Chapter 2: LAN Redundancy

Scaling Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 2

2.0 Introduction

2.1 Spanning Tree Concepts

2.2 Varieties of Spanning Tree Protocols

2.3 Spanning Tree Configuration

2.4 First-Hop Redundancy Protocols

2.5 Summary

Chapter 2: Objectives

- Describe the issues with implementing a redundant network.
- Describe IEEE 802.1D STP operation.
- Describe the different spanning tree varieties.
- Describe PVST+ operation in a switched LAN environment.
- Describe Rapid PVST+ operation in a switched LAN environment.
- Configure PVST+ in a switched LAN environment.
- Configure Rapid PVST+ in a switched LAN environment.
- Identify common STP configuration issues.
- Describe the purpose and operation of first hop redundancy protocols.
- Describe the different varieties of first hop redundancy protocols.
- Use Cisco IOS commands to verify HSRP and GLBP implementations.

2.1 Spanning Tree Concepts

Cisco | Networking Academy®
Mind Wide Open™

Purpose of Spanning Tree

Redundancy at OSI Layers 1 and 2

Multiple cabled paths between switches:

- Provide physical redundancy in a switched network.
- Improves the reliability and availability of the network.
- Enables users to access network resources, despite path disruption.

Considerations When Implementing Redundancy:

- **MAC database instability** - Instability in the content of the MAC address table results from copies of the same frame being received on different ports of the switch. Data forwarding can be impaired when the switch consumes the resources that are coping with instability in the MAC address table.
- **Broadcast storms** - Without some loop-avoidance process, each switch may flood broadcasts endlessly. This situation is commonly called a broadcast storm.
- **Multiple frame transmission** - Multiple copies of unicast frames may be delivered to destination stations. Many protocols expect to receive only a single copy of each transmission. Multiple copies of the same frame can cause unrecoverable errors.

Purpose of Spanning Tree

Issues with Layer 1 Redundancy: MAC Database Instability

- Ethernet frames do not have a time to live (TTL) attribute.
  - Frames continue to propagate between switches endlessly, or until a link is disrupted and breaks the loop.
  - Results in MAC database instability.
  - Can occur due to broadcast frames forwarding.
- If there is more than one path for the frame to be forwarded out, an endless loop can result.
  - When a loop occurs, it is possible for the MAC address table on a switch to constantly change with the updates from the broadcast frames, resulting in MAC database instability.

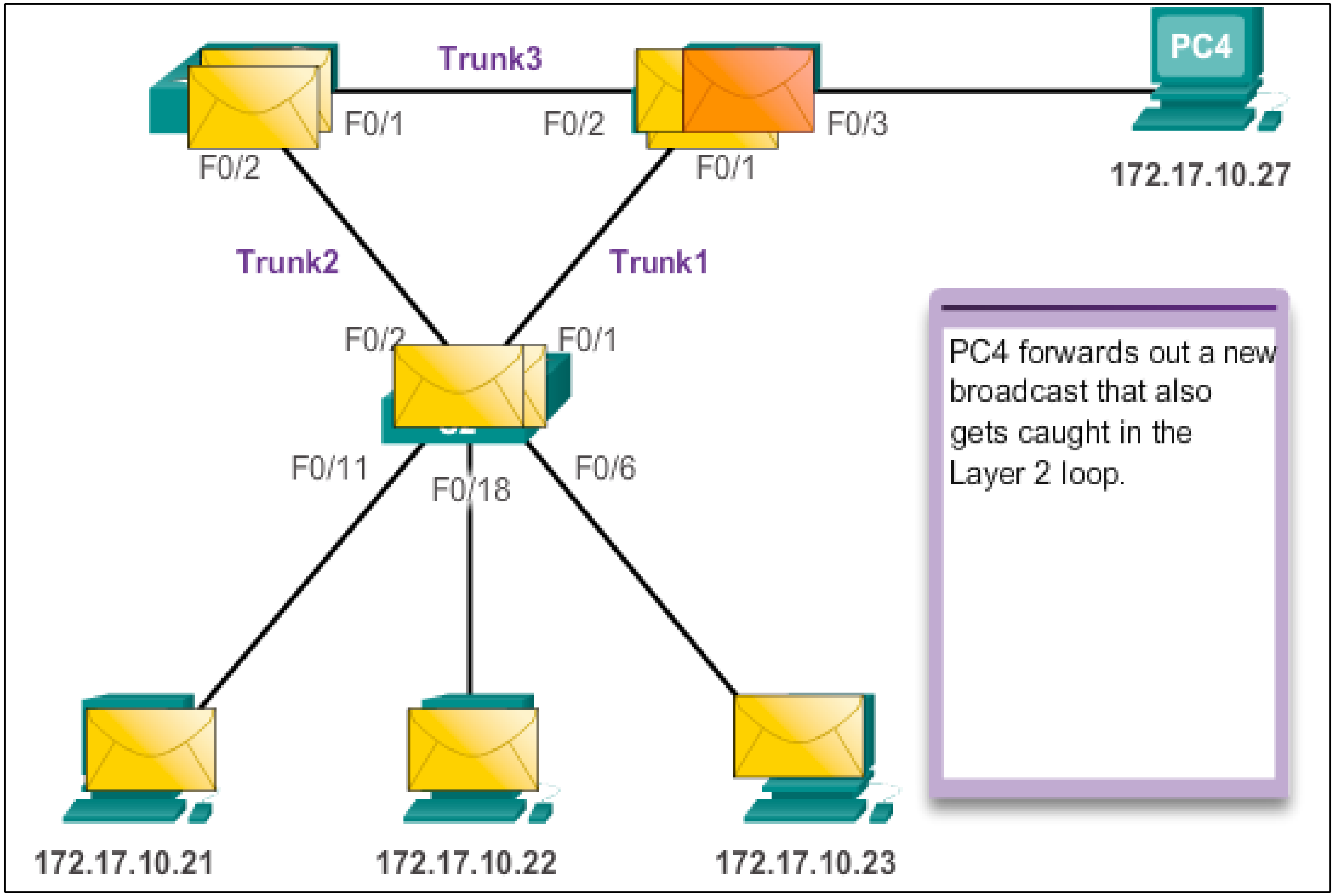
Purpose of Spanning Tree

Issues with Layer 1 Redundancy: 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. It is also known as denial of service
- A broadcast storm is inevitable on a looped network.
  - As more devices send broadcasts over the network, more traffic is caught within the loop; thus consuming more resources.
  - This eventually creates a broadcast storm that causes the network to fail.

Purpose of Spanning Tree

Issues with Layer 1 Redundancy: Broadcast Storms



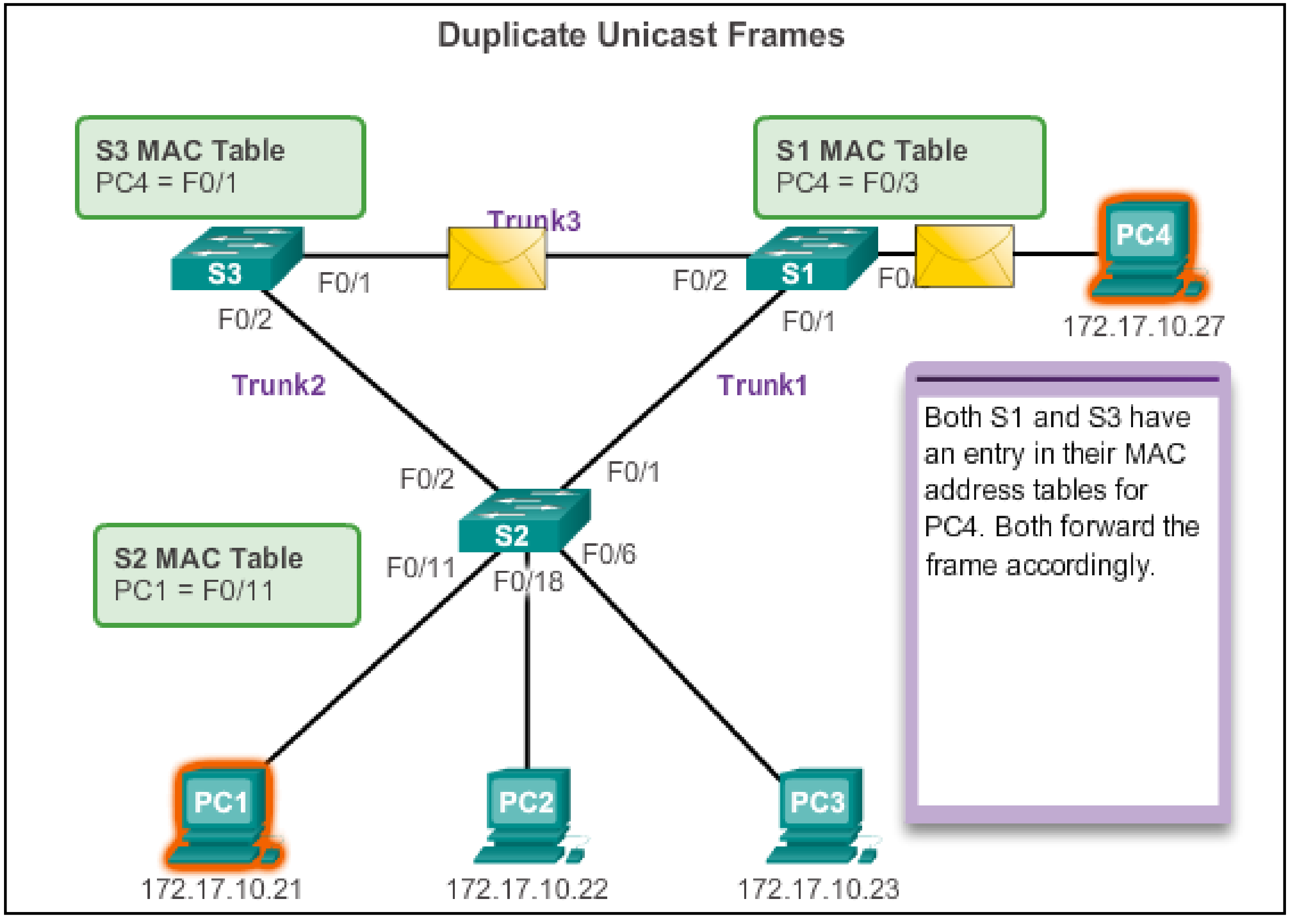
Purpose of Spanning Tree

Issues with Layer 1 Redundancy: Duplicate Unicast Frames

- Unicast frames sent onto a looped network can result in duplicate frames arriving at the destination device.
- Most upper layer protocols are not designed to recognize, or cope with, duplicate transmissions.
- Layer 2 LAN protocols, such as Ethernet, lack a mechanism to recognize and eliminate endlessly looping frames.

