Switching Concepts Cheat Sheet

A quick reference guide to networking switch concepts and terminology, covering VLANs, spanning tree protocol, port security, and more.

Switch Basics

Fundamentals

Switch: A network device that forwards data packets between devices on the same network.
Operates at Layer 2 (Data Link Layer) of the OSI model, using MAC addresses to make forwarding decisions.

MAC Address Table (CAM Table): A table maintained by the switch that maps MAC addresses to switch ports. Used to determine where to forward traffic.

Forwarding Methods:

- **Store and Forward:** Switch receives the entire frame, checks for errors (CRC), and then forwards it.
- **Cut-Through:** Switch starts forwarding the frame as soon as the destination MAC address is read. Reduces latency, but doesn't check for errors.

Switching Loop: Occurs when there are multiple paths between switches, causing frames to circulate endlessly. Spanning Tree Protocol (STP) prevents this.

Switch Ports

Access Port	Connects to end-user devices (e.g., computers, printers). Belongs to a single VLAN.
Trunk Port	Carries traffic for multiple VLANs. Uses tagging protocols like 802.1Q to identify VLAN membership.
Hybrid Port	Can behave as both an access port and a trunk port, allowing both tagged and untagged traffic. More flexible but potentially more complex to configure.

Duplex and Speed

Half-Duplex	Devices can only send or receive data at a time. Older technology, prone to collisions.
Full-Duplex	Devices can send and receive data simultaneously. Reduces collisions, increases throughput.
Autonegotiation	Process where devices automatically negotiate the best speed and duplex settings. Mismatched settings can lead to performance issues.

VLANs (Virtual LANs)

VLAN Concepts

VLAN: A logical grouping of network devices that allows them to communicate as if they were on the same physical LAN, regardless of their physical location. Improves security, performance, and manageability.

VLAN ID: A unique identifier assigned to each VLAN, ranging from 1 to 4094. VLAN 1 is the default VLAN.

Native VLAN: The VLAN assigned to untagged traffic on a trunk port. Important for interoperability.

VLAN Types

Static VLAN	Manually configured VLAN assignments. Simple but requires more administration.
Dynamic VLAN	VLAN assignments based on MAC addresses or user authentication. More complex but simplifies administration.

VLAN Configuration (Cisco Example)

```
! Create VLAN 10
switch(config)# vlan 10
switch(config-vlan)# name VLAN10

! Assign port FastEthernet0/1 to VLAN 10
switch(config)# interface FastEthernet0/1
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 10

! Configure trunk port FastEthernet0/2
switch(config)# interface FastEthernet0/2
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk
encapsulation dot1q
switch(config-if)# switchport trunk allowed
vlan 10,20
```

Spanning Tree Protocol (STP)

STP Fundamentals

STP: A Layer 2 protocol that prevents switching loops by blocking redundant paths in a network. Ensures a single logical path between any two switches.

Root Bridge: The central switch in the STP topology. All path calculations are made relative to the root bridge.

Bridge Protocol Data Units (BPDUs): Messages exchanged between switches to elect the root bridge and determine the STP topology.

STP Port States

Blocking	Port receives BPDUs but does not forward data. Prevents loops.
Listening	Port receives BPDUs and determines the network topology.
Learning	Port learns MAC addresses from received frames.
Forwarding	Port forwards data traffic.
Disabled	Port is administratively disabled.

STP Variants

Common Spanning Tree (CST): One spanning tree instance for the entire network. Less efficient than per-VLAN STP.

Per-VLAN Spanning Tree (PVST): A separate spanning tree instance for each VLAN. More efficient but requires more processing power.

Rapid Spanning Tree Protocol (RSTP/802.1w): Faster convergence than STP. Uses alternate and backup ports for quicker failover.

Multiple Spanning Tree Protocol (MSTP/802.1s): Maps multiple VLANs to a single spanning tree instance. Combines the benefits of PVST and CST.

Switch Security

Port Security

Port Security: A feature that limits the number of MAC addresses that can be learned on a port. Prevents MAC address flooding attacks and unauthorized access.

Sticky MAC Address: Dynamically learns MAC addresses and adds them to the running configuration.

Violation Modes:

- **Protect:** Drops traffic from unknown MAC addresses without notification.
- **Restrict:** Drops traffic from unknown MAC addresses and increments a security violation counter.
- **Shutdown:** Disables the port upon a security violation.

Other Security Measures

DHCP Snooping	Prevents rogue DHCP servers from assigning invalid IP addresses.
Dynamic ARP Inspection (DAI)	Prevents ARP spoofing attacks by validating ARP packets against the DHCP snooping database.
** storm control **	Limit traffic from unknown MAC addresses and increment security violations.

Security Configuration (Cisco Example)

```
! Enable port security on FastEthernet0/1
switch(config)# interface FastEthernet0/1
switch(config-if)# switchport port-security

! Limit to 1 MAC address
switch(config-if)# switchport port-security
maximum 1

! Enable sticky MAC address learning
switch(config-if)# switchport port-security
mac-address sticky

! Set violation mode to shutdown
switch(config-if)# switchport port-security
violation shutdown
```