Course CCNA 200-120

Bok 2 (CCENT/CCNA)

Part I: LAN Switching

Teacher: Magnus Colding

Part I: LAN Switching

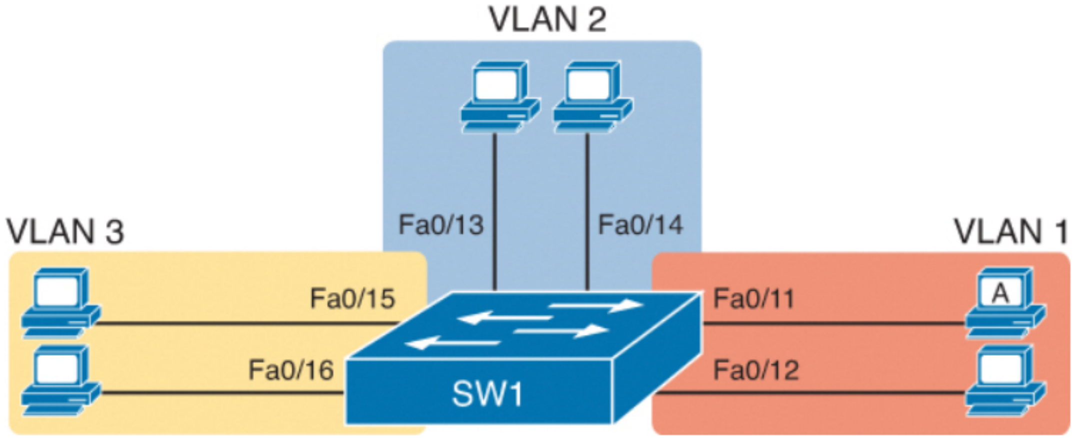


Figure 1-1. Small Ethernet LAN with VLANs

Step 1. Determine the VLAN in which the frame should be forwarded, as follows:

A. If the frame arrives on an access interface, use the interface's access VLAN.

B. If the frame arrives on a trunk interface, use the VLAN listed in the frame's trunking header.

Step 2. Add the source MAC address to the MAC address table, with incoming interface and VLAN ID.

Step 3. Look for the destination MAC address of the frame in the MAC address table, but only for entries in the VLAN identified at Step 1. Follow one of the next steps depending on whether the destination MAC is found:

A. Found: Forward the frame out the only interface listed in the matched address table entry.

B. Not found: Flood the frame out all other access ports in that same VLAN and out all trunk ports that list this VLAN as fully supported (active, in the allowed list, not pruned, STP forwarding).

Part I: LAN Switching

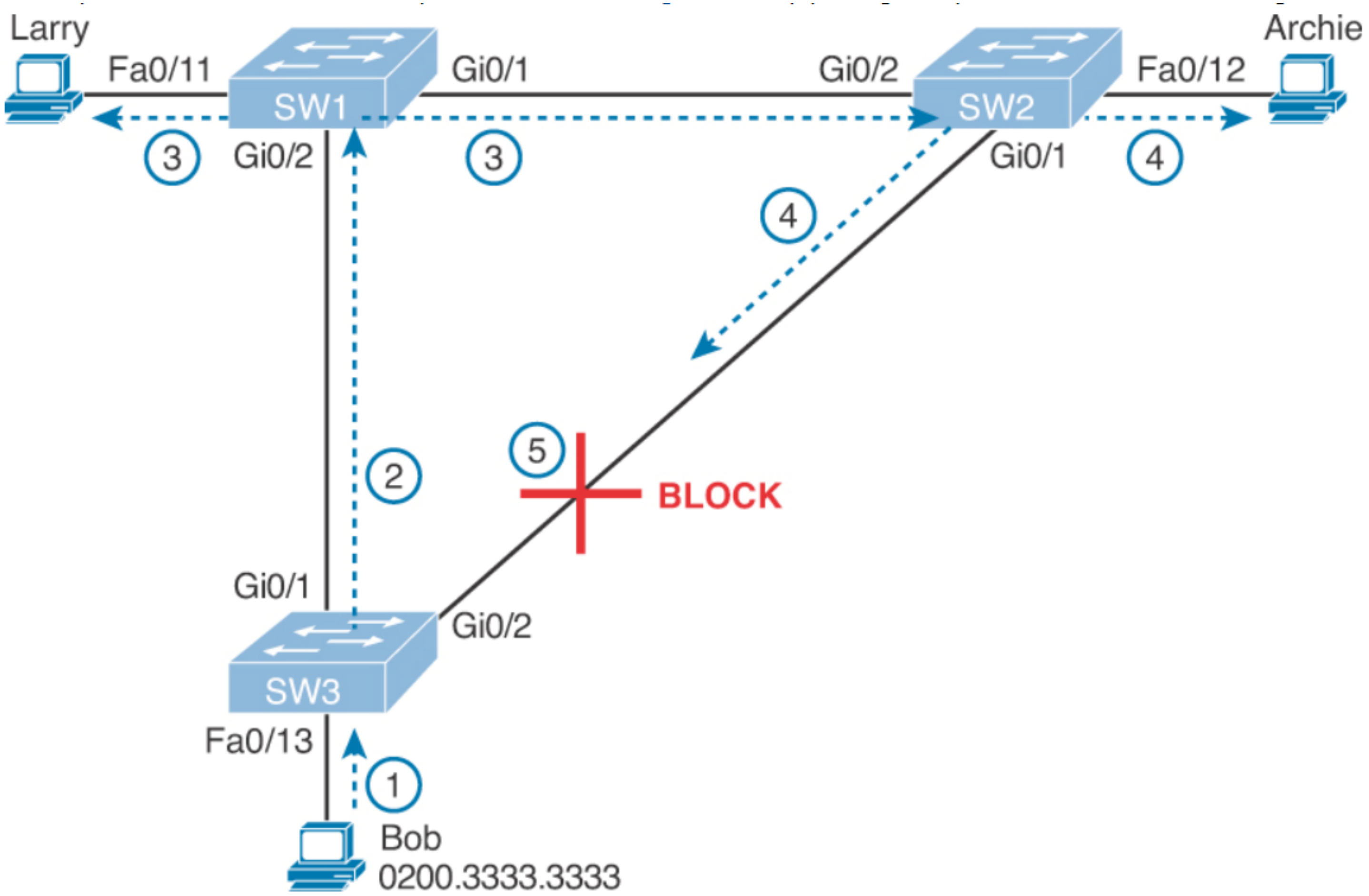
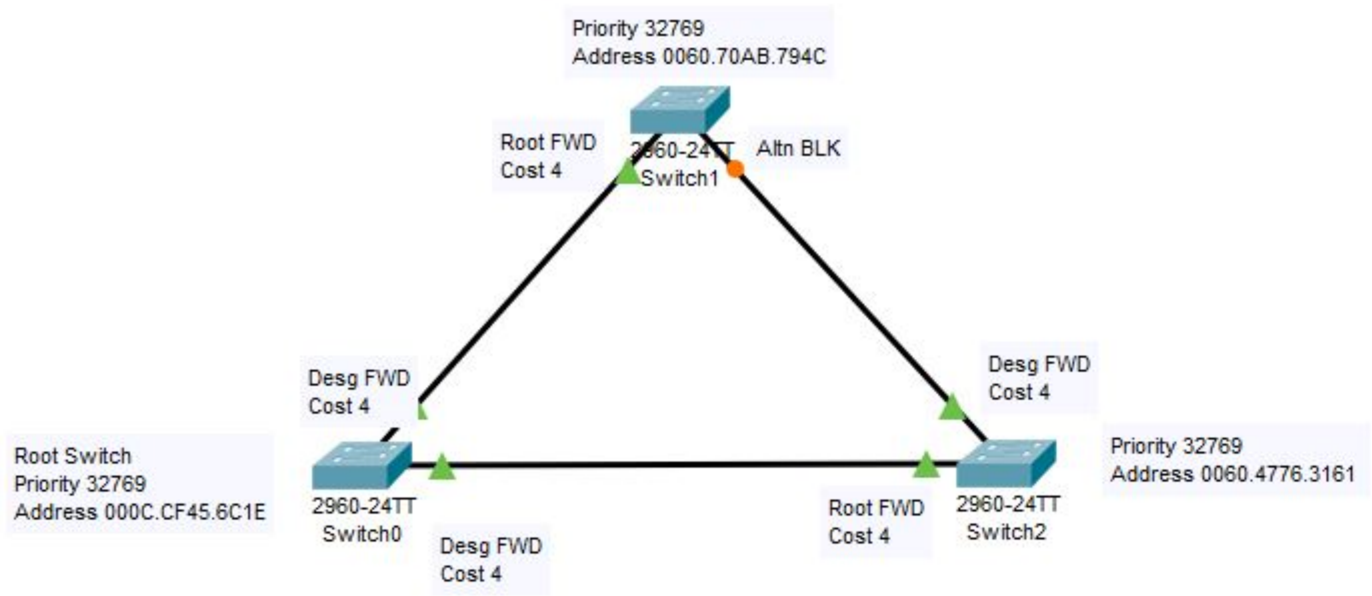


