# Switching Basics & Intermediate Routing (LAN Switching and Wireless)

Lecture 3: Spanning Tree

*CCNA Routing and Switching 3*
*- Scaling Networks*

# Recap on last week

- Campus Wired LAN Designs
  - Why it is important to design a scalable hierarchical network
- Selecting Network Devices
  - Select network devices based on feature compatibility and network requirements
- VTP, Extended VLANs, and DTP
  - Configure enhanced inter-switch connectivity technologies

# Objective for this lecture:

- Troubleshoot Multi-VLAN Issues
  - Troubleshoot issues in an inter-VLAN routing environment.
- Layer 3 Switching
  - Implement inter-VLAN routing using Layer 3 switching to forward data in a small to medium-sized business LAN
- Spanning Tree Concepts
  - Examine the purpose of STP and how the spanning tree algorithm is used create a loop-free topology.
- Varieties of Spanning Tree Protocols
  - Examine the varieties of Spanning Tree protocols including PVST+ and Rapid PVST+.

# Troubleshoot Multi-VLAN Issues

# Deleting a VLAN

- To delete a VLAN, use the `no vlan vlan-id` global configuration mode command

```
S1(config)# no vlan 99
S1(config)# exit
S1# show vlan id 99
VLAN id 99 not found in current VLAN database
```

- If switch is in VTP server mode, VLAN is removed from the VLAN database for all switches in the VTP domain
- When you delete a VLAN, any ports assigned to that VLAN become inactive until you assign them to a new VLAN

# Switch Configuration Problems

- If a switch port is not configured for the correct VLAN, devices configured on that VLAN cannot connect to the router interface
- When a problem is suspected with a switch configuration, use the various verification commands to examine the configuration and identify the problem

```
S1# show interfaces FastEthernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: up
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
S1#
```

# Router Configuration Problems

- When enabling inter-VLAN routing on a router, one of the most common configuration errors is to connect the physical router interface to the wrong switch port
- With router-on-a-stick configurations, a common problem is assigning the wrong VLAN ID to the subinterface
- Using the show interfaces and the show running-config commands can be useful in troubleshooting this type of issue

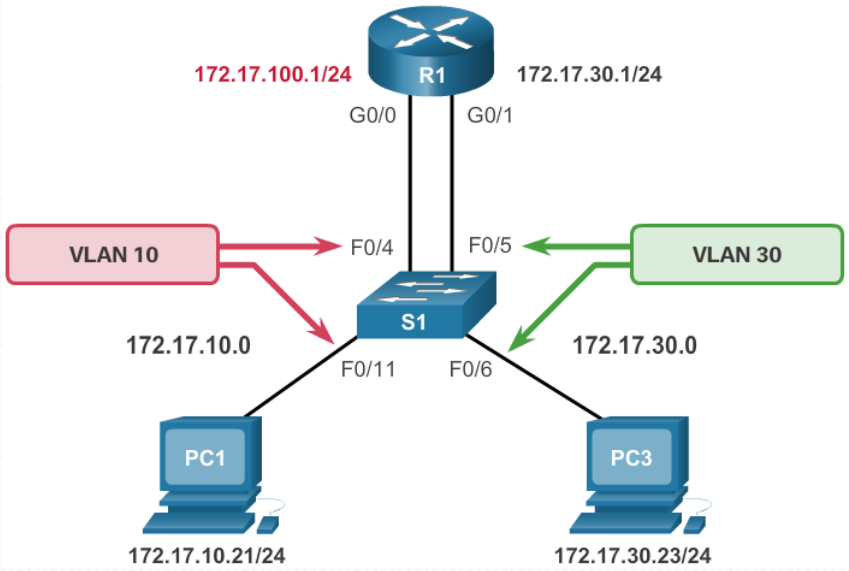
```
R1# show interfaces

<output omitted>

GigabitEthernet0/0.10 is up,line protocol is down (disabled)
 Encapsulation 802.1Q Virtual Lan,Vlan ID 100
 ARP type :ARPA,ARP Timeout 04:00:00,
 Last clearing of "show interface" counters never
```

# Errors with IP Addresses and Subnet Masks

- For inter-VLAN routing to operate, a router must be connected to all VLANs, either by separate physical interfaces or by subinterfaces




- Each interface, or subinterface, must be assigned an IP address that corresponds to the subnet to which it is connected
- Use the show running-config and show ip interface commands to verify IP address and subnet masks

# Troubleshooting VTP Issues

There are 5 common problems with VTP:

- Incompatible VTP Versions - Ensure that all switches are capable of supporting the required VTP version
- VTP Password Issues - If VTP authentication is enabled, switches must all have the same password configured to participate in VTP
- Incorrect VTP Domain Name - improperly configured VTP domain affects VLAN synchronization between switches and if a switch receives the wrong VTP advertisement, the switch discards the message. Should only be set by server
- All Switches Set to Client Mode – Cannot manage VLANs
- Incorrect Configuration Revision Number – Caused by a switch being added to the domain with the same VTP domain name but a higher configuration number

# Troubleshooting DTP Issues

- There are three common problems associated with trunks.

| VTP Components | Definition |
|---|---|
| Trunk mode mismatches | • For example, one trunk port is configured to trunk and the other side is configured as an access port. Another example is that both sides are configure in DTP auto mode. Other mismatches are also possible.<br>• This configuration error causes the trunk link to stop working.<br>• Correct the situation by shutting down the interface, correcting the DTP mode settings, and re-enabling the interface. |
| Allowed VLANs on trunks | • The list of allowed VLANs on a trunk has not been updated with the current VLAN trunking requirements.<br>• In this situation, unexpected traffic or no traffic is being sent over the trunk.<br>• Configure the correct VLANs that are allowed on the trunk. |
| Native VLAN mismatches | • When native VLANs do not match, the switches will generate informational messages letting you know of the problem.<br>• Ensure that both sides of a trunk link are using the same native VLAN. |