Purpose of Spanning Tree

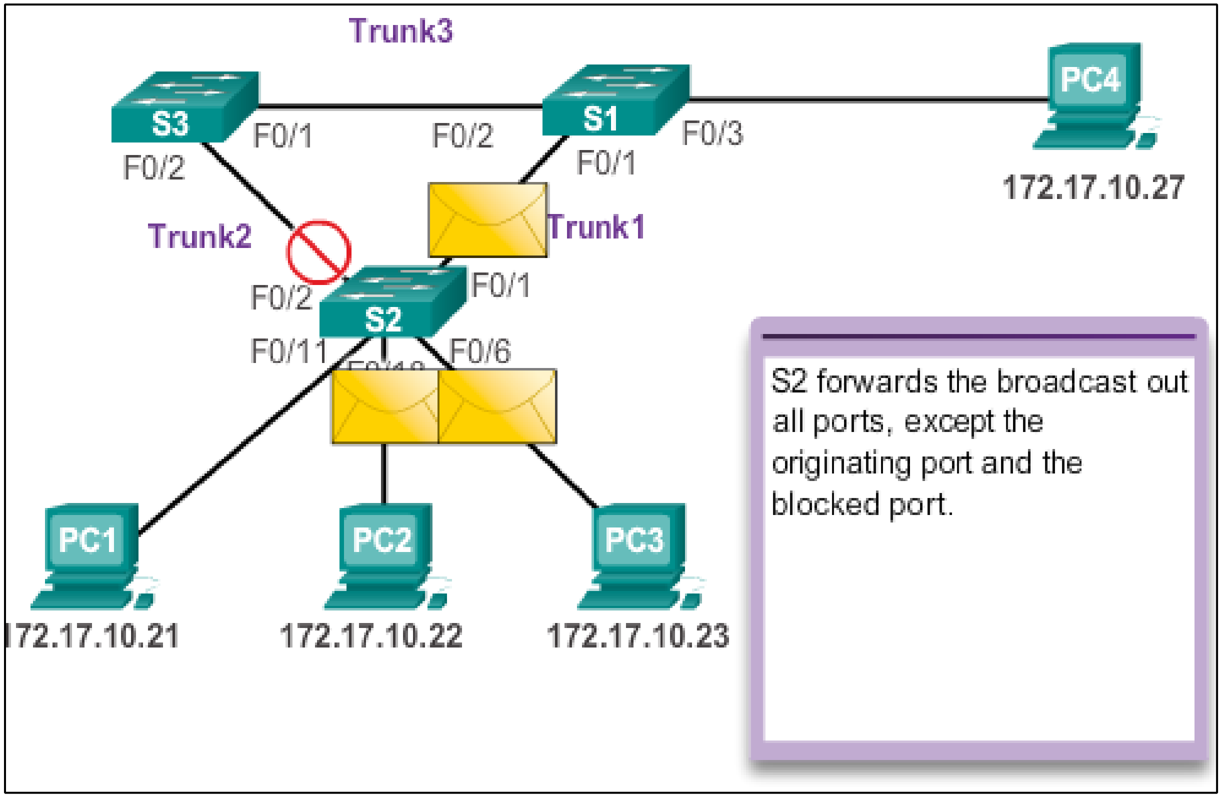
Issues with Layer 1 Redundancy: Duplicate Unicast Frames



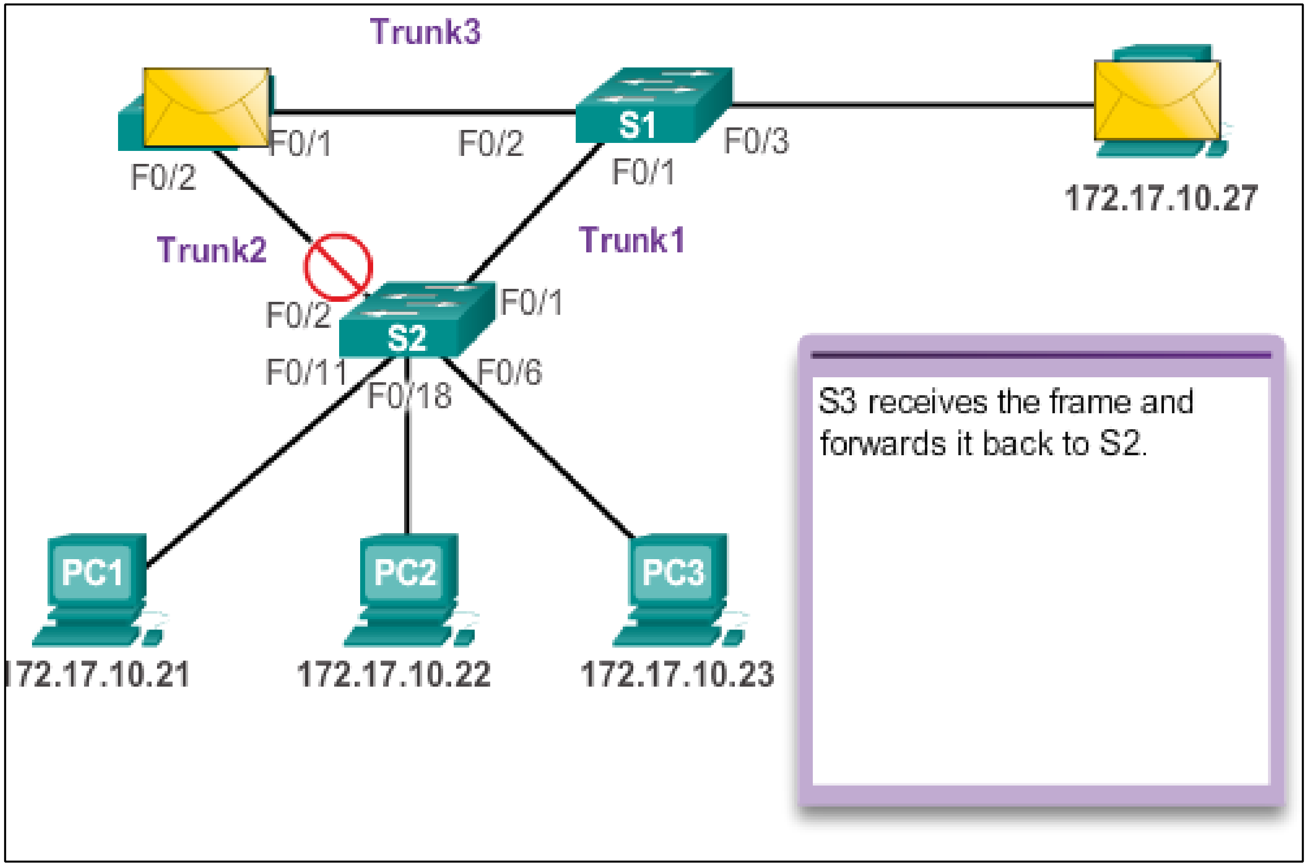
STP Operation
Spanning Tree Algorithm: Introduction

- 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.
- A port is considered blocked when user data is prevented from entering or leaving that port. This does not include bridge protocol data unit (BPDU) frames that are used by STP to prevent loops.
- The physical paths still exist to provide redundancy, but these paths are disabled to prevent the loops from occurring.
- If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

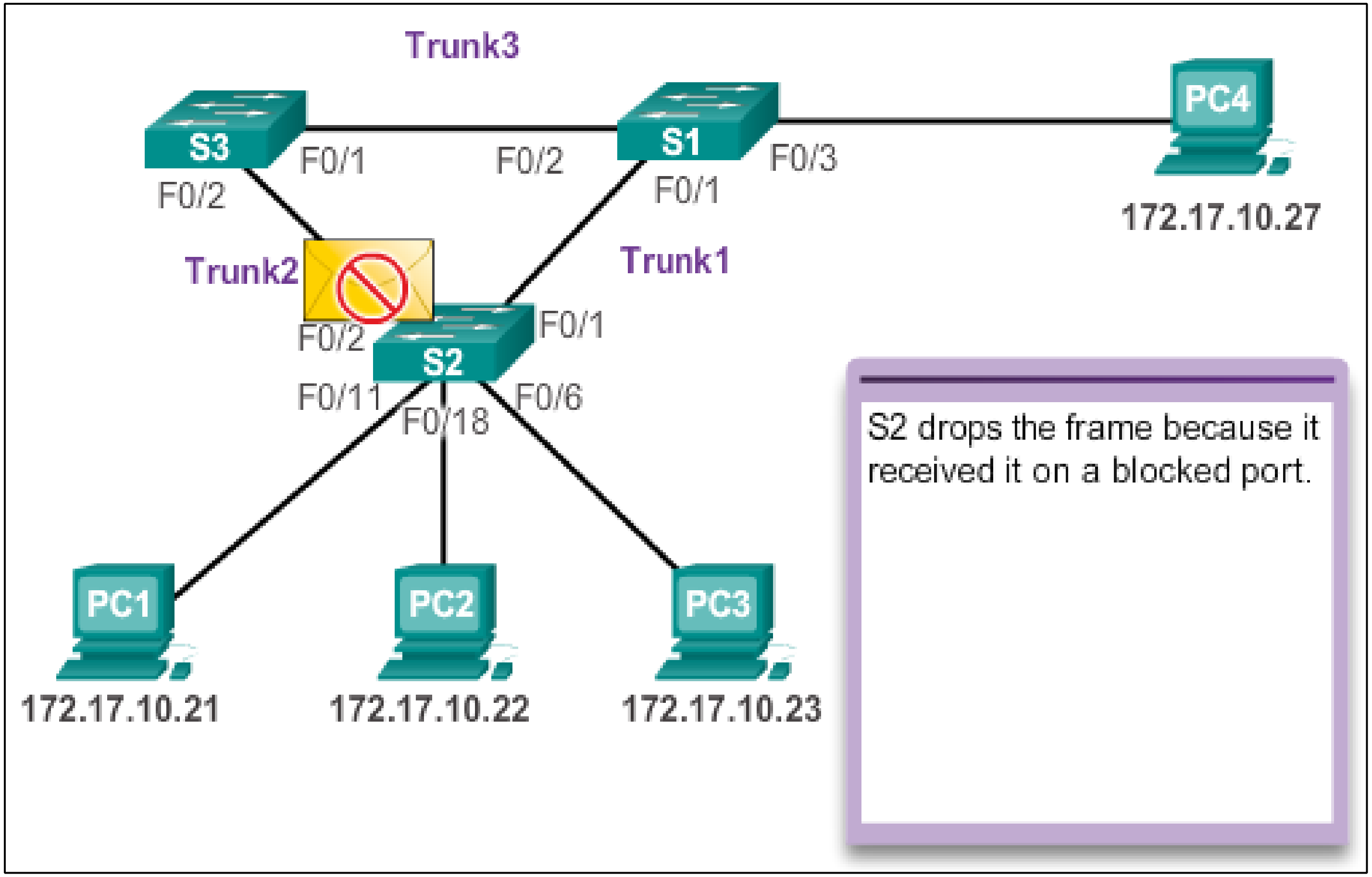
STP Operation
Spanning Tree Algorithm: Introduction