Figure 1-4. What STP Does: Blocks a Port to Break the Loop

Part I: LAN Switching



Part I: LAN Switching

Table 1-3. STP: Reasons for Forwarding or Blocking

Characterization of Port	STP State	Description
All the root switch's ports	Forwarding	The root switch is always the designated switch on all connected segments.
Each nonroot switch's root port	Forwarding	The port through which the switch has the least cost to reach the root switch (lowest root cost).
Each LAN's designated port	Forwarding	The switch forwarding the hello on to the segment, with the lowest root cost, is the designated switch for that segment.
All other working ports	Blocking	The port is not used for forwarding user frames, nor are any frames received on these interfaces considered for forwarding.

Part I: LAN Switching

Table 1-4. Fields in the STP Hello BPDU

Field	Description
Root bridge ID	The bridge ID of the switch the sender of this hello currently believes to be the root switch
Sender's bridge ID	The bridge ID of the switch sending this hello BPDU
Sender's root cost	The STP cost between this switch and the current root
Timer values on the root switch	Includes the hello timer, MaxAge timer, and forward delay timer

Part I: LAN Switching

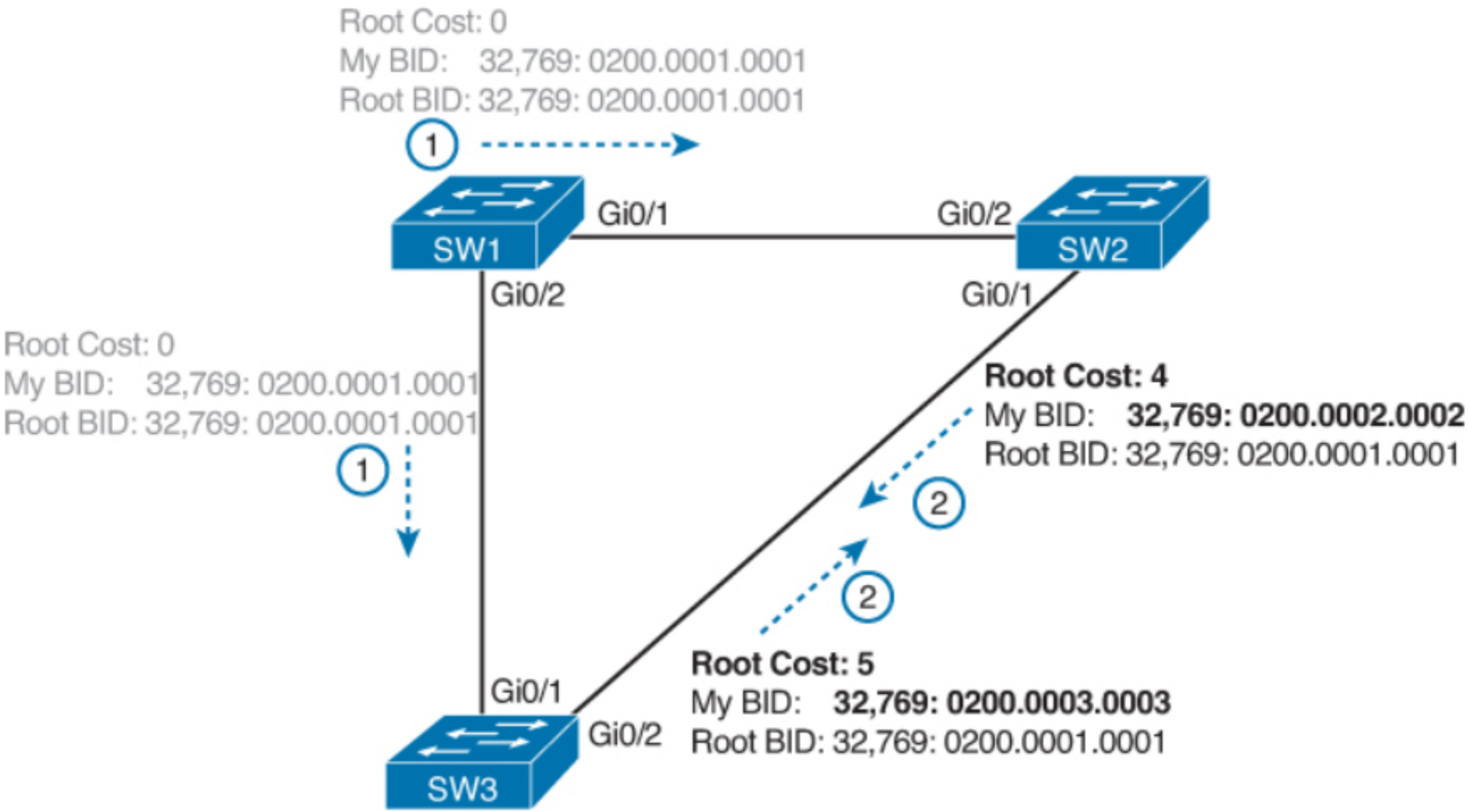


Figure 1-6. SW1 Wins the Election

Part I: LAN Switching

Table 1-6. Default Port Costs According to IEEE

Ethernet Speed	IEEE Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

Part I: LAN Switching

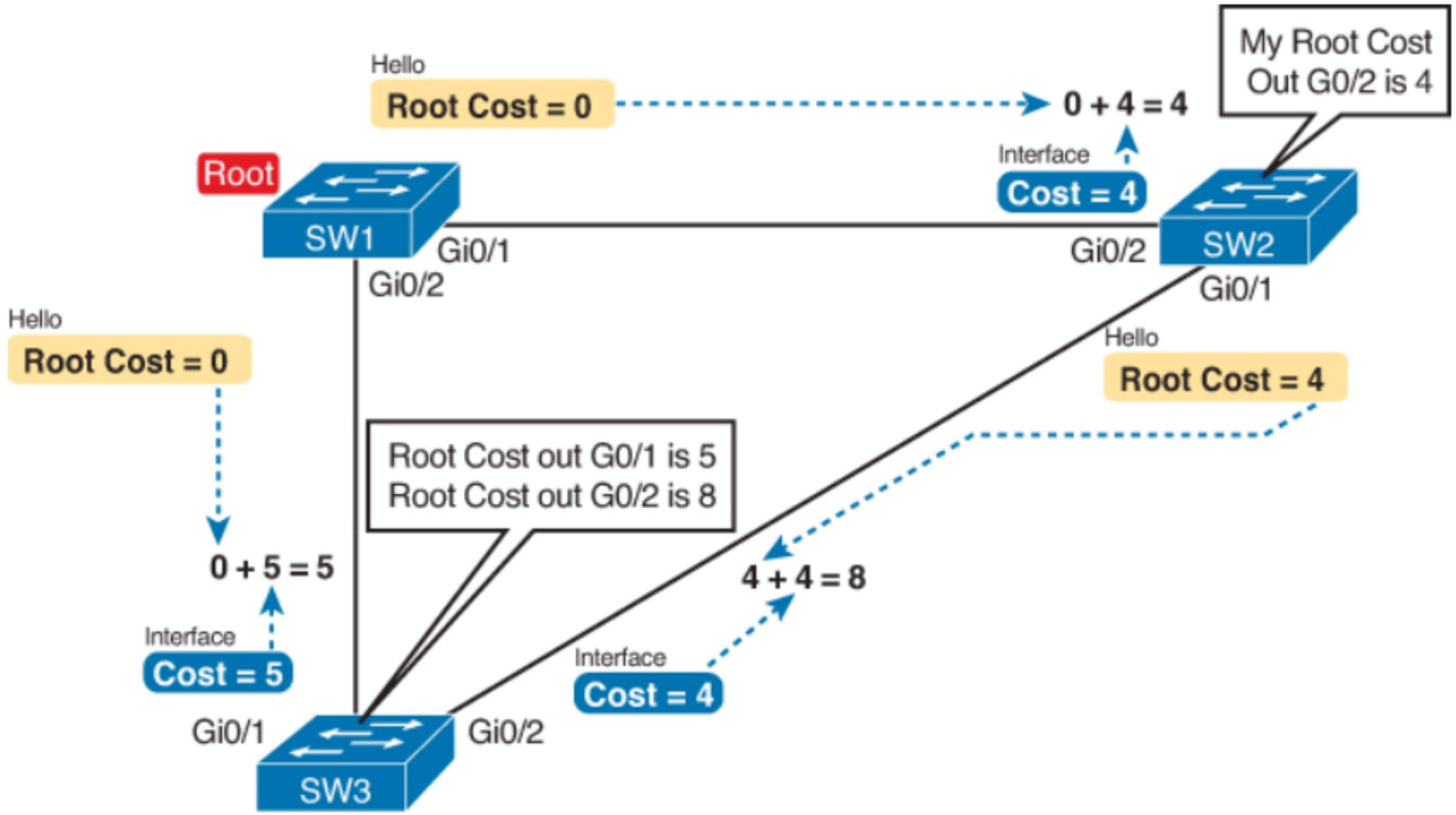


Figure 1-8. How STP Actually Calculates the Cost from SW3 to the Root

Part I: LAN Switching

Table 1-7. STP Timers

Timer	Description	Default Value
Hello	The time period between hellos created by the root.	2 seconds
MaxAge	How long any switch should wait, after ceasing to hear hellos, before trying to change the STP topology.	10 times hello
Forward delay	Delay that affects the process that occurs when an interface changes from blocking state to forwarding state. A port stays in an interim listening state, and then an interim learning state, for the number of seconds defined by the forward delay timer.	15 seconds