# Layer 3 Switching

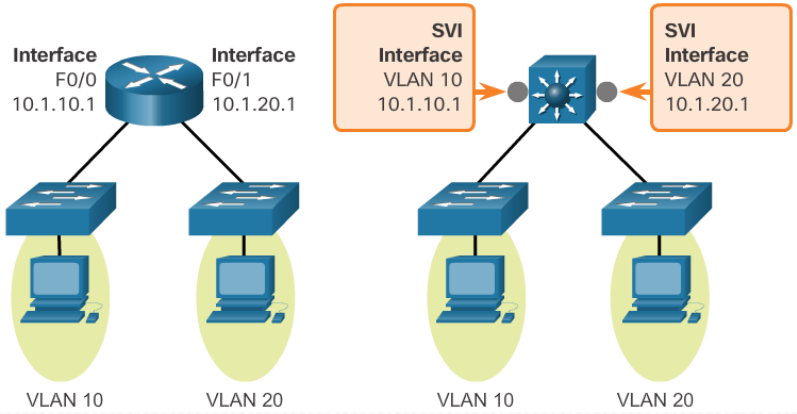
# Layer 3 Switching Introduction

- Modern enterprise networks use multilayer switches to achieve high-packet processing rates using hardware-based switching

- Catalyst multilayer switches support the following types of Layer 3 interfaces:
  - Routed port: A pure Layer 3 interface similar to a physical interface on a Cisco IOS router
  - Switch virtual interface (SVI): A virtual VLAN interface for inter-VLAN routing. In other words, SVIs are the virtual-routed VLAN interfaces

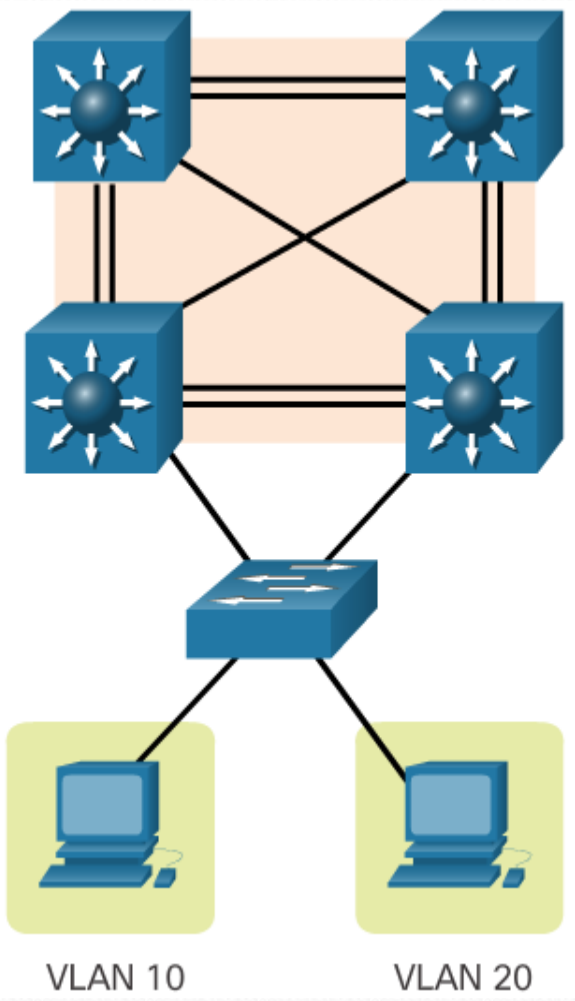
# Inter-VLAN Routing and SVIs

- Routing can be transferred to the core and the distribution layers (and sometimes even the access layer) without impacting network performance
- An SVI can be created for any VLAN that exists on the switch
- SVIs are created the first time the VLAN interface configuration mode is entered for a particular VLAN SVI



# Inter-VLAN Routing with Routed Ports

- A routed port is a physical port that acts similarly to an interface on a router
- A routed port is not associated with a particular VLAN
- Routed ports on a Cisco IOS switch do not support subinterfaces
- Routed ports are used for point-to-point links
- To configure routed ports, use the `no switchport interface` configuration mode command on the appropriate ports



# Troubleshooting Layer 3 Switching Configuration Issues

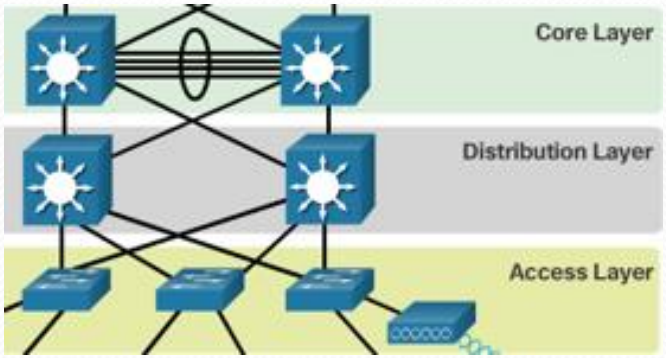
Check the following configurations for accuracy:

- VLANs - VLANs must be defined across all the switches. VLANs must be enabled on the trunk ports. Ports must be in the right VLANs
- SVIs - SVIs must have the correct IP address or subnet mask. SVIs must be up. Each SVI must match with the VLAN number
- Routing - Routing must be enabled. Each interface or network should be added to the routing protocol, or static routes entered, where appropriate
- Hosts - Hosts must have the correct IP address or subnet mask. Hosts must have a default gateway associated with an SVI or routed port

# Spanning Tree Concepts

# Purpose of Spanning Tree

- Last week we looked at the importance of having redundancy as part of the 3-tier hierarchical network design




➢ This is on the physical layer (i.e. OSI Layer 1) using multiple links & devices

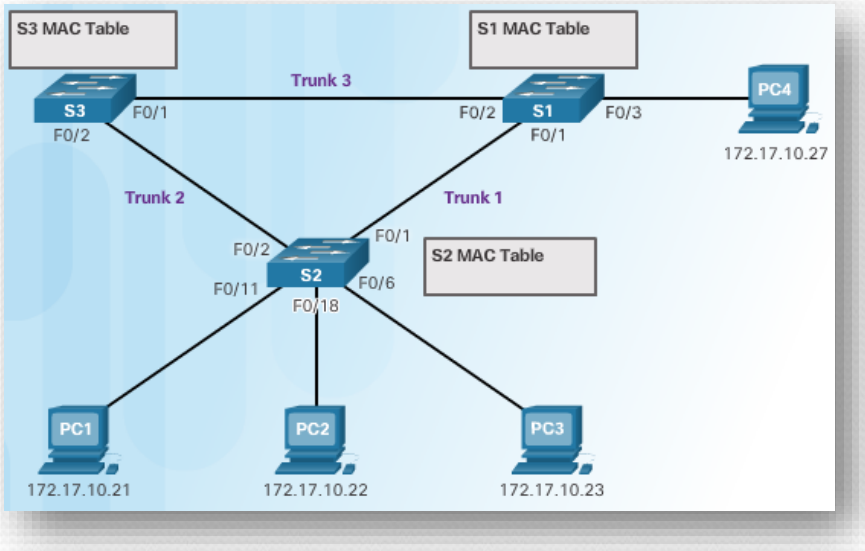
- However, for this to operate correctly we also need to use OSI Layer 2 protocols such as Spanning Tree Protocol (STP)