STP Operation
Spanning Tree Algorithm: Introduction

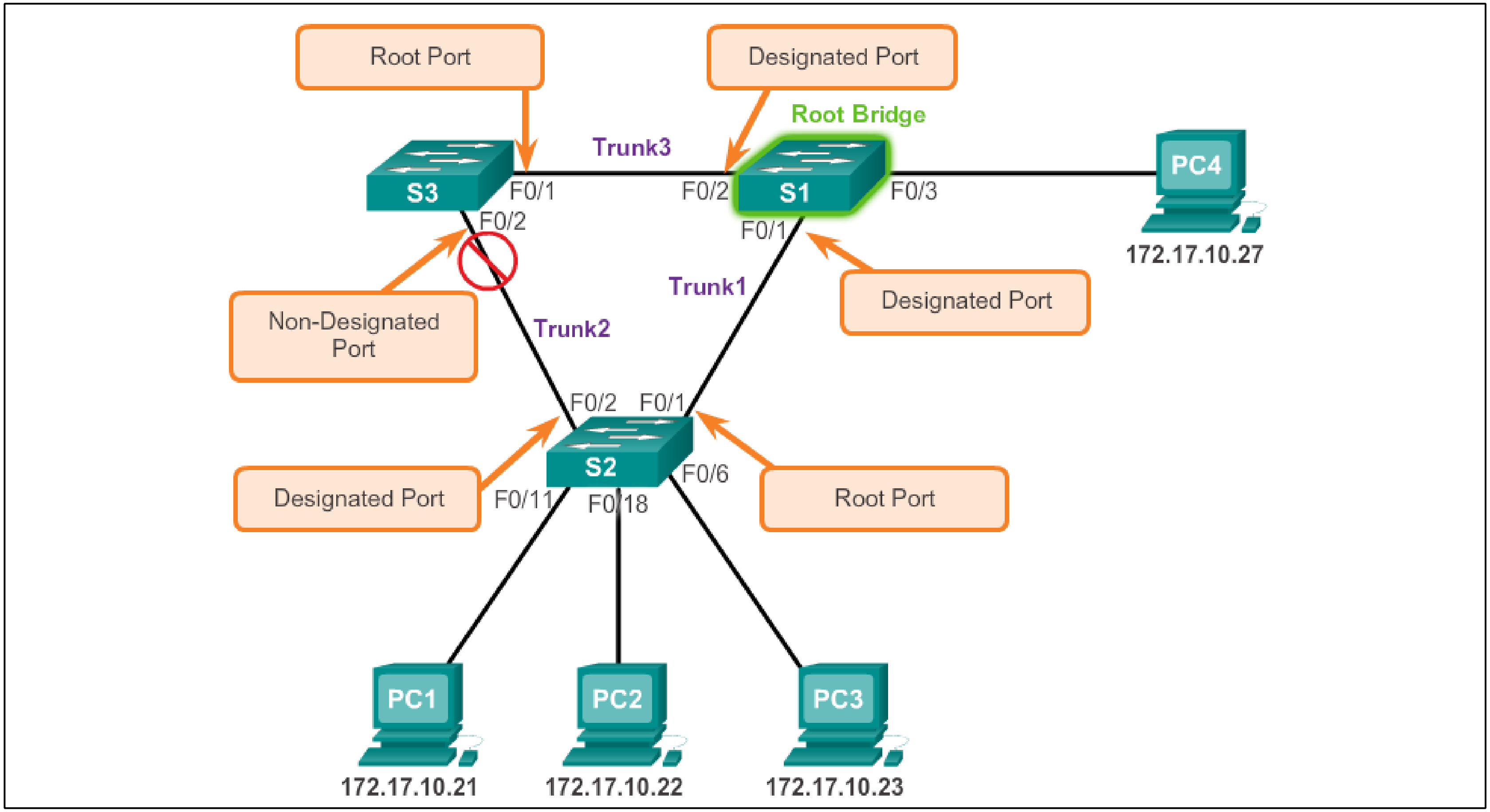


STP Operation
Spanning Tree Algorithm: Introduction



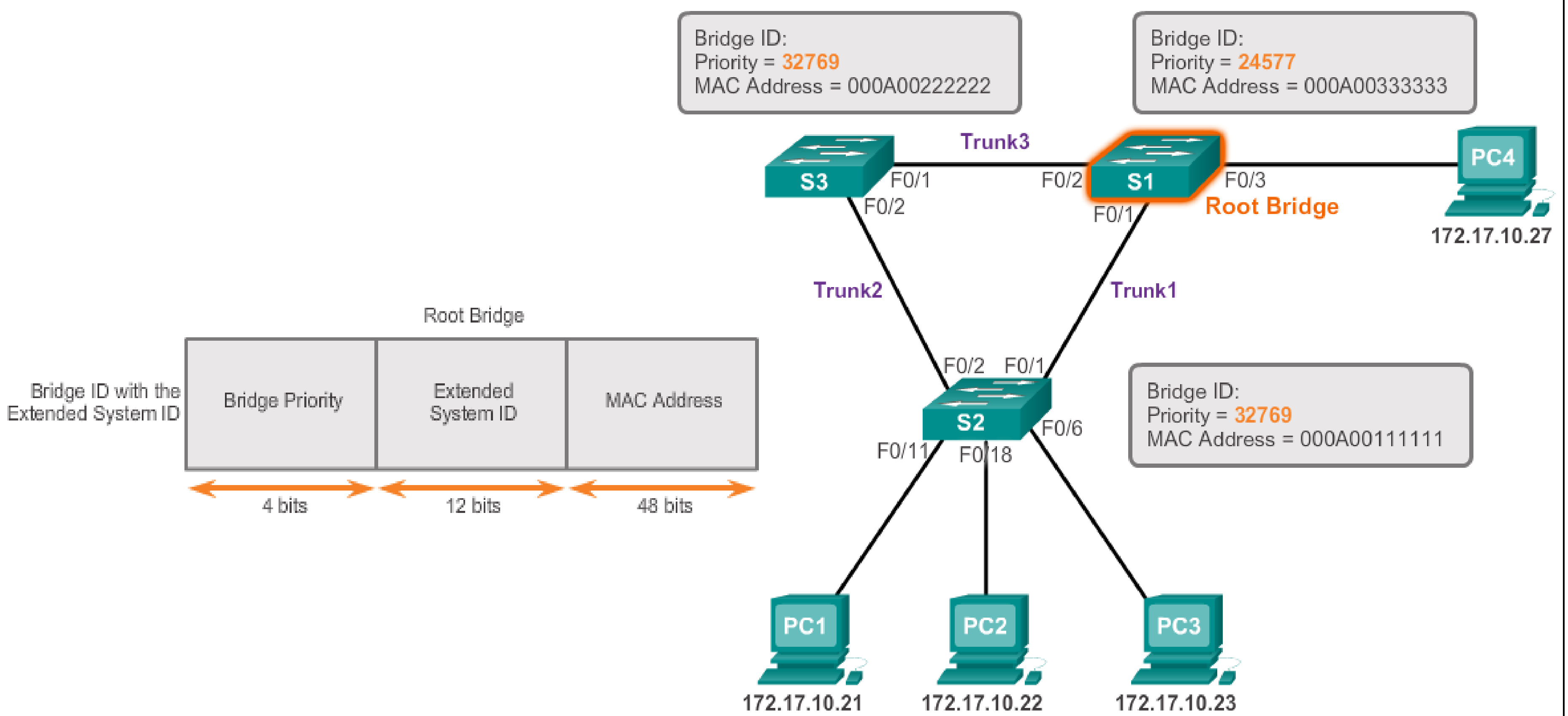
STP Operation

Spanning Tree Algorithm: Port Roles



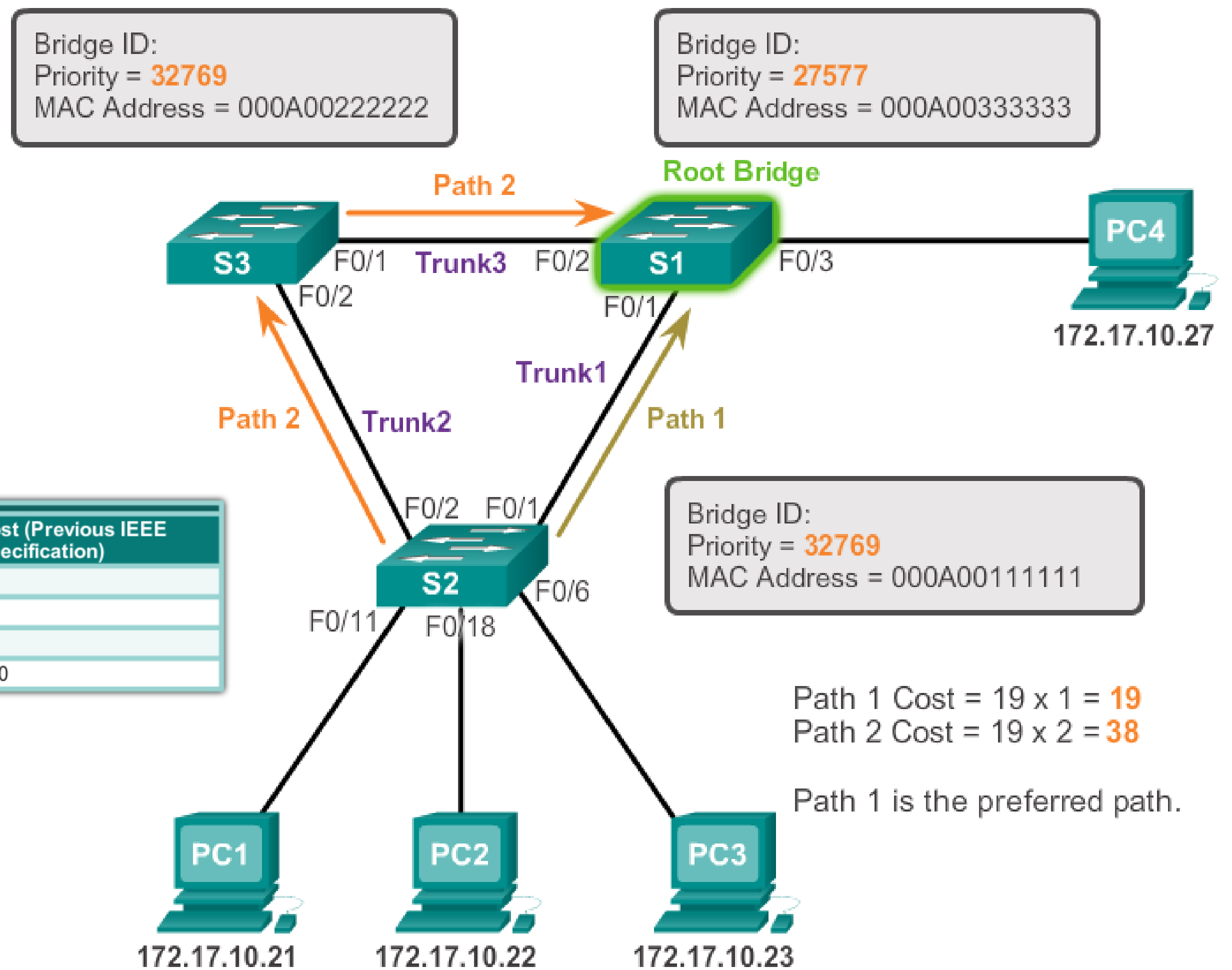
STP Operation

Spanning Tree Algorithm: Root Bridge

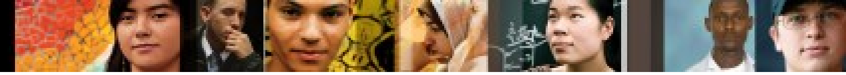


STP Operation

Spanning Tree Algorithm: Path Cost



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

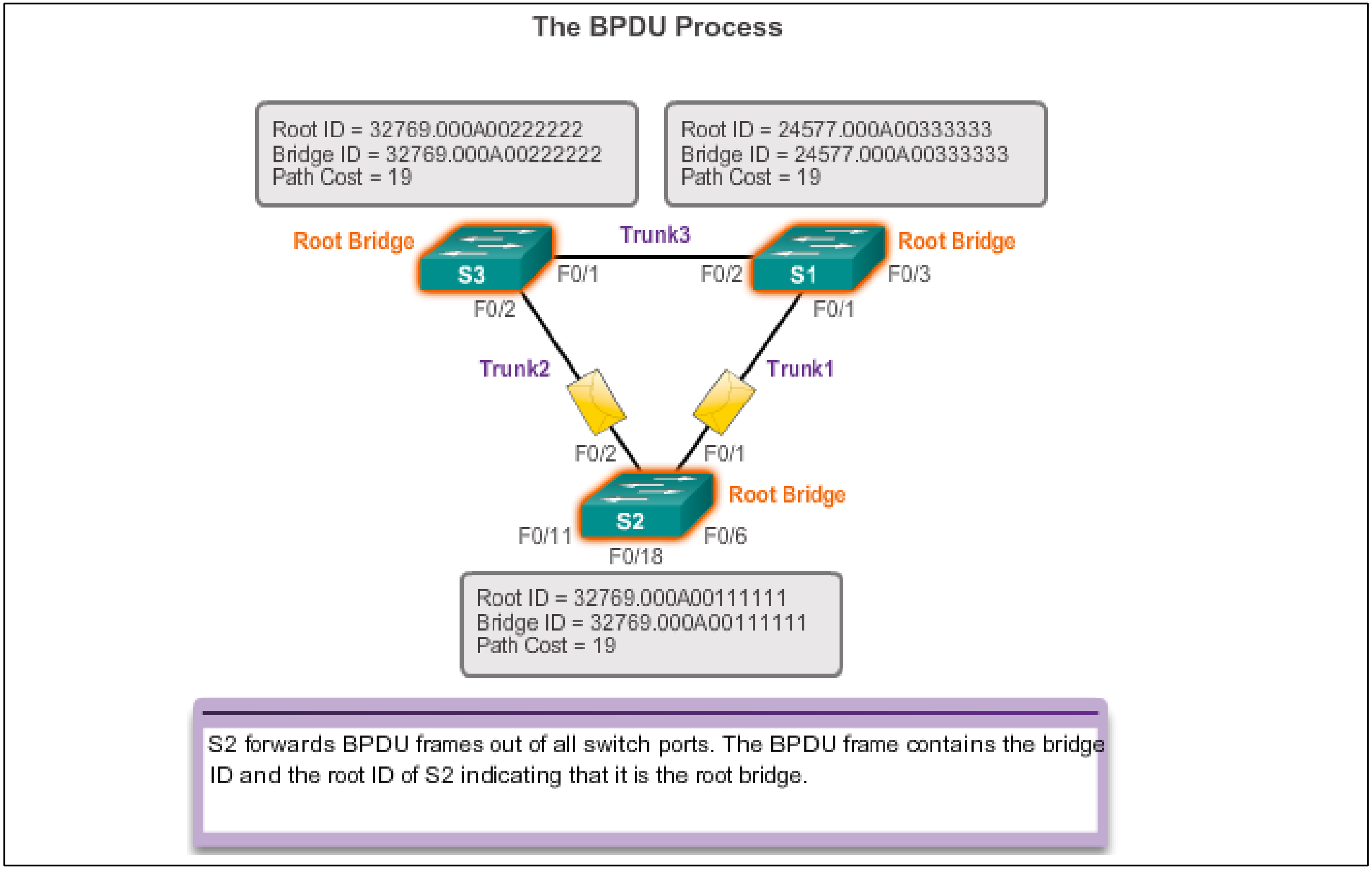


STP Operation

802.1D BPDU Frame Format

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊟ IEEE 802.3 Ethernet
  ⊞ Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
  ⊞ Source: Cisco_9e:93:03 (00:19:aa:9e:93:03)
    Length: 38
    Trailer: 0000000000000000
⊞ Logical-Link Control
⊟ Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Spanning Tree (0)
    BPDU Type: Configuration (0x00)
  ⊞ BPDU flags: 0x01 (Topology Change)
    Root Identifier: 24577 / 00:19:aa:9e:93:00
    Root Path Cost: 0
    Bridge Identifier: 24577 / 00:19:aa:9e:93:00
    Port identifier: 0x8003
    Message Age: 0
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
```

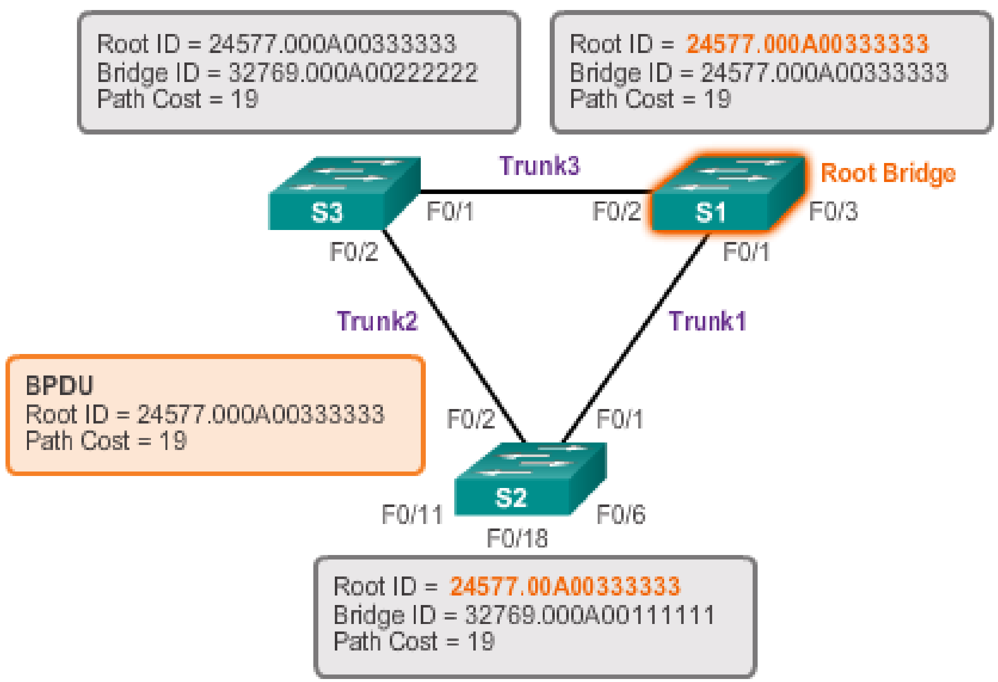
STP Operation
BPDU Propagation and Process



STP Operation

BPDU Propagation and Process

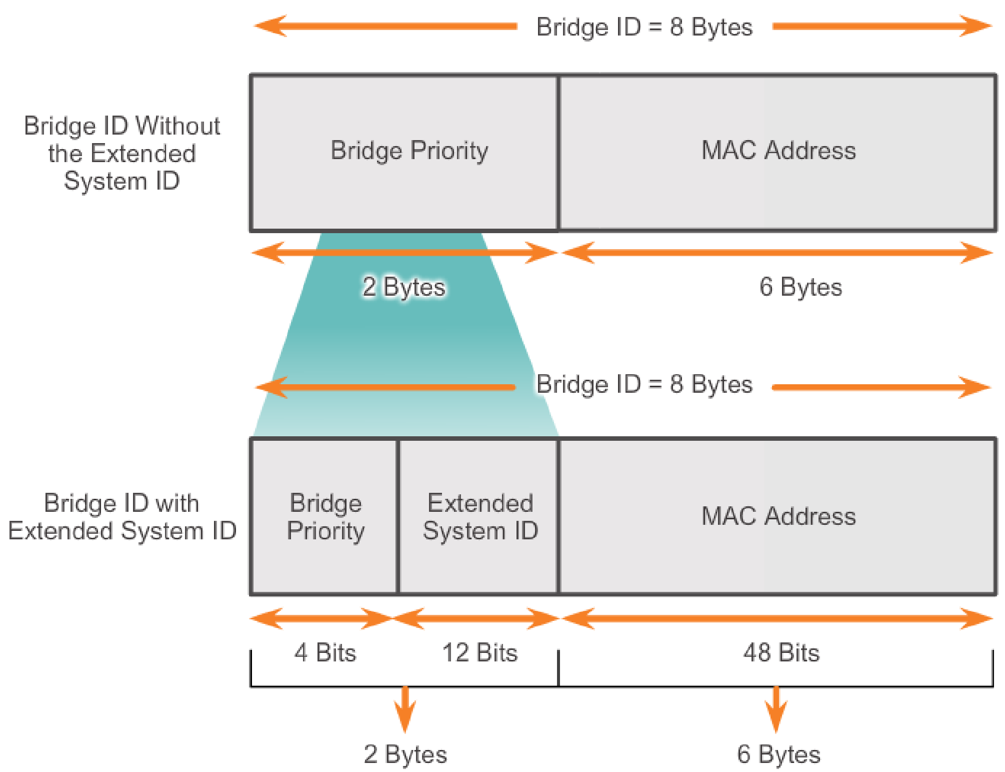
The BPDU Process