Part I: LAN Switching

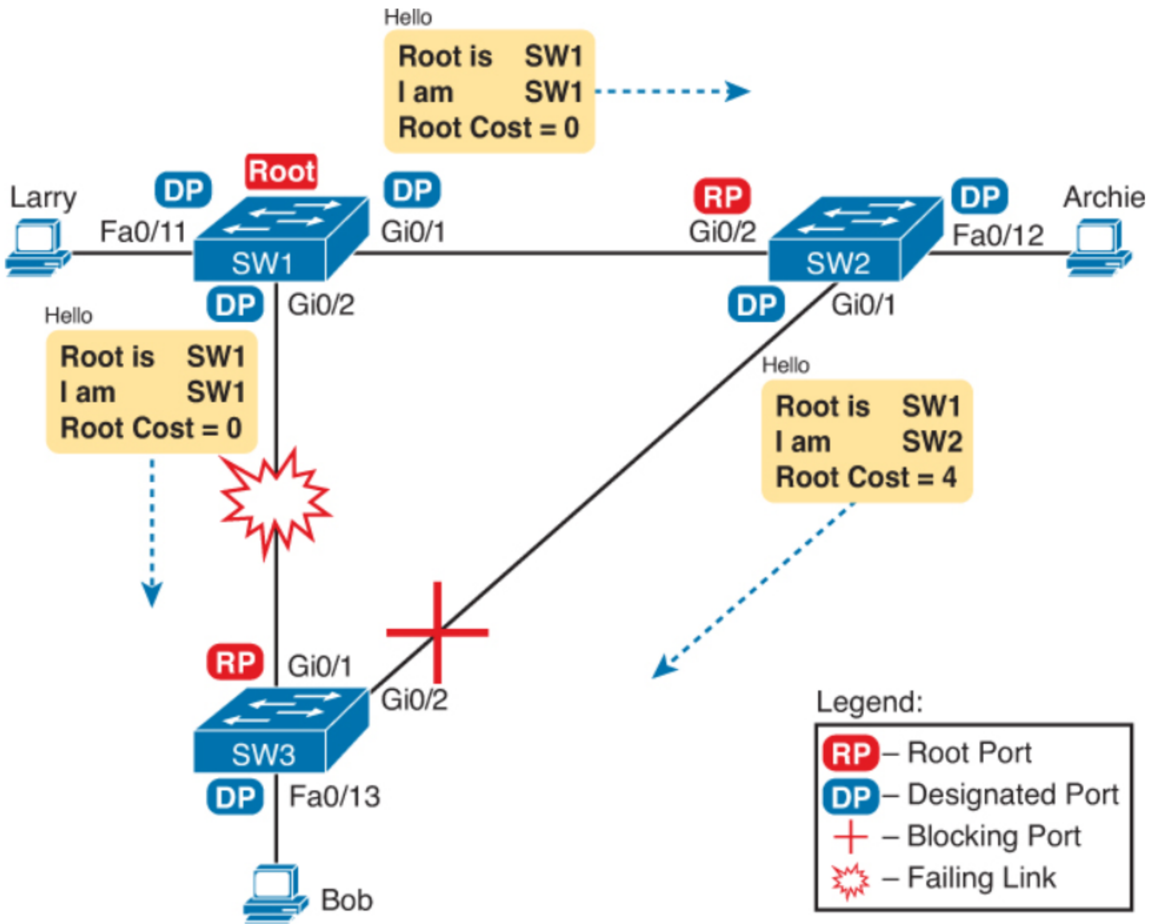


Figure 1-9. Initial STP State Before SW1-SW3 Link Fails

Part I: LAN Switching

Table 1-8. IEEE 802.1D Spanning-Tree States

State	Forwards Data Frames?	Learns MACs Based on Received Frames?	Transitory or Stable State?
Blocking	No	No	Stable
Listening	No	No	Transitory
Learning	No	Yes	Transitory
Forwarding	Yes	Yes	Stable
Disabled	No	No	Stable

Part I: LAN Switching

Optional STP Features

STP has been around for more than 30 years, first being used even before the IEEE took over the development of Ethernet standards from Xerox and other vendors. The IEEE first standardized STP as IEEE 802.1D back in the 1980s. Cisco switches today still use STP. And other than changes to the default cost values, the description of STP in this chapter so far works like the original STP as created all those years ago.

Even with such an amazingly long life, STP has gone through several changes over these decades, some small, some large. For instance, Cisco added proprietary features to make improvements to STP. In some cases, the IEEE added these same improvements, or something like them, to later IEEE standards, whether as a revision of the 802.1D standard or as an additional standard. And STP has gone through one major revision that improves convergence, called the *Rapid Spanning Tree Protocol* (RSTP), as originally defined in IEEE 802.1w.

This final of three major sections of this chapter briefly discusses the basics of several of these optional features that go beyond the base 802.1D STP concepts, including EtherChannel, PortFast, and BPDU Guard.