- Otherwise, we may get logical Layer 2 loops which will slow down and eventually crash our network

# Issues with Layer 1 Redundancy

- There are 3 main issues that can be caused by implementing Layer 1 redundancy (if STP is not implemented):

1. MAC Database Instability
2. Broadcast Storms
3. Duplicate Unicast Frames



# 1. MAC Database Instability

- Ethernet frames have no time to live (TTL) so there is no mechanism enabled to block continued propagation of frames on switched network
- Broadcast frames are forwarded out all switch ports, except the original incoming port
- If there is more than one path for the frame to be forwarded out of, an endless loop can result
- This results in constant changes to the MAC address table which leads to MAC database instability
- See animation…..

https://static-course-assets.s3.amazonaws.com/ScaN6/en/index.html#3.1.1.2

# 2. Broadcast Storms

- A broadcast storm occurs when there are so many broadcast frames caught in a Layer 2 loop that all available bandwidth is consumed
- No bandwidth is available for legitimate traffic – same effect as Denial of Service (DoS) attack
- Is unavoidable in a looped network
- See animation…

https://static-course-assets.s3.amazonaws.com/ScaN6/en/index.html#3.1.1.3

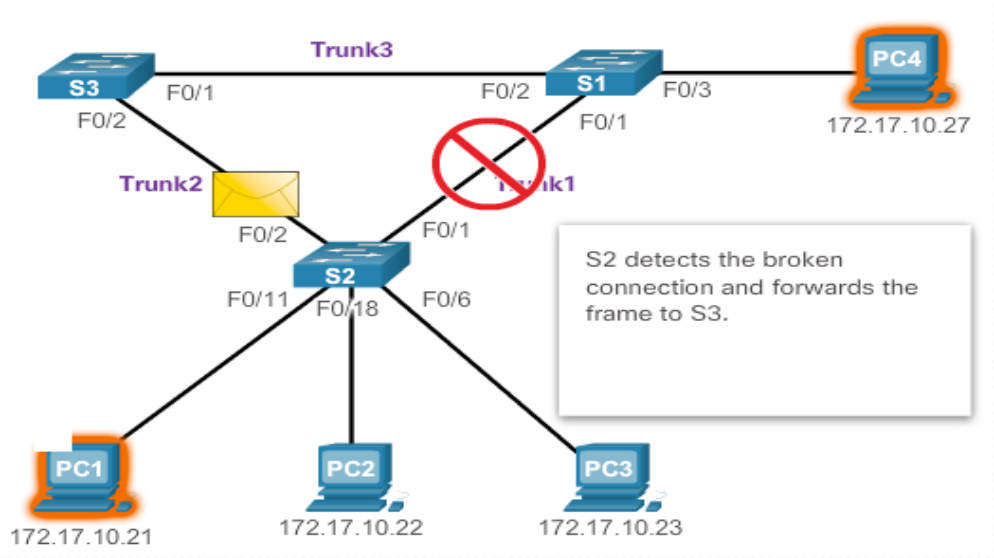
# 3. Duplicate Unicast Frames

- An unknown unicast frame is when the switch does not have the destination MAC address in its MAC address table and must forward the frame out all ports (except the incoming port)
- Unknown unicast frames sent onto a looped network can result in duplicate frames arriving at the destination device
- See animation…

https://static-course-assets.s3.amazonaws.com/ScaN6/en/index.html#3.1.1.4

# Spanning Tree Protocol (STP) Introduction

- STP was developed to address the issues caused by loops
- STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop

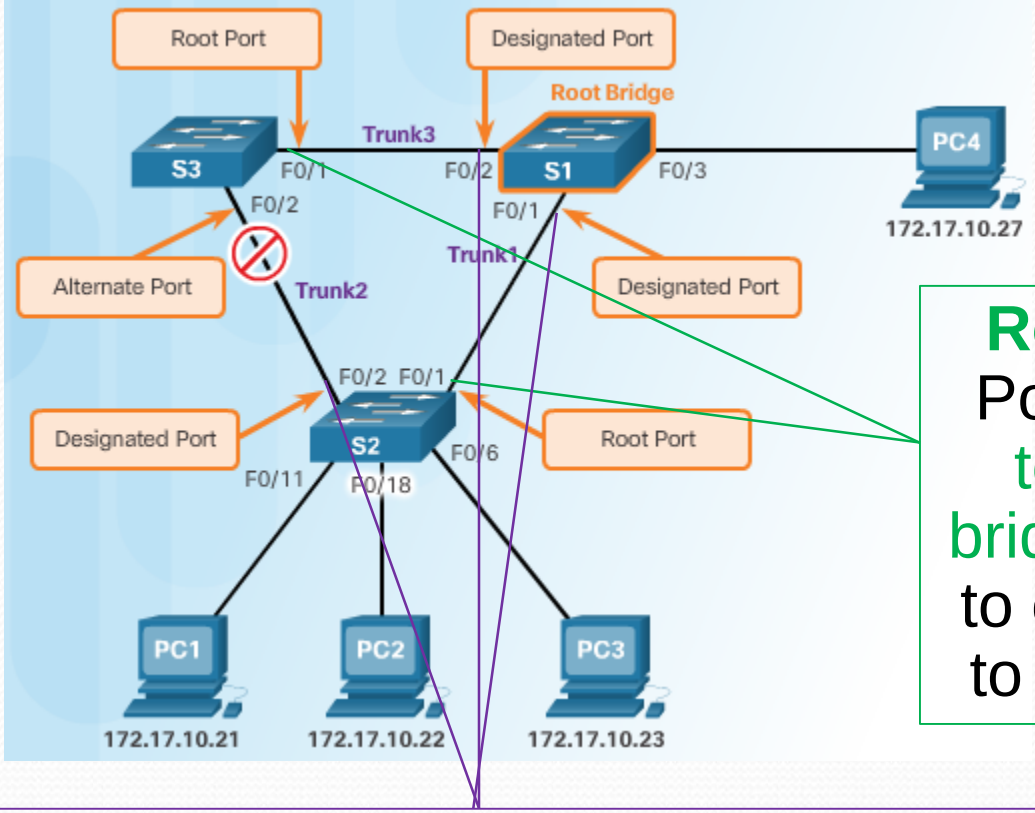



If there is a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active

# Spanning Tree Algorithm

- Spanning Tree Algorithm (STA) is used to determine which switch ports on the network are set to blocking to prevent loops from occurring
- STA designates a single switch as the root bridge which serves as a reference point for all STP calculations
- The switch with the lowest bridge ID (BID) will become the root bridge for the STA calculations
- The STA then determines the best paths to the root bridge for all switch ports in the broadcast domain
- When the STA has determined which paths are most desirable relative to each switch, it assigns port roles to the participating switch ports

# STA - Port Roles

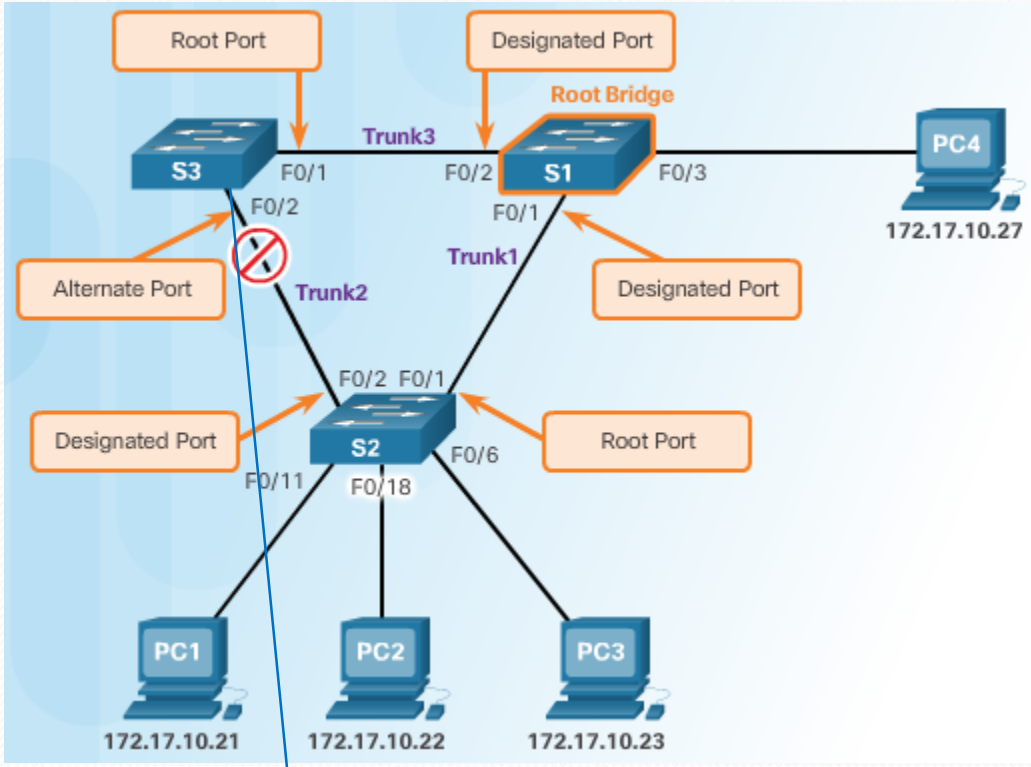



**Root ports:** Ports closest to the root bridge, relative to overall cost to root bridge

**Designated ports** – All non-root ports that are still permitted to forward traffic. If one end of a segment is a root port, then the other end is a designated port. All ports on the root bridge are designated ports

# STA - Port Roles

**Disabled ports**: A switch port that is shut down

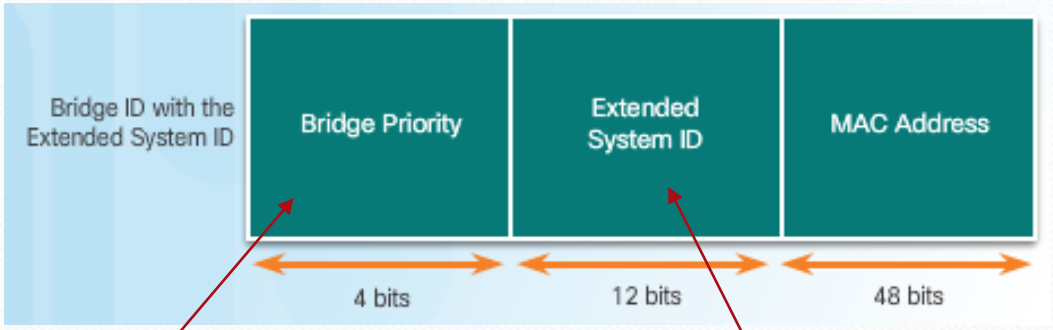



**Alternate and backup ports**: Blocking / discarding state to prevent loops. Only selected on links where neither end is a root port

# STA – Root Bridge Selection

- Initially at boot up, every switch declares itself as the root bridge and records its own BID as the root ID
- An election process determines which switch is actual root bridge
- All switches in the broadcast domain participate in election and send BPDU frames
  - BPDU's contain the switch BID and the root ID
  - If the root ID from a BPDU received is lower than root ID on receiving switch, the receiving switch updates its root ID
- Eventually, the switch with lowest BID ends up being identified as the root bridge for the spanning tree instance
- A root bridge elected for each spanning tree instance – could have different root bridges for different VLANs

# Bridge ID Fields




Configurable value between 0 and 65,535. Default is 32,768

Used to specify a VLAN ID or a multiple spanning tree protocol (MSTP) instance ID