S2 compares the received root ID with its own and identifies S1 as the lower root ID. S2 updates its root ID with the root ID of S1. S2 now considers S1 as the root bridge. S2 updates the path cost to 19 since the BPDU was received on a Fast Ethernet port.

STP Operation

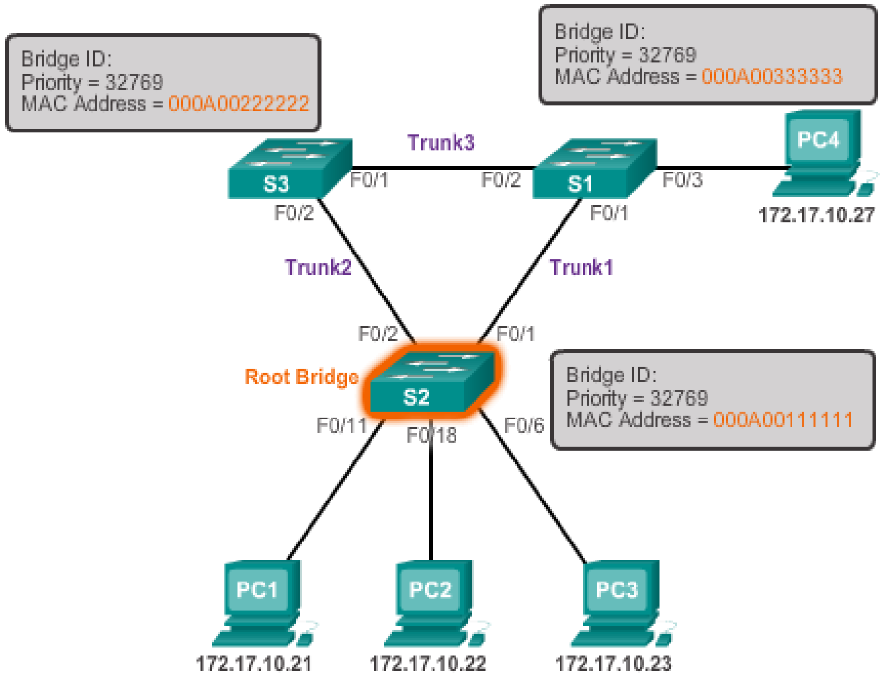
Extended System ID



STP was enhanced to include support for VLANs, requiring the VLAN ID to be included in the BPDU frame through the use of the extended system ID

STP Operation
Extended System ID

MAC Address-based decision



In the example, the priority of all the switches is 32769. The value is based on the 32768 default priority and the VLAN 1 assignment associated with each switch (32768+1).

2.2 Varieties of Spanning Tree Protocols

Cisco | Networking Academy®
Mind Wide Open™

Overview

List of Spanning Tree Protocols

- STP or IEEE 802.1D-1998
- PVST+
- IEEE 802.1D-2004
- Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1w
- Rapid PVST+
- Multiple Spanning Tree Protocol (MSTP) or IEEE 802.1s

STP Overview

Characteristics of the 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

PVST+

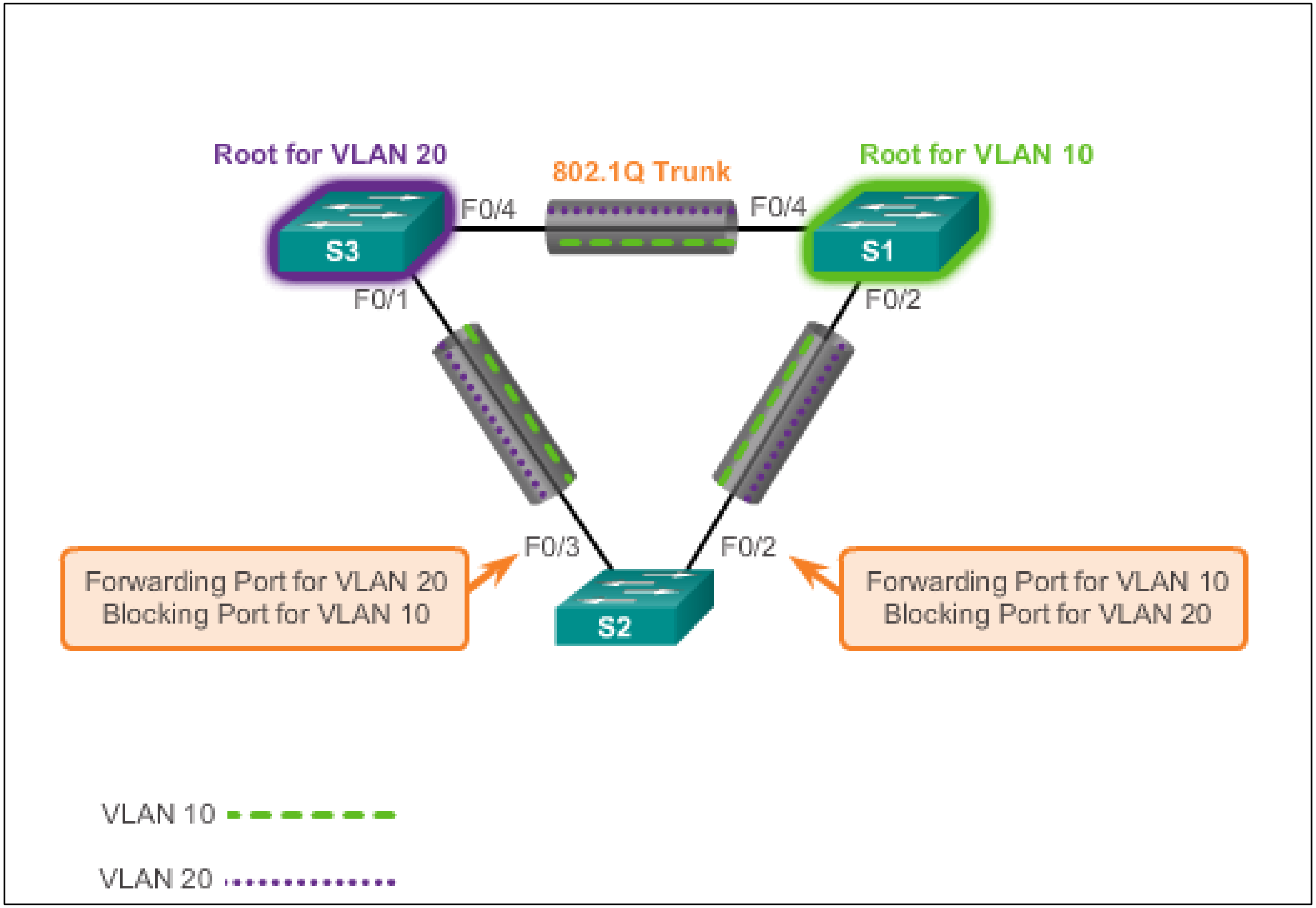
Overview of PVST+

Networks running PVST+ have these characteristics:

- A network can run an independent IEEE 802.1D STP instance for each VLAN in the network.
- Optimum load balancing can result.
