STP (Spanning Tree Protocol)

- **Definition:** A Layer 2 protocol used to prevent **loops** in a switched network by blocking redundant paths.
- **Purpose:** Eliminates single points of failure in Layer 2 networks.
- **Benefit:** Ensures that if a link or a switch goes down, there is a **backup path** without creating broadcast storms.

Broadcast Storms

- **Definition:** An excessive amount of broadcast traffic that overwhelms the network.
- **Cause:** Usually the result of **Layer 2 loops** when STP is not implemented or fails.
- **Effect:** Consumes bandwidth, degrades performance, and can cause network outages.

STP BPDU (Bridge Protocol Data Unit)

- **Definition:** The control message exchanged between switches to build and maintain the Spanning Tree topology.
- **Contents of a BPDU:**
  - **Protocol Identifier** – Identifies the protocol as STP (always 0x0000).
  - **Protocol Version** – STP version (1 = STP, 2 = RSTP).
  - **BPDU Type** – Configuration or TCN (Topology Change Notification).
  - **Flags** – Indicate topology changes or proposal/agreement states.
  - **Root Bridge ID** – The Bridge ID of the root switch (BID = priority + MAC address).
  - **Root Path Cost** – Total cost from the sending switch to the root bridge.
  - **Sending Bridge ID** – The Bridge ID of the switch sending the BPDU.
  - **Sending Port ID** – Port ID of the sending switch (priority + port number).
  - **Message Age** – How long the BPDU has been in the network.
  - **Max Age** – Maximum lifetime of a BPDU before it is discarded (default 20 seconds).

- **Hello Time** – Interval between BPDUs sent by the root bridge (default 2 seconds).
- **Forward Delay** – Time spent in listening and learning states (default 15 seconds).

Types of Spanning Tree Protocol

- **STP (802.1D)** – Original standard.
  - **Convergence Time:** ~30–50 seconds after a fault.
- **PVST+ (Per-VLAN Spanning Tree Plus)** – Cisco proprietary; separate STP instance per VLAN.
  - **Convergence Time:** 30–50 seconds.
- **Rapid STP (802.1w)** – Faster convergence.
  - **Convergence Time:** ~3–5 seconds.
- **Rapid PVST+** – Cisco's enhancement of RSTP, separate instance per VLAN.
  - **Convergence Time:** ~3–5 seconds.
- **MST (802.1s)** – Multiple VLANs mapped to same spanning tree instance.
  - **Convergence Time:** ~3–5 seconds.

Spanning-Tree Algorithm Steps

1. **Root Bridge Election**
   a. All switches assume they are the root bridge at startup.
   b. The switch with the **lowest Bridge ID (BID)** becomes the root bridge.
   c. BID = Bridge Priority (default 32768) + MAC address.
   d. **Tie-Breaker:** If Bridge Priority is the same, the switch with the **lowest MAC address** becomes the root.

2. **Root Port Selection (Stand of the Switch)**
    a. On non-root switches, the **Root Port (RP)** is chosen.
    b. The RP is the port with the **lowest cumulative path cost** to the root bridge.
    c. Path Cost Reference (802.1D):

Speed	Short Method	Long Method
10 Mbps	100	200000
100 Mbps	19	20000
1 Gbps	4	2000
10 Gbps	2	200

    d. Configuration:
        i. Short method: `spanning-tree pathcost method short`
        ii. Long method: `spanning-tree pathcost method long`
    e. **Tie-Breaker:** If multiple ports have the same path cost, the port connected to the switch with the **lowest Bridge ID** is selected. If still tied, the **lowest port ID** is chosen.
3. **Designated Port Selection (Stand of the segment)**
    a. On each network segment, the port with the **lowest path cost to the root** becomes the **Designated Port (DP)**.
    b. DPs are responsible for forwarding traffic toward and from that segment.
    c. A designated port is always opposite of a root port.
4. **Blocking Non-Designated Ports**
    a. Ports that are neither **Root Ports** nor **Designated Ports** are placed in a **Blocking State**.
5. **Port States Transition (802.1D STP)**
    a. Blocking → Listening → Learning → Forwarding
        i. **Blocking:** Does not forward traffic; only listens for BPDUs.
        ii. **Listening:** Processes BPDUs; does not forward or learn MACs.
        iii. **Learning:** Learns MAC addresses but does not forward traffic.
        iv. **Forwarding:** Forwards traffic and learns MAC addresses.
        v. **Disabled:** Admin-shutdown; not part of STP.
    b. Each transition is controlled by timers (Forward Delay, Max Age, Hello Time).