# STA – Root Path Cost

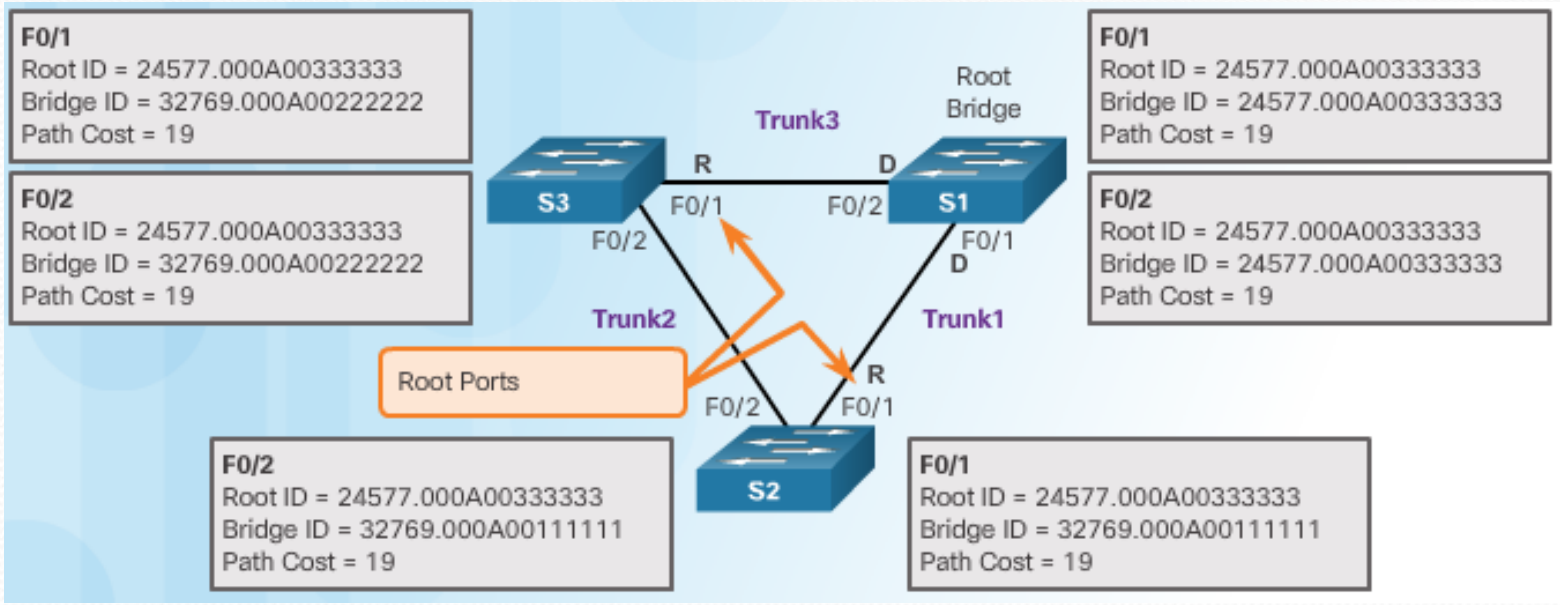
- STA determines the best paths to the root bridge from all destinations in the broadcast domain
- Default port costs are defined by the speed at which the port operates

| Link Speed | Cost (Revised IEEE Specification) |
|---|---|
| 10 Gb/s | 2 |
| 1 Gb/s | 4 |
| 100 Mb/s | 19 |
| 10 Mb/s | 100 |

- Internal root path cost is determined by summing up the individual port costs along the path from the switch to the root bridge
- Use the `spanning-tree cost` *`value`* interface configuration command on both ends of a link to apply a custom cost
- Use the `show spanning-tree` command to verify the port and internal root path cost to the root bridge

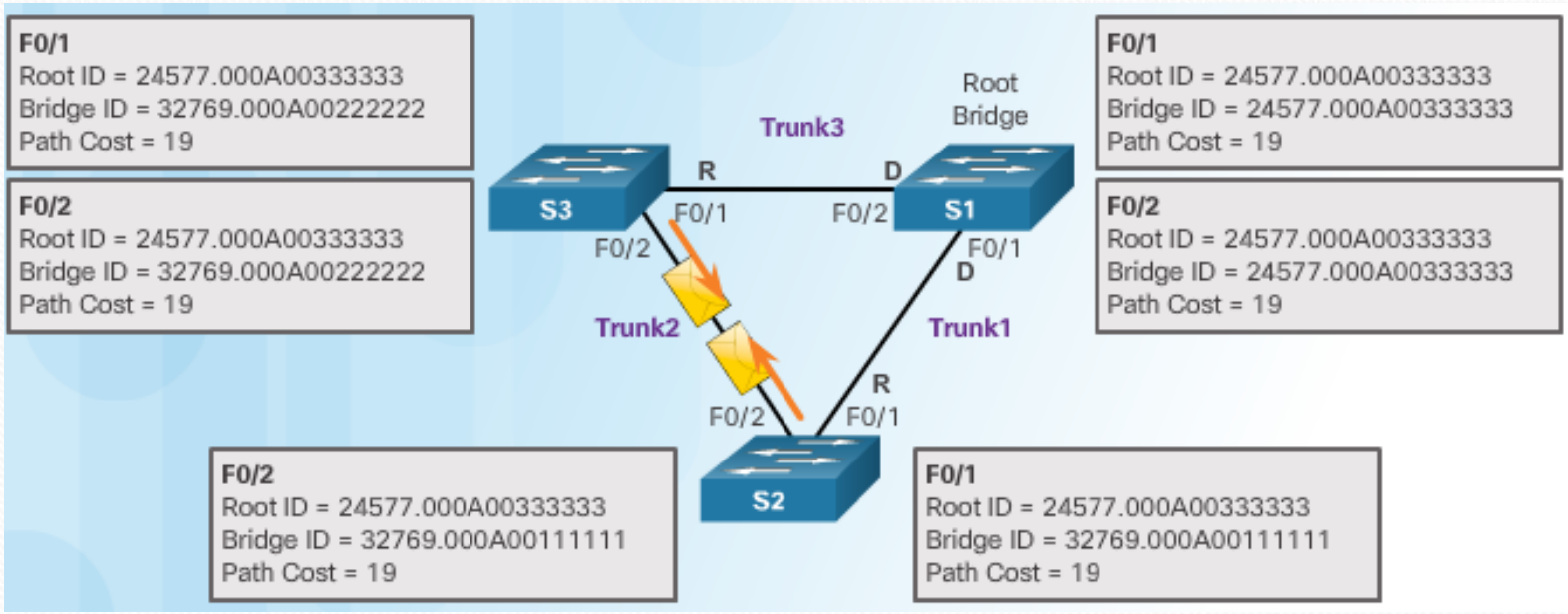
# Port Role Decisions for RSTP

- Root bridge automatically configures all of its switch ports in the designated role
- STP then determines which switch port serves in the root port role on each switch
- Switch port with the lowest overall path cost to the root bridge is automatically assigned the root port role