- One spanning-tree instance for each VLAN maintained can mean a considerable waste of CPU cycles for all the switches in the network. In addition to the bandwidth that is used for each instance to send its own BPDU.

PVST+

Overview of PVST+



PVST+

Port States and PVST+ Operation

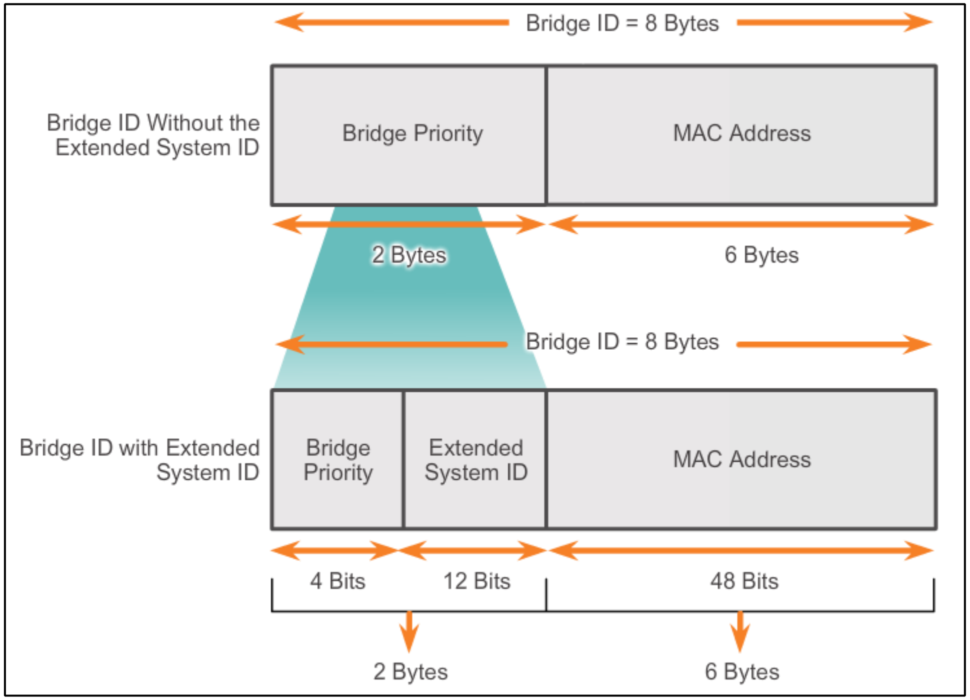
STP introduces the five port states:

Port States

Processes	Blocking	Listening	Learning	Forwarding	Disabled
Processes received BPDUs	YES	YES	YES	YES	NO
Forward data frames received on interface	NO	NO	NO	YES	NO
Forward data frames switched from another interface	NO	NO	NO	YES	NO
Learn MAC addresses	NO	NO	YES	YES	NO

Extended System ID and PVST+ Operation

- In a PVST+ environment, the extended switch ID ensures each switch has a unique BID for each VLAN.
- For example, the VLAN 2 default BID would be 32770; priority 32768, plus the extended system ID of 2.

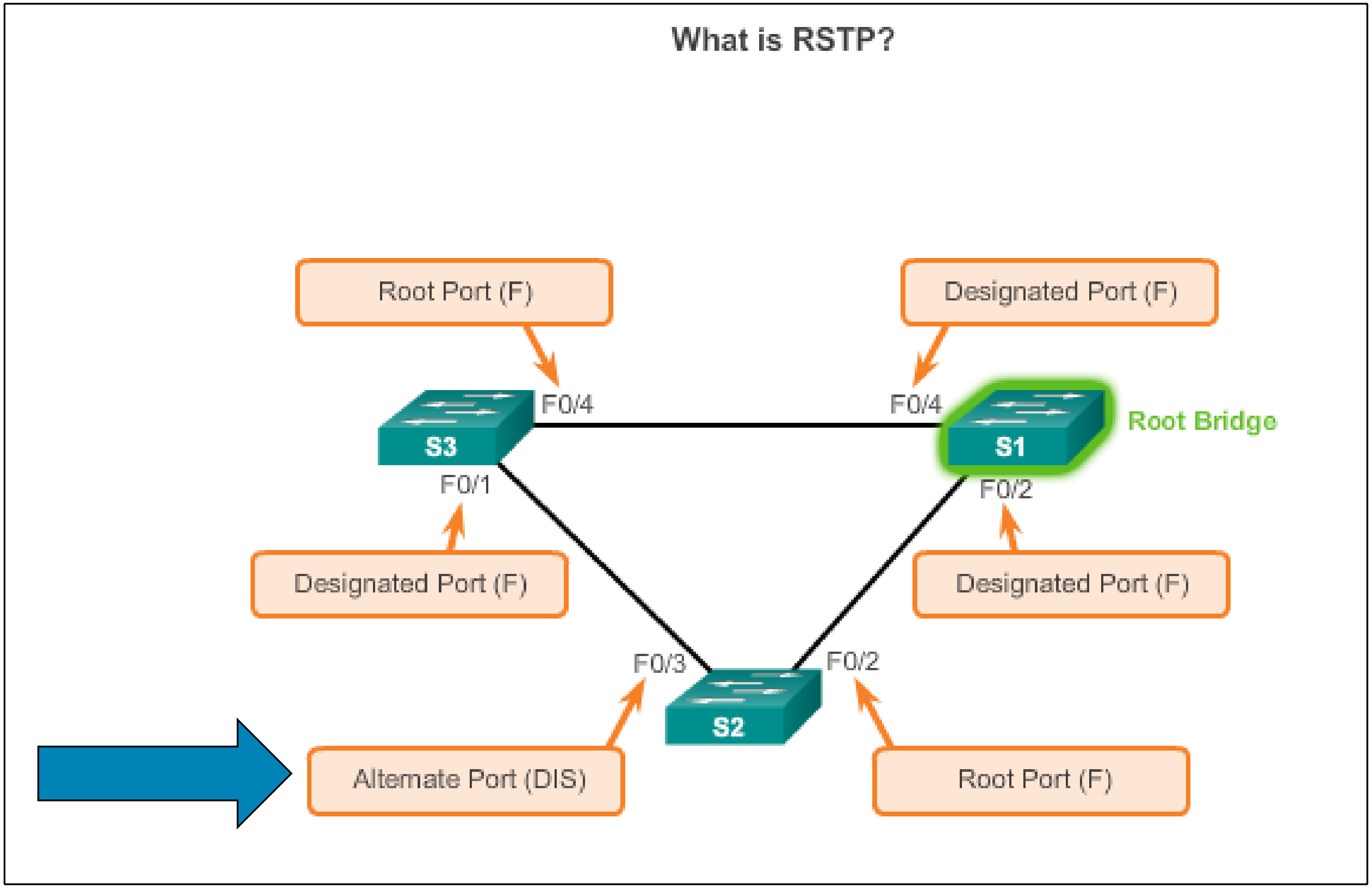


Overview of Rapid PVST+

- RSTP is the preferred protocol for preventing Layer 2 loops in a switched network environment.
- With Rapid PVST+, an independent instance of RSTP runs for each VLAN.
- RSTP supports a new port type: an alternate port in discarding state.
- There are no blocking ports. RSTP defines port states as discarding, learning, or forwarding.
- RSTP (802.1w) supersedes STP (802.1D) while retaining backward compatibility
- RSTP keeps the same BPDU format as IEEE 802.1D, except that the version field is set to 2 to indicate RSTP, and the flags field uses all 8 bits.