Part I: LAN Switching

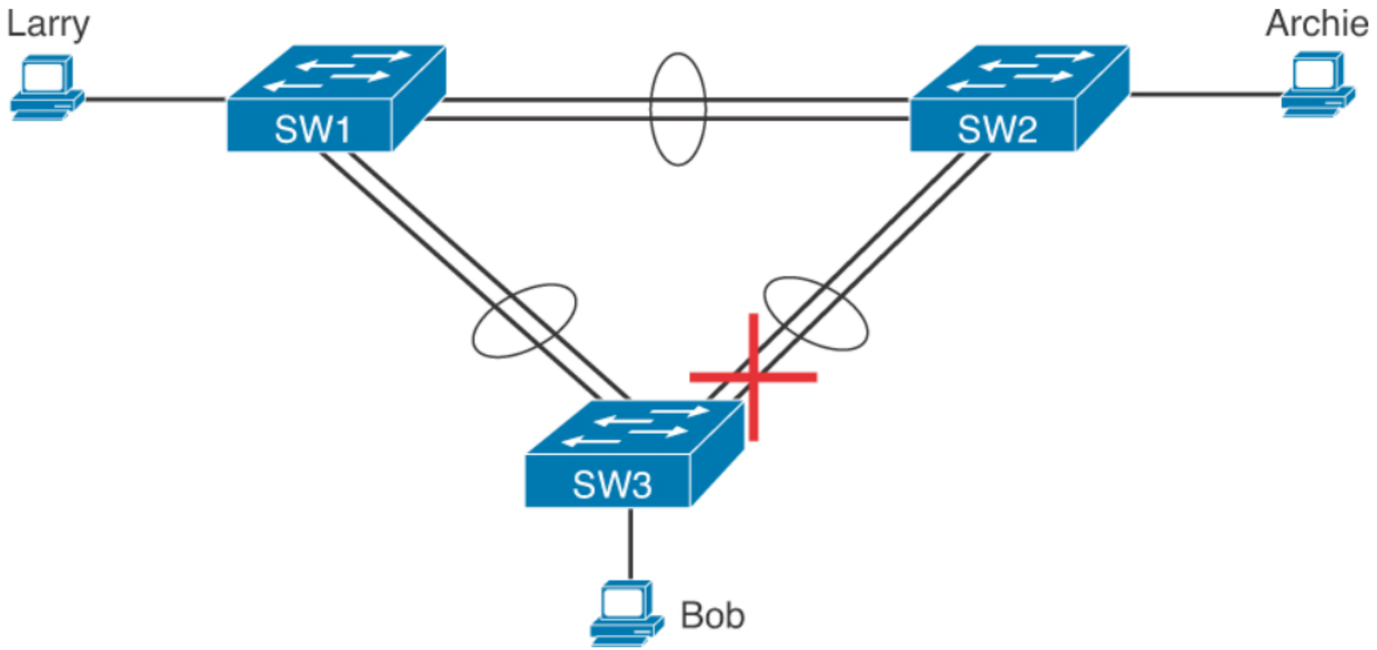


Figure 1-10. Two-Segment EtherChannels Between Switches

Part I: LAN Switching

PortFast

PortFast allows a switch to immediately transition from blocking to forwarding, bypassing listening and learning states. However, the only ports on which you can safely enable PortFast are ports on which you know that no bridges, switches, or other STP-speaking devices are connected. Otherwise, using PortFast risks creating loops, the very thing that the listening and learning states are intended to avoid.

PortFast is most appropriate for connections to end-user devices. If you turn on PortFast on ports connected to end-user devices, when an end-user PC boots, the switch port can move to an STP forwarding state and forward traffic as soon as the PC NIC is active. Without PortFast, each port must wait while the switch confirms that the port is a DP, and then wait while the interface sits in the temporary listening and learning states before settling into the forwarding state.

BPDU Guard

STP opens up the LAN to several different types of possible security exposures. For example:

- An attacker could connect a switch to one of these ports, one with a low STP priority value, and become the root switch. The new STP topology could have worse performance than the desired topology.
- The attacker could plug into multiple ports, into multiple switches, become root, and actually forward much of the traffic in the LAN. Without the networking staff realizing it, the attacker could use a LAN analyzer to copy large numbers of data frames sent through the LAN.
- Users could innocently harm the LAN when they buy and connect an inexpensive consumer LAN switch (one that does not use STP). Such a switch, without any STP function, would not choose to block any ports and would likely cause a loop.

The Cisco BPDU Guard feature helps defeat these kinds of problems by disabling a port if any BPDUs are received on the port. So, this feature is particularly useful on ports that should be used only as an access port and never connected to another switch.

In addition, the BPDU Guard feature helps prevent problems with PortFast. PortFast should be enabled only on access ports that connect to user devices, not to other LAN switches. Using BPDU Guard on these same ports makes sense because if another switch connects to such a port, the local switch can disable the port before a loop is created.

Part I: LAN Switching

Rapid STP (IEEE 802.1w)

As mentioned earlier in this chapter, the IEEE defines STP in the 802.1D IEEE standard. The IEEE has improved the 802.1D protocol with the definition of Rapid Spanning Tree Protocol (RSTP), as defined in standard 802.1w.

RSTP (802.1w) works just like STP (802.1D) in several ways:

- It elects the root switch using the same parameters and tiebreakers.
- It elects the root port on nonroot switches with the same rules.
- It elects designated ports on each LAN segment with the same rules.
- It places each port in either forwarding or blocking sate, although RSTP calls the blocking state the discarding state.

RSTP can be deployed alongside traditional 802.1D STP switches, with RSTP features working in switches that support it, and traditional 802.1D STP features working in the switches that support only STP.

With all these similarities, you might be wondering why the IEEE bothered to create RSTP in the first place. The overriding reason is convergence. STP takes a relatively long time to converge (50 seconds with the default settings). RSTP improves network convergence when topology changes occur, usually converging within a few seconds, or in poor conditions, in about 10 seconds.

In real life, most enterprise LANs use designs that require STP, and most of those prefer to use RSTP because of the better convergence. However, with the current exams, Cisco defers the deeper discussion of RSTP until the CCNP Switch exam and the CCNP certification. For those of you working with LAN switching for work, make sure to look further at 802.1w/RSTP and how to implement it in your switches.