# Designated and Alternate Ports

- STP then needs to decide which ports have the designated and alternate roles
- For shared segments (i.e. a redundant paths to root bridge), switches exchange BPDU frames
- Switch with lower cost path to the root bridge (root path cost) will have its port selected as the designated port
- Other side of link set as alternate port (i.e. port will be blocking)
- If costs are same, one with lower BID chosen as designated



# 802.1D BPDU Frame Format

- The spanning tree algorithm depends on the exchange of BPDUs to determine a root bridge
- The BPDU frame information is included in the Data portion of an Ethernet frame and identifies the following fields:

| Field Number | Bytes | Field |
|---|---|---|
| 1-4 | 2 | Protocol ID |
| | 1 | Version |
| | 1 | Message Type |
| | 1 | Flags |
| 5-8 | 8 | Root ID |
| | 4 | Root Path Cost |
| | 8 | Bridge ID |
| | 2 | Port ID |
| 9-12 | 2 | Message Age |
| | 2 | Max Age |
| | 2 | Hello Time |
| | 2 | Forward Delay |

# 802.1D BPDU Propagation and Process

- By default, BPDU frames are sent every two seconds
- Each switch maintains local information about its own BID, the root ID, and the root path cost
- When adjacent switches receive a BPDU frame, they compare the frame's root ID with their local root ID
- If the received BPDU root ID is lower than the local root ID, switch updates local root ID & ID its BPDU messages
- The incoming port cost is then added to the root path cost in the BPDU to determine the internal root path cost from this switch to the root bridge

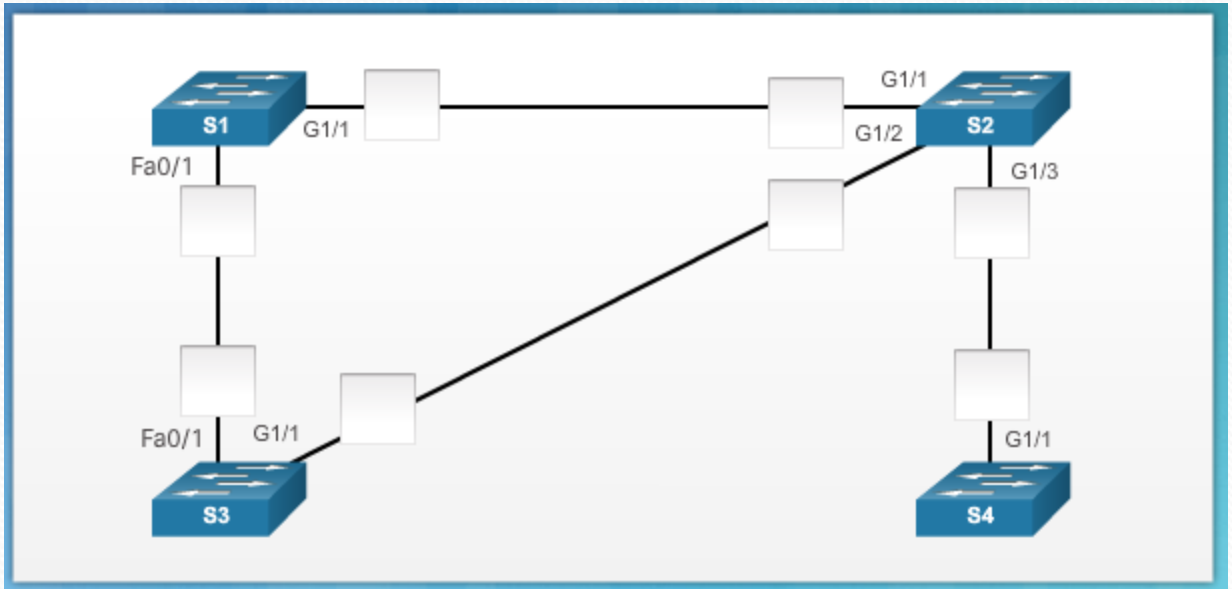
# Exercise

- What will be the RSTP port role names for each switch ports in the topology?

RP Root Port

DP Designated Port

AP Alternate Port




| | Priority | MAC Address |
|---|---|---|
| S1 | 32769 | 000A00111111 |
| S2 | 24577 | 000A00222222 |
| S3 | 32769 | 000A00333333 |
| S4 | 32769 | 000A00444444 |