Rapid PVST+

Overview of Rapid PVST+



Rapid PVST+

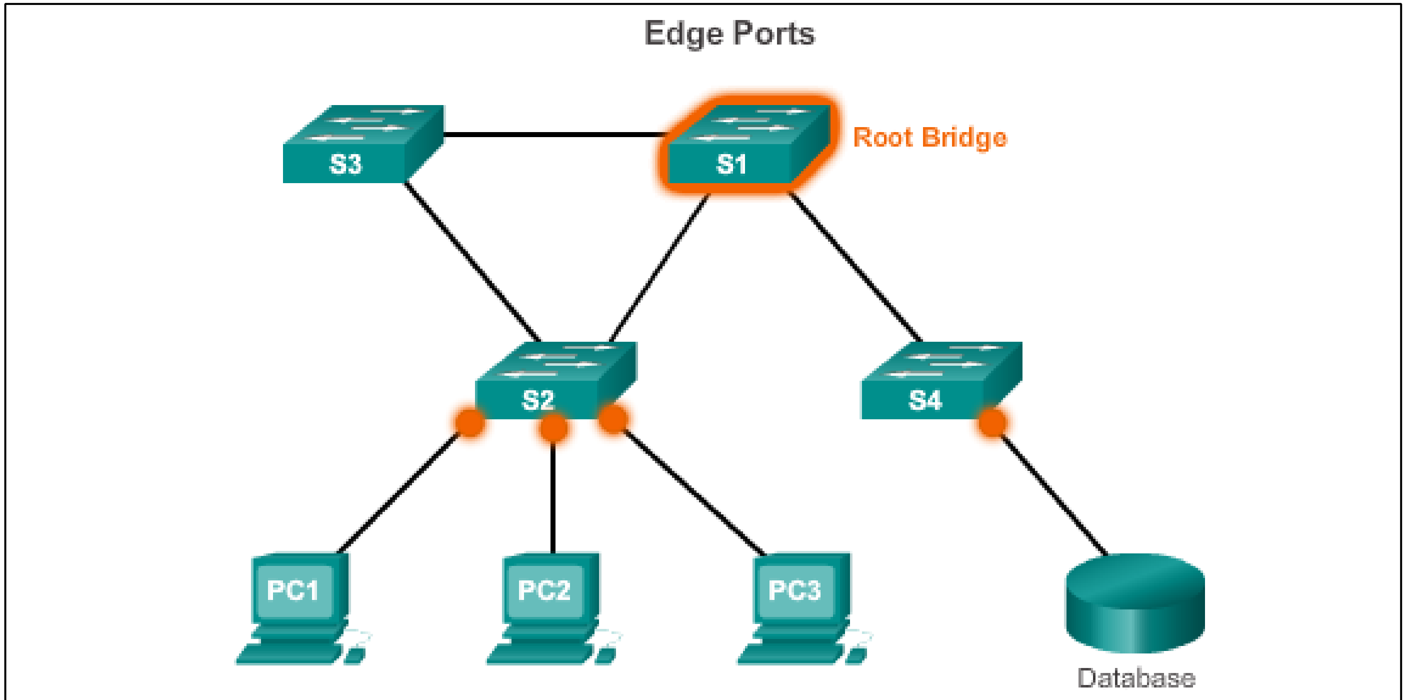
RSTP BPDU

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 Unknown Port Alternate or Backup Port Root Port Designated Port	2-3 00 01 10 11
Learning	4
Forwarding	5
Agreement	6
Topology Change Acknowledgment	7

Rapid PVST+

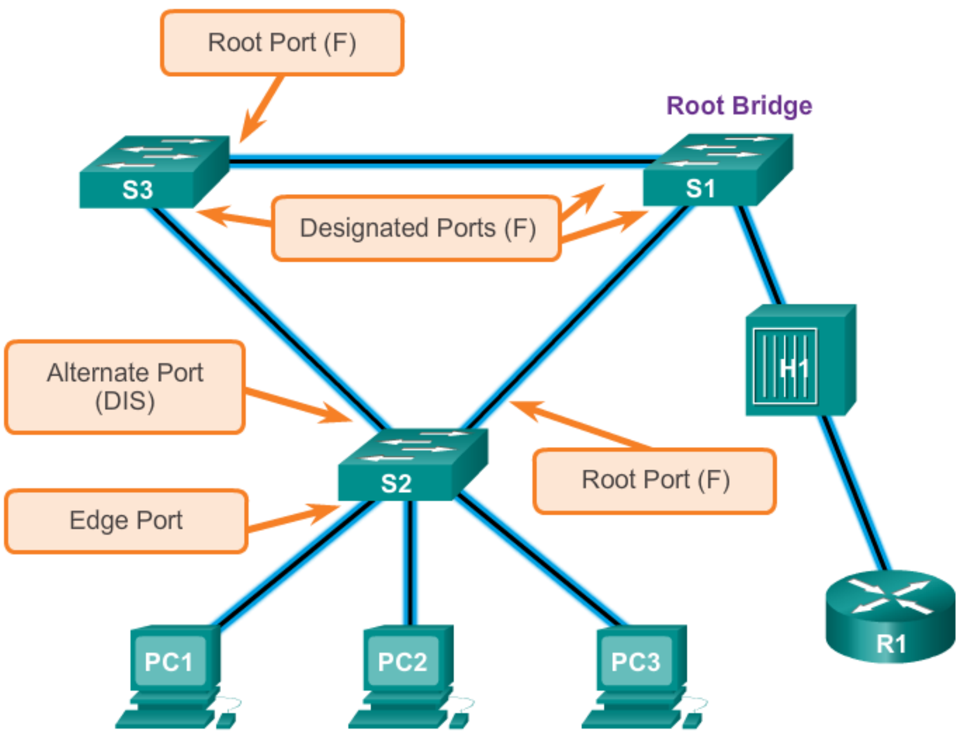
Edge Ports



Edge Ports

- Will never have a switch connected to it
- Immediately transitions to forwarding
- Functions similarly to a port configured with Cisco PortFast
- On a Cisco switch configured using the `spanning-tree portfast`

Rapid PVST+
Link Types



The link type can determine whether the port can immediately transition to forwarding state. Edge port connections and point-to-point connections are candidates for rapid transition to forwarding state.

2.3 Spanning Tree Configuration

Cisco | Networking Academy®
Mind Wide Open™

PVST+ Configuration
Catalyst 2960 Default Configuration

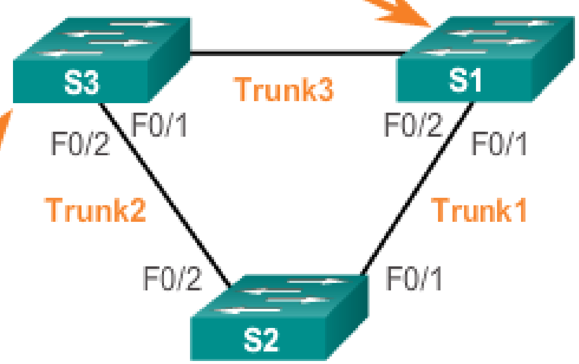
Feature	Default Setting
Enable state	Enabled on VLAN 1
Spanning-tree mode	PVST+ (Rapid PVST+ and MSTP are disabled.)
Switch priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree timers	Hello time: 2 seconds Forward-delay time: 15 seconds Maximum-aging time: 20 seconds Transmit hold count: 6 BPDUs

PVST+ Configuration

Configuring and Verifying the Bridge ID

Method 1