6. **Loop-Free Topology Established**
    a. Traffic flows via Root and Designated Ports.
    b. Redundant links remain in **Blocking State** until needed.

STP Convergence, Configuration and Manipulation

RSTP Port Roles, States, and Operational Effects

- **Root Port (RP)**
    - **State:** Forwarding
    - **Effect:** The single port on a non-root switch that has the best path (lowest cost) to the root bridge. Always forwards traffic toward the root.
- **Designated Port (DP)**
    - **State:** Forwarding
    - **Effect:** One per segment, chosen to forward traffic away from the root bridge onto that segment.
- **Alternate Port (AP)**
    - **State:** Discarding
    - **Effect:** Provides a backup path to the root bridge. Immediately takes over if the Root Port fails.
- **Backup Port (BP)**
    - **State:** Discarding
    - **Effect:** Provides a redundant connection on a segment where another port is already the Designated Port. Rare in modern topologies.
- **Disabled Port**
    - **State:** Discarding (administratively down)
    - **Effect:** Not participating in STP, manually shut down.

RSTP Port States (Simplified vs Legacy STP)

- **Discarding** = (Blocking + Listening in 802.1D)
- **Learning** = Still a valid RSTP state; MAC addresses are learned but no forwarding yet.
- **Forwarding** = Full forwarding and learning.

👉 **Note:** RSTP has exactly **three port states**: **Discarding, Learning, Forwarding**. The old 802.1D states Blocking and Listening are combined into Discarding.

RSTP improves convergence to **~3–5 seconds** compared to 802.1D's **30–50 seconds**.

Root Bridge Placement and Configuration

- Place the Root Bridge near the L2/L3 boundary.
- Force a switch to be the Root Bridge by lowering its priority:
  - `spanning-tree vlan 10 priority 0`
- For exam purposes only (not recommended in production):
  - `spanning-tree vlan 10 root primary`
  - This does not guarantee the switch will be the Root Bridge.

STP Protection Mechanisms

- **PortFast**
  - Immediately places an access port into the Forwarding state, bypassing Listening and Learning.
  - Improves convergence time.
  - Used for ports connected to end devices (PCs, printers).
    - Depending on the device connected, could be spanning-tree port trunk
  - Should not be enabled on ports connected to switches, as it can create loops.
  - Reduces STP messages when ports are enabled or disabled.
  - **Configuration:**
    - Global: `spanning-tree portfast default`
    - Interface: `spanning-tree portfast`
- **BPDU Guard**
  - Shuts down a PortFast-enabled port if any BPDU is received.

    - Protects the network from misconfigurations or malicious devices attempting to participate in STP.
    - **Configuration:**
        - Global: `spanning-tree portfast bpduguard default`
        - Interface: `spanning-tree bpduguard enable`
- **Root Guard**
    - Prevents a designated port from becoming a root port.
    - Ensures the intended Root Bridge remains the root by blocking superior BPDUs on that port.
    - **Configuration:**
        - Interface: `spanning-tree guard root`
- **BPDU Filter**
    - Prevents sending or receiving BPDUs on a port.
    - Can be dangerous if misconfigured, as it effectively removes STP protection on that port.
    - **Configuration:**
        - Global (preferred): `spanning-tree portfast bpdufilter default`
        - Interface: `spanning-tree bpdufilter enable`
- **Loop Guard**
    - Prevents ports from erroneously transitioning to Forwarding if BPDUs are missing (e.g., unidirectional link failure).
        - Link failure is likely do to the transcieving or reciveing cable being broken.
    - Keeps the port in a loop-inconsistent (blocking) state until BPDUs are received again.
    - Protects STP from loops caused by unidirectional links.
    - **Configuration:**
        - Interface: `spanning-tree guard loop`