# Varieties of Spanning Tree Protocols

# Types of Spanning Tree Protocols

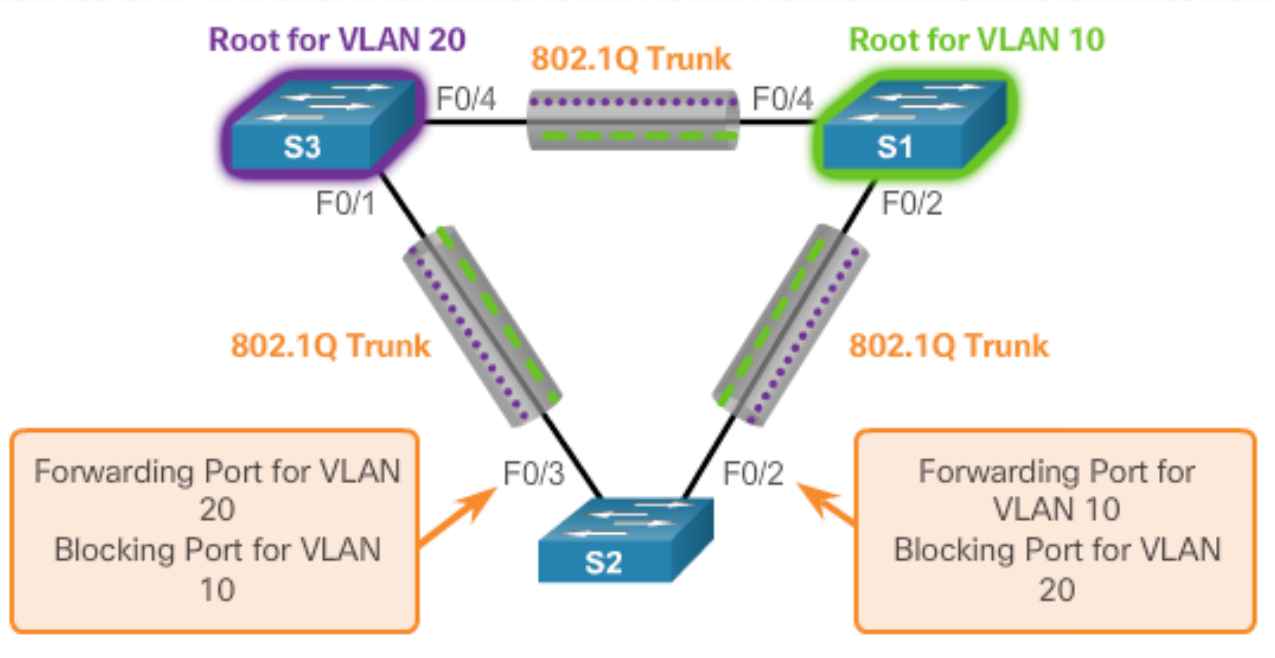
- Several varieties of spanning tree protocols have emerged since the original IEEE 802.1D
  - PVST+: A Cisco enhancement of STP that provides a separate 802.1D spanning-tree instance for each VLAN configured in the network
  - 802.1D-2004: An updated bridging and STP standard
  - 802.1w (RSTP): Improves convergence over 1998 STP by adding roles to ports and enhancing BPDU exchanges
  - Rapid PVST+: A Cisco enhancement of RSTP using PVST+.
  - 802.1s (MSTP): Maps multiple VLANs into the same spanning-tree instance

# Characteristics of Spanning Tree Protocols

| Protocol | Standard | Resources Needed | Convergence | Tree Calculation |
|---|---|---|---|---|
| STP | 802.1D | Low | Slow | All VLANs |
| PVST+ | Cisco | High | Slow | Per VLAN |
| RSTP | 802.1w | Medium | Fast | All VLANs |
| Rapid PVST+ | Cisco | Very high | Fast | Per VLAN |
| MSTP | 802.1s, Cisco | Medium or high | Fast | Per Instance |

# Overview of PVST+

- Cisco developed PVST+ to run an independent instance of the Cisco implementation of IEEE 802.1D for each VLAN in the network
- With PVST+, it is possible for one trunk port on a switch to block for a VLAN while forwarding for other VLANs



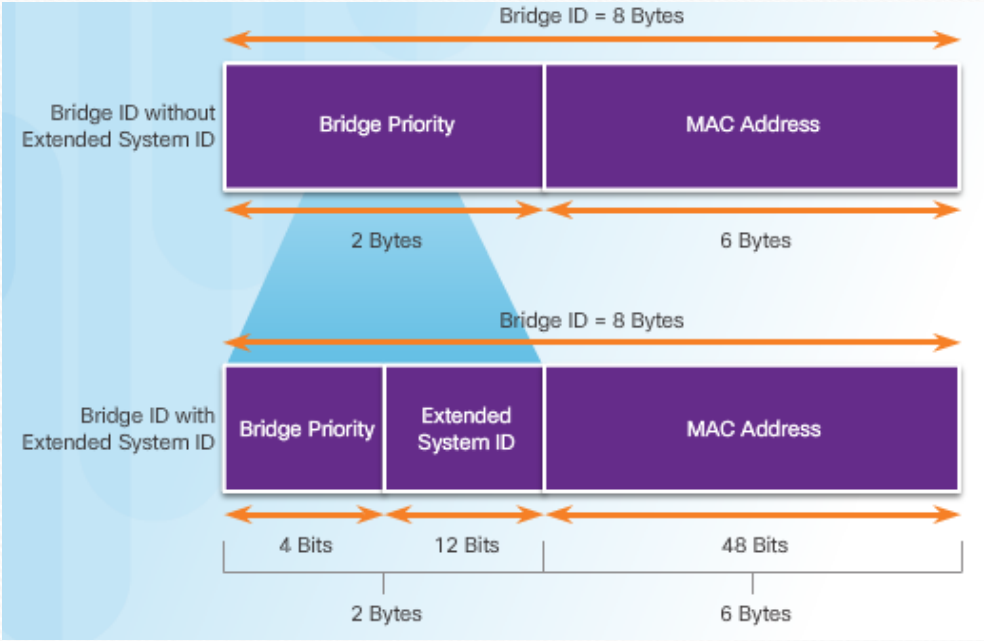
# Port States and PVST+ Operation

- STP and PVST+ use five port states consisting of Blocking, Listening, Learning, Forwarding, and Disabled

| | Port State | | | | |
|---|---|---|---|---|---|
| **Operation Allowed** | **Blocking** | **Listening** | **Learning** | **Forwarding** | **Disabled** |
| Can receive and process BPDUs | YES | YES | YES | YES | NO |
| Can forward data frames received on interface | NO | NO | NO | YES | NO |
| Can forward data frames switched from another interface | NO | NO | NO | YES | NO |
| Can learn MAC addresses | NO | NO | YES | YES | NO |

# Extended System ID and PVST+ Operation

- Extended system ID ensures switches have unique BIDs for each VLAN




- To manipulate the root-bridge election, assign a lower priority to the desired root bridge switch for the VLAN(s).