```
s1(config)# spanning-tree VLAN 1 root primary
s1(config)# end
```



Method 2

```
s3(config)# spanning-tree VLAN 1 priority 24576
s3(config)# end
```

Method 1

```
s2(config)# spanning-tree VLAN 1 root secondary
s2(config)# end
```

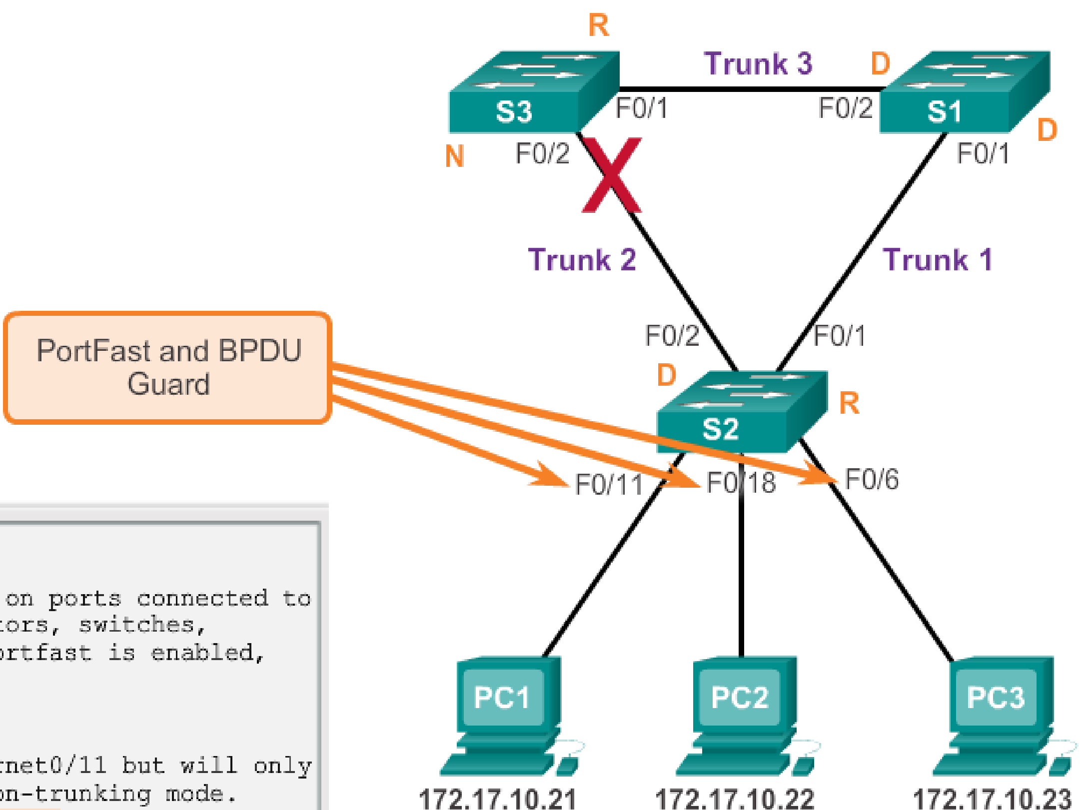
PVST+ Configuration

Configuring and Verifying the Bridge ID

```
S3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority     24577
               Address      00A.0033.3333
               This bridge is the root
               Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID    Priority     24577  (priority  24576  sys-id-ext  1)
               Address      000A.0033.3333
               Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time   300

Interface      Role    Sts    Cost     Prio.Nbr      Type
------------   -----   ----   -----    ----------    ------
Fa0/1          Desg    FWD    4        128.1         p2p
Fa0/2          Desg    FWD    4        128.2         p2p
S3#
```

PVST+ Configuration
PortFast and BPDU Guard

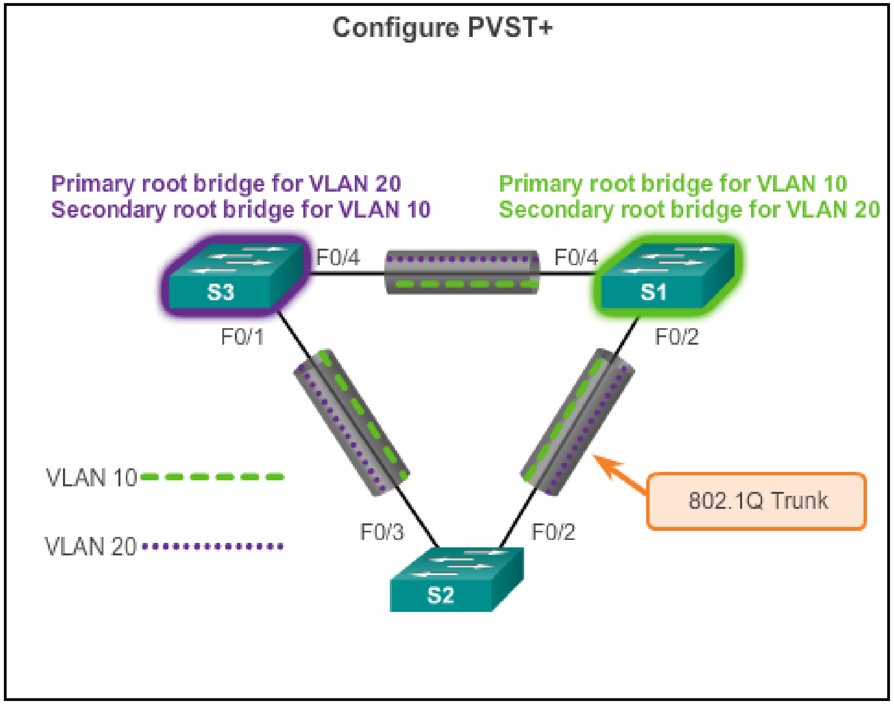
- When a switch port is configured with PortFast that port transitions from blocking to forwarding state immediately.
- BPDU guard puts the port in an *error-disabled* state on receipt of a BPDU.




```
S2(config)# interface FastEthernet 0/11
S2(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 FastEthernet0/11 but will only
 have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
S2(config-if)# end
```

PVST+ Configuration

PVST+ Load Balancing



Configure PVST+

```
S3(config)# spanning-tree vlan 20 root primary
```

This command forces S3 to be the primary root for VLAN 20.

```
S3(config)# spanning-tree vlan 10 root secondary
```

This command forces S3 to be the secondary root for VLAN 10.

```
S1(config)# spanning-tree vlan 10 root primary
```

This command forces S1 to be the primary root for VLAN 10.