EtherChannels (CCNA Focus)

EtherChannel

- A technology that allows multiple physical Ethernet links (minimum 2, maximum 8 active) to be bundled into one logical link.
    - PAgP and LACP support 8 active links, but PAgP allows up to 16 with 8 as spare links.
- Provides increased bandwidth and redundancy.
- Seen by STP and routing protocols as a single logical interface.
- Helps prevent loops while maximizing link utilization.
- Commonly used between switches or between switches and routers/servers.
- **CCNA Tip:** EtherChannel concepts are tested in terms of configuration, verification, and how STP interacts with bundled links.
    - **Port Requirements:** All physical ports in an EtherChannel must have the same configuration:
        - Speed and Duplex
        - Trunk: Native VLAN and allowed VLANs
        - Access: VLAN assigned to ports

Key Benefits:

- **Load Balancing:** Distributes traffic across multiple physical links.
- **Fault Tolerance:** If one physical link fails, traffic continues over the remaining links.
- **Simplified STP:** STP treats the EtherChannel as one logical link, reducing blocked redundant paths.
- **CCNA Tip:** Understand how EtherChannel affects spanning tree and logical interface representation.

Configuration Protocols:

- **PAgP (Port Aggregation Protocol):** Cisco proprietary.
- **LACP (Link Aggregation Control Protocol):** IEEE 802.3ad standard, multi-vendor support.
- **Static (On):** No negotiation protocol; ports are manually forced into an EtherChannel.
- **CCNA Tip:** Know the differences between PAgP, LACP, and Static for the exam.

Basic Configuration Example:

```
interface range f0/1 - 2
 channel-group 1 mode active   ! LACP (active/passive)
 channel-group 1 mode desirable ! PAgP (desirable/auto)
 channel-group 1 mode on        ! Static
```

Verification Commands:

```
show etherchannel summary
show running-config
```

- **CCNA Tip:** Be able to interpret show etherchannel summary output to confirm EtherChannel operation and port participation.

```
DSW1#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      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not r
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------
12     Po12(RU)         LACP      Gi1/0/17(P) Gi1/0/18(P) Gi1/0/19(P)
                                  Gi1/0/20(P)
```

DHCP for IPv4

Setting up a Cisco Router or L3 Switch as a DHCP Server

- Configure the DHCP pool for a subnet.
- Define the network, default gateway, DNS server, and optionally a domain name.
- Optionally, exclude addresses that should not be assigned (like static IPs).
- Optionally, configure DHCP options such as **option 150** for TFTP server address (commonly used for VoIP phones).

Example Configuration:

```
! Exclude IP addresses
ip dhcp excluded-address 192.168.1.1 192.168.1.10

! Create DHCP pool
ip dhcp pool VLAN10
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 8.8.8.8 8.8.4.4
 domain-name example.com
 option 150 ip 192.168.1.50   ! TFTP server for IP phones
 lease 7
```

Verification Commands:

```
show ip dhcp binding    ! Displays IP addresses leased to clients
show running-config     ! Confirms DHCP pool configuration
show ip dhcp pool       ! Displays DHCP pool statistics
```

CCNA Tip:

- Always remember to exclude IPs used for routers, servers, and other static devices.
- You can have multiple DHCP pools on the same router for different VLANs.
- Assigning a domain name and DNS options ensures clients can resolve internal hostnames.
- **Option 150** is important for Cisco IP phones to find their TFTP server for configuration files.

DHCP Relay Agent (Cisco Router or L3 Switch)

- A DHCP Relay Agent allows clients on different VLANs or subnets to obtain IP addresses from a DHCP server that is not on the same local subnet.
- The router or L3 switch receives DHCP requests from clients and forwards them to the DHCP server using the **`ip helper-address`** command.

Example Configuration:

```
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
 ip helper-address 192.168.1.1   ! IP of DHCP server
```

- Typically in enterprise enviroment you will have the switch be a relay with a centralized DHCP server intead of the switches acting as there own DHCP servers per vlan.