.

CAPWAP Tunneling

- **Control Traffic:** UDP 5246 (Encrypted via DTLS by default).
- **Data Traffic:** UDP 5247 (Unencrypted by default).

WLAN Security

Standard	Cipher / Protocol	Status
WPA / WEP	TKIP / RC4	Compromised. Do not use.
WPA2	AES / CCMP	Current Enterprise Standard.

Standard	Cipher / Protocol	Status
WPA3	SAE	Modern Standard (Replaces PSK Handshake).

Authentication Modes:

- **Personal:** Uses a Pre-Shared Key (PSK).
- **Enterprise (802.1X):** Uses an external RADIUS server (AAA) for individual user credentials. WLC acts as the authenticator.