```
S1(config)# spanning-tree vlan 20 root secondary
```

This command forces S1 to be the secondary root for VLAN 20.

PVST+ Configuration

PVST+ Load Balancing

- Another method to specify the root bridge is to set the spanning tree priority on each switch to the lowest value so that the switch is selected as the primary bridge for its associated VLAN.

Configure PVST+

```
S3(config)# spanning-tree vlan 20 priority 4096
```

This command sets the priority for S3 to be the lowest possible, making it most likely that S3 will be the primary root for VLAN 20.

```
S1(config)# spanning-tree vlan 10 priority 4096
```

This command sets the priority for S1 to be the lowest possible, making it most likely that S1 will be the primary root for VLAN 10.

PVST+ Configuration
PVST+ Load Balancing

- Display and verify spanning tree configuration details.

Configure PVST+

```
S3# show spanning-tree active
<output omitted>
VLAN0010
   Spanning tree enabled protocol ieee
   Root ID       Priority     4106
                 Address      0019.aa9e.b000
                 This bridge is the root
                 Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
   Bridge ID     Priority     4106  (priority  4096  sys-id-ext  10)
                 Address      0019.aa9e.b000
                 Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
                 Aging Time   300

Interface        Role    Sts    Cost     Prio.Nbr      Type
------------     -----   ----   -----    ----------    ------
Fa0/2            Desg    FWD    19        128.2         p2p
Fa0/4            Desg    FWD    19        128.4         p2p
<output omitted>
```

PVST+ Configuration

PVST+ Load Balancing

Configure PVST+

```
S1# show running-config
Building configuration...

Current configuration : 1595 bytes
!
version 12.2
 <output omitted>

!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
 <output omitted>
```

Rapid PVST+ Configuration
Spanning Tree Mode

Rapid PVST+ is the Cisco implementation of RSTP. It supports RSTP on a per-VLAN basis.

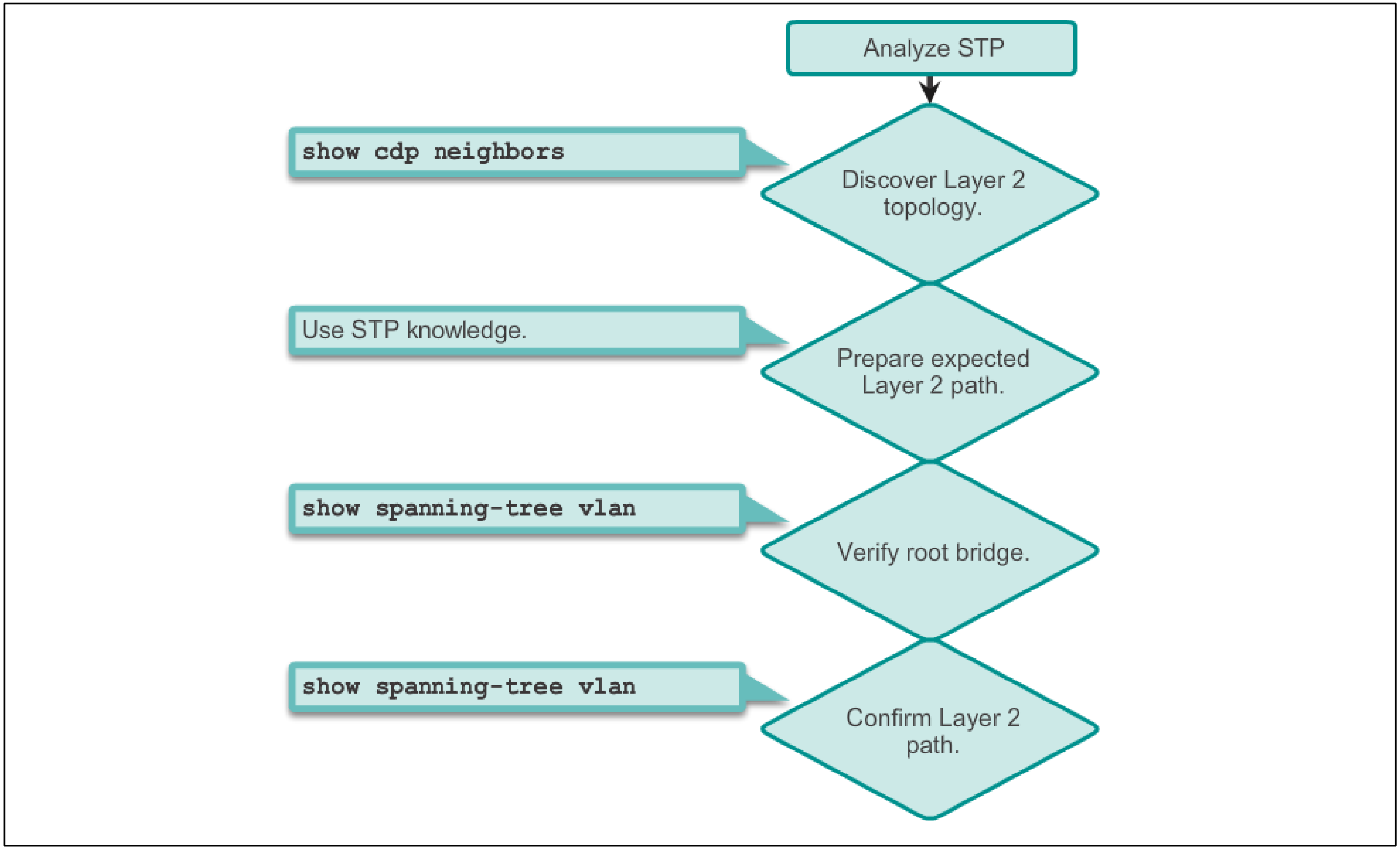
```
S1# configure terminal
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/2
S1(config-if)# spanning-tree link-type point-to-point
S1(config-if)# end
S1# clear spanning-tree detected-protocols
```

Cisco IOS Command Syntax

Enter global configuration mode.	**configure terminal**
Configure Rapid PVST+ spanning-tree mode.	**spanning-tree mode rapid-pvst**
Enter interface configuration mode and specify an interface to configure. Valid interfaces include physical ports, VLANs, and port channels.	**interface** *interface-id*
Specify that the link type for this port is point-to-point.	**spanning-tree link-type point-to-point**
Return to privileged EXEC mode.	**end**
Clear all detected STP.	**clear spanning-tree detected-protocols**

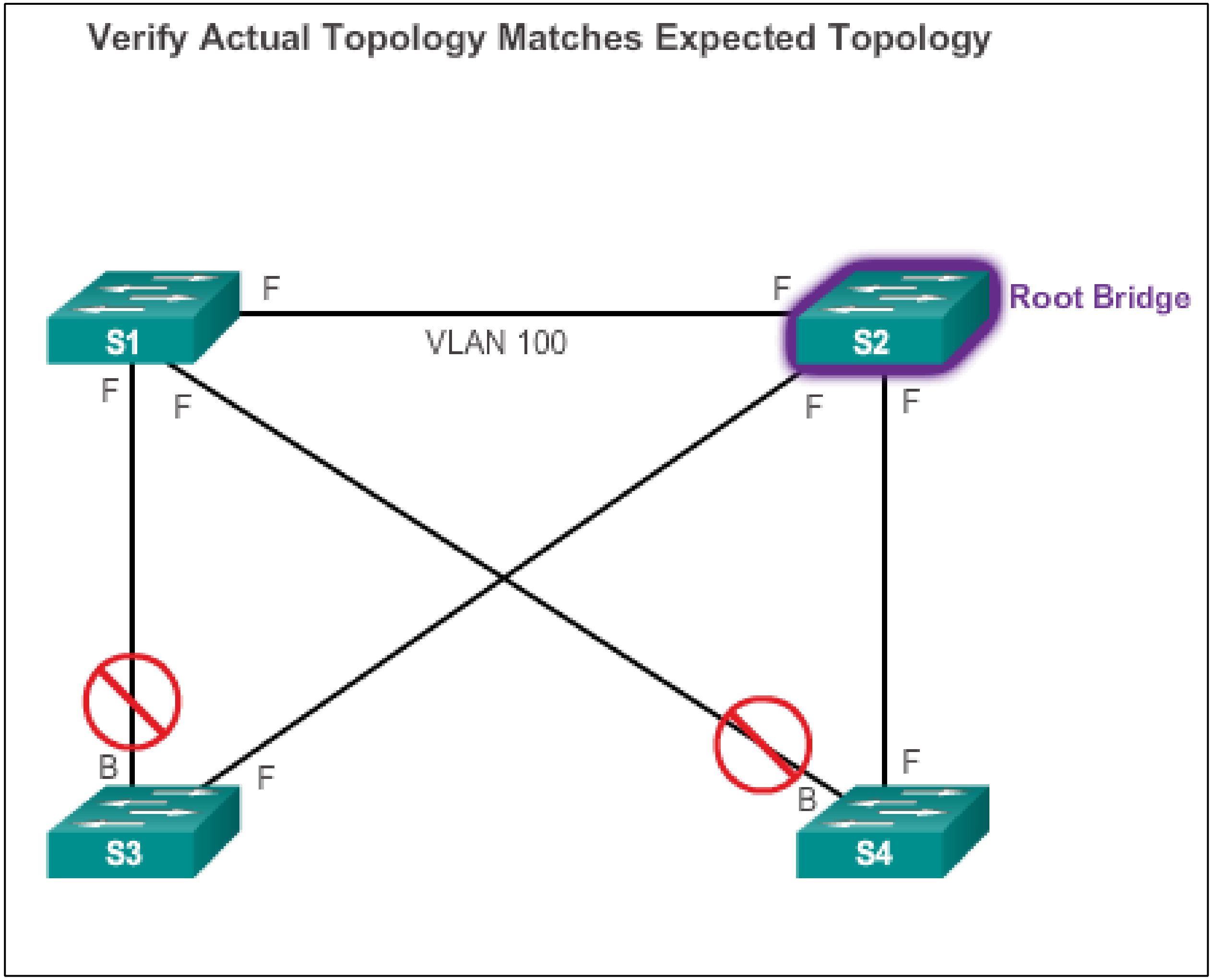
STP Configuration Issues

Analyzing the STP Topology



STP Configuration Issues