Part I: LAN Switching

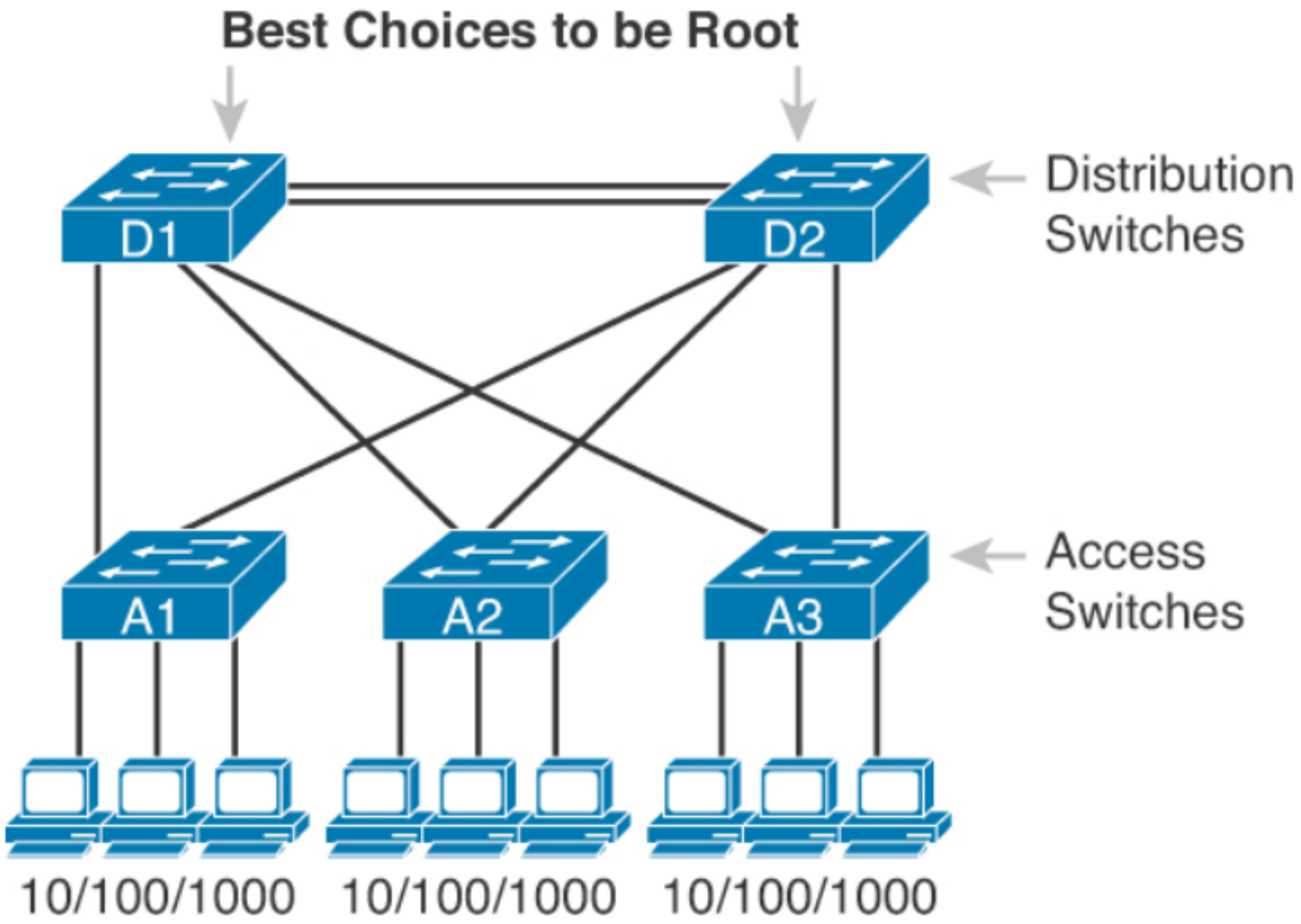


Figure 2-1. Typical Configuration Choice: Making Distribution Switch Be Root

Part I: LAN Switching

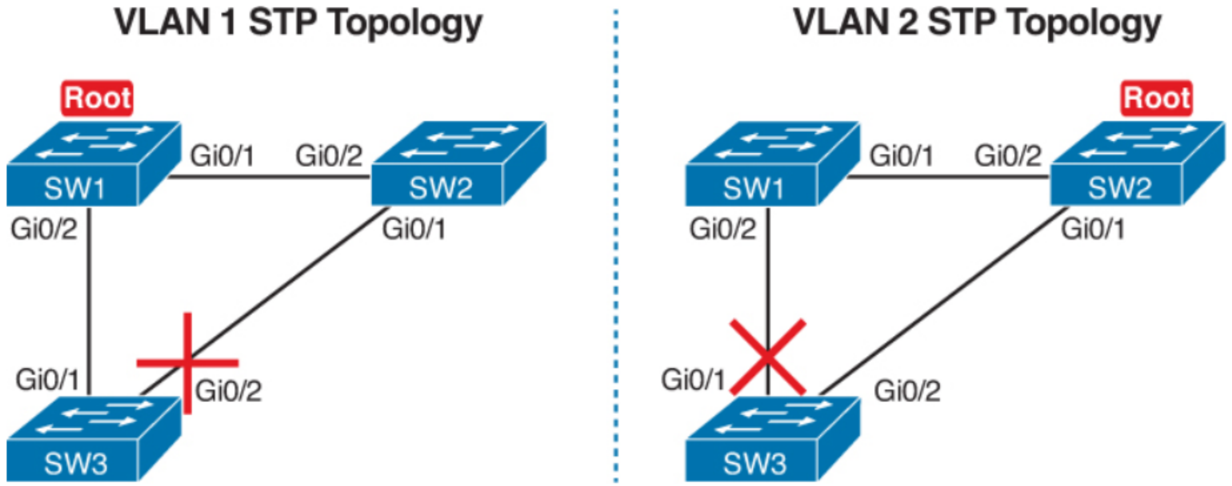


Figure 2-2. Load Balancing with PVST+

Part I: LAN Switching

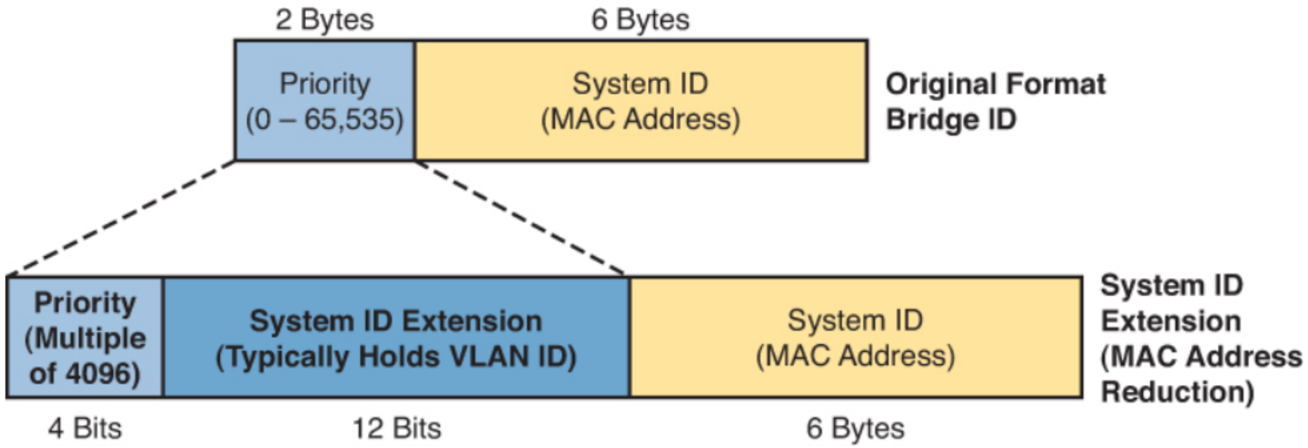


Figure 2-3. STP System ID Extension

Part I: LAN Switching

Table 2-2. STP Defaults and Configuration Options

Setting	Default	Command(s) to Change Default
BID priority	Base: 32,768	**spanning-tree vlan** *vlan-id* **root** {**primary** | **secondary**} **spanning-tree vlan** *vlan-id* **priority** *priority*
Interface cost	100 for 10 Mbps 19 for 100 Mbps 4 for 1 Gbps 2 for 10 Gbps	**spanning-tree vlan** *vlan-id* **cost** *cost*
PortFast	Not enabled	**spanning-tree portfast**
BPDU Guard	Not enabled	**spanning-tree bpduguard enable**

Part I: LAN Switching

Example 2-6. Enabling PortFast and BPDU Guard on One Interface

Click here to view code image

```
SW3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)# interface fastEthernet 0/4
SW3(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/4 but will only
 have effect when the interface is in a non-trunking mode.

SW3(config-if)# spanning-tree bpduguard ?
  disable  Disable BPDU guard for this interface