# Overview of Rapid PVST+

- Rapid PVST+ is the Cisco implementation of per-VLAN RSTP
- RSTP can achieve much faster convergence
- If a port is configured to be an alternate port or a backup port, it can immediately change to a forwarding state without waiting for the network to converge

# RSTP BPDU

- RSTP uses type 2, version 2 BPDUs and populates the flag byte in a slightly different manner than in the original 802.1D

**RSTP Version 2 BPDU**

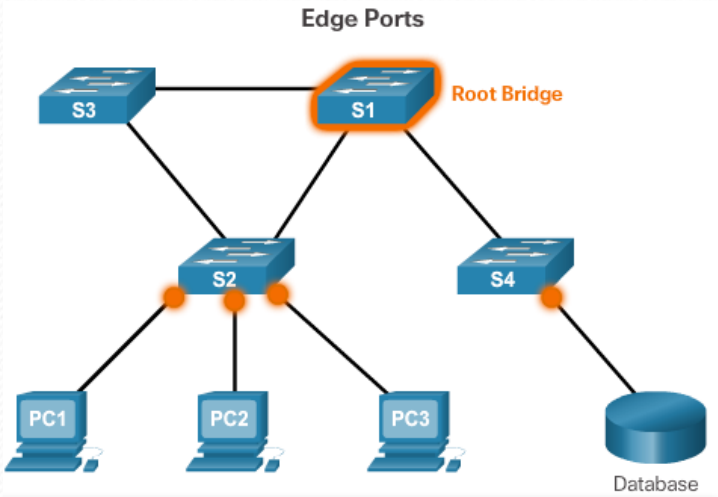
| Field | Byte Length |
|---|---|
| Protocol ID=0x0000 | 2 |
| Protocol Version ID=0x02 | 1 |
| BPDU Type=0X02 | 1 |
| Flags | 1 |
| Root ID | 8 |
| Root Path Cost | 4 |
| Bridge ID | 8 |
| Port ID | 2 |
| Message Age | 2 |
| Max Age | 2 |
| Hello Time | 2 |
| Forward Delay | 2 |

**Flag Field**

| Field Bit | Bit |
|---|---|
| Topology Change | 0 |
| Proposal | 1 |
| Port Role<br>Unknown Port<br>Alternate or Backup Port<br>Root Port<br>Designated Port | 2-3<br>00<br>01<br><br>10<br>11 |
| Learning | 4 |
| Forwarding | 5 |
| Agreement | 6 |
| Topology Change Acknowledgment | 7 |

# Edge Ports

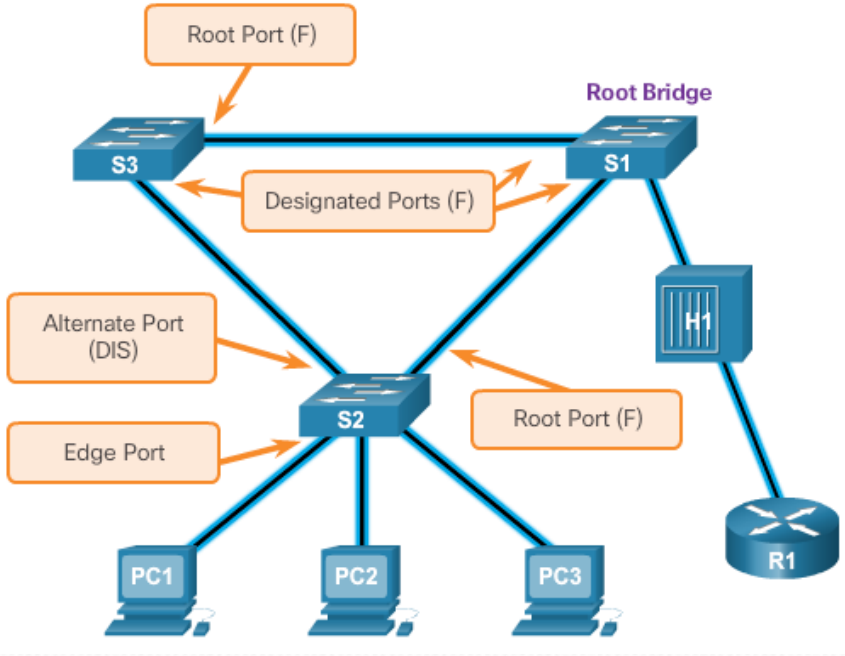
- RSTP edge port is a switch port that is never intended to be connected to another switch.
- It immediately transitions to the forwarding state when enabled



# Link Types

- Point-to-Point - A port operating in full-duplex mode typically connects a switch to a switch and is a candidate for a rapid transition to a forwarding state
- Shared - A port operating in half-duplex mode connects a switch to a legacy hub that attaches multiple devices.

- RSTP must determine the port role:
- Root ports and Alternate (backup) ports do not use the link-type parameter in most cases.
- Designated ports make the most use of the link-type parameter and transition to the forwarding state if the link-type parameter is set to point-to-point.



# Summary

- Troubleshooting VTP can also involve solving errors with incompatible VTP versions & incorrectly configured domain names/passwords
- When troubleshooting DTP, problems can be related to trunk mode mismatches, allowed VLANS on a trunk, and native VLAN mismatches
- SVIs is a method of inter-VLAN routing on Layer 3 switching. An SVI with appropriate IP addressing is configured for each VLAN
- Another method of Layer 3 inter-VLAN routing is using routed ports. A routed port is a physical port that acts similarly to an interface on a router
- Troubleshooting inter-VLAN routing with a router or a Layer 3 switch are similar. Common errors involve VLAN, trunk, Layer 3 interface, and IP address configurations

## Summary (continued)

- Problems that can result from a redundant Layer 2 network include broadcast storms, MAC database instability, and duplicate unicast frames. STP is a Layer 2 protocol that ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.
- STP sends BPDU frames for communication between switches. One switch is elected as the root bridge for each instance of spanning tree. An administrator can control this election by changing the bridge priority. Root bridges can be configured to enable spanning tree load balancing by VLAN or by a group of VLANs, depending on the spanning tree protocol used. STP then assigns a port role to each participating port using a path cost. The root path cost is equal to the sum of all the port costs along the path to the root bridge. A port cost is automatically assigned to each port; however, it can also be manually configured. Paths with the lowest cost become preferred, and all other redundant paths are blocked.
- PVST+ is the default configuration of IEEE 802.1D on Cisco switches. It runs one instance of STP for each VLAN. A newer, faster-converging spanning tree protocol, RSTP, can be implemented on Cisco switches on a per-VLAN basis in the form of Rapid PVST+. Multiple Spanning Tree (MST) is the Cisco implementation of Multiple Spanning Tree Protocol (MSTP), where one instance of spanning tree runs for a defined group of VLANs. Features such as PortFast and BPDU guard ensure that hosts in the switched environment are provided immediate access to the network without interfering with spanning tree operation.