  enable   Enable BPDU guard for this interface

SW3(config-if)# spanning-tree bpduguard enable
SW3(config-if)# ^Z
SW3#
*Mar  1 07:53:47.808: %SYS-5-CONFIG_I: Configured from console by console
SW3# show running-config interface f0/4
Building configuration...

Current configuration : 138 bytes
!
interface FastEthernet0/4
 switchport access vlan 104
 spanning-tree portfast
 spanning-tree bpduguard enable
end

SW3# show spanning-tree interface fastethernet0/4 portfast
VLAN0104            enabled
```

Part I: LAN Switching

- STP Tiebreakers when choosing Root Port

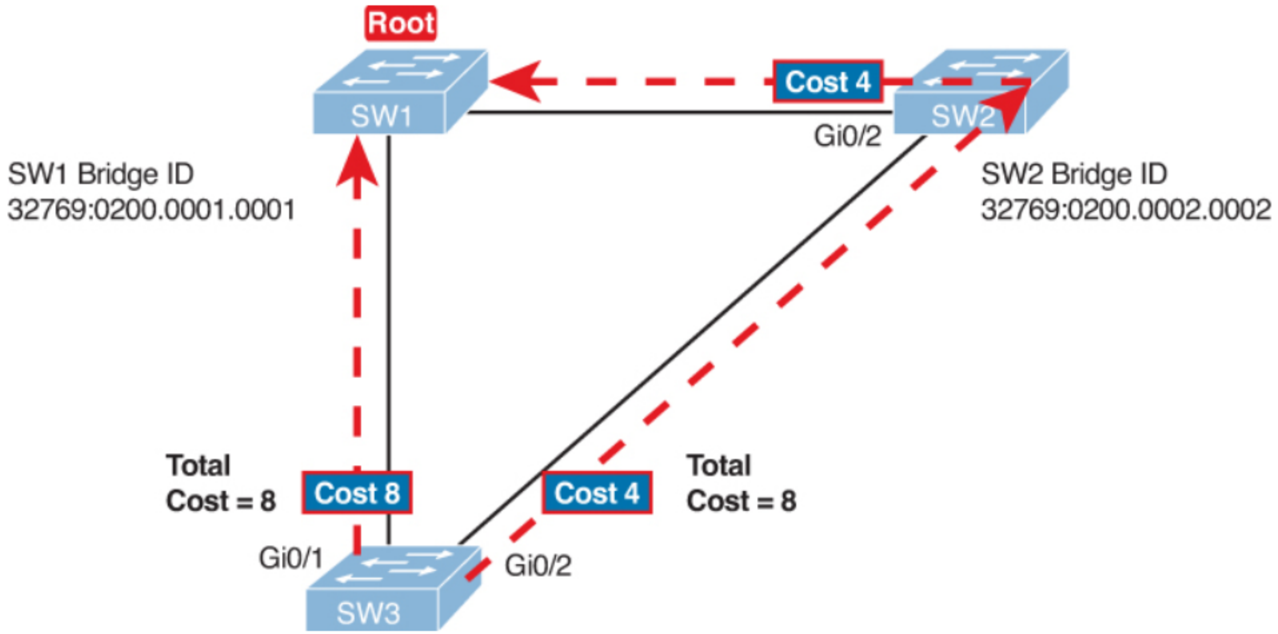


Figure 2-8. SW3's Root Cost Calculation Ends in a Tie

1) Local port with least cost path

2) Local port connect with neighbor lowest BID

Part I: LAN Switching

Key Topic

- Determining DP on each LAN segment

Step 1. For switches connected to the same LAN segment, the switch with the lowest cost to reach the root, as advertised in the hello they send onto the link, becomes the DP on that link.

Step 2. In case of a tie, among the switches that tied on cost, the switch with the lowest BID becomes the DP.

For example, consider Figure 2-10. This figure notes the root, RPs, and DPs and each switch's least cost to reach the root over its respective RP.

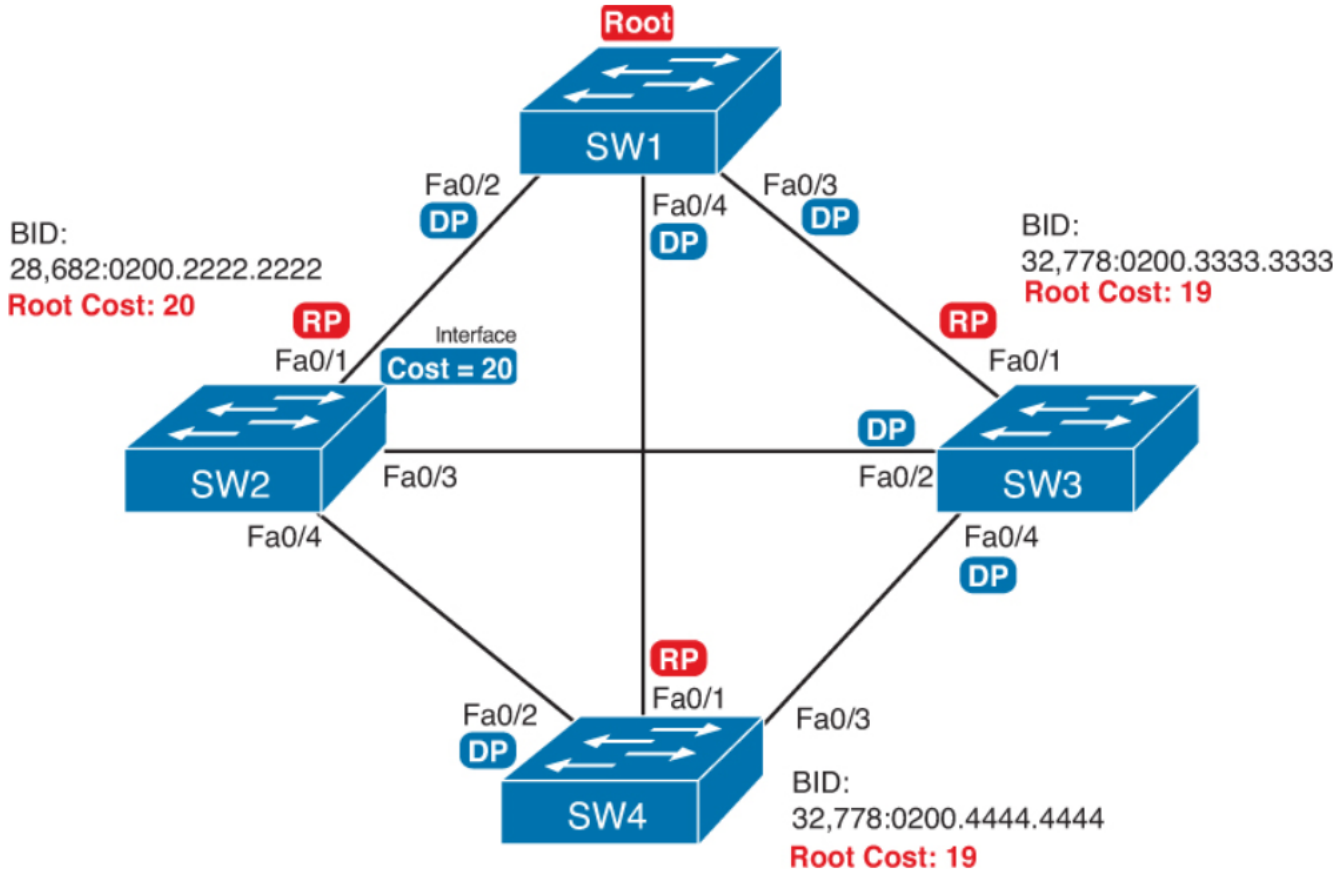


Figure 2-10. Picking the DPs

Part I: LAN Switching

Table 2-4. Chapter 2 Configuration Command Reference

Command	Description
spanning-tree mode { **pvst** | **rapid-pvst** | **mst** }	Global configuration command to set the STP mode.
spanning-tree vlan *vlan-number* **root primary**	Global configuration command that changes this switch to the root switch. The switch's priority is changed to the lower of either 24,576 or 4096 less than the priority of the current root bridge when the command was issued.
spanning-tree vlan *vlan-number* **root secondary**	Global configuration command that sets this switch's STP base priority to 28,672.
spanning-tree [**vlan** *vlan-id*] {**priority** *priority*}	Global configuration command that changes the bridge priority of this switch for the specified VLAN.
spanning-tree [**vlan** *vlan-number*] **cost** *cost*	Interface subcommand that changes the STP cost to the configured value.
spanning-tree [**vlan** *vlan-number*] **port-priority** *priority*	Interface subcommand that changes the STP port priority in that VLAN (0 to 240, in increments of 16).
channel-group *channel-group-number* **mode** {**auto** | **desirable** | **active** | **passive** | **on**}	Interface subcommand that enables EtherChannel on the interface.
spanning-tree portfast	Interface subcommand that enables PortFast on the interface.
spanning-tree bpduguard enable	Interface subcommand to enable BPDU Guard on an interface

Part I: LAN Switching

spanning-tree portfast default	Global command that changes the switch default for PortFast on access interfaces from disabled to enabled.
spanning-tree portfast bpduguard default	Global command that changes the switch default for BPDU Guard on access interfaces from disabled to enabled.
spanning-tree portfast disable	Interface subcommand that disables PortFast on the interface.
spanning-tree bpduguard disable	Interface subcommand to disable BPDU Guard on an interface

Part I: LAN Switching

Table 2-5. Chapter 2 EXEC Command Reference

Command	Description
show spanning-tree	Lists details about the state of STP on the switch, including the state of each port
show spanning-tree *interface interface-id*	Lists STP information only for the specified port
show spanning-tree vlan *vlan-id*	Lists STP information for the specified VLAN
show spanning-tree [**vlan** *vlan-id*] **root**	Lists information about each VLAN's root or for just the specified VLAN
show spanning-tree [**vlan** *vlan-id*] **bridge**	Lists STP information about the local switch for each VLAN or for just the specified VLAN
debug spanning-tree events	Causes the switch to provide informational messages about changes in the STP topology
show spanning-tree interface *type number* **portfast**	Lists a one-line status message about PortFast on the listed interface
show etherchannel [*channel-group-number*] {**brief** | **detail** / **port** | **port-channel** | **summary**}	Lists information about the state of EtherChannels on this switch

Part I: LAN Switching

- PRACTICE with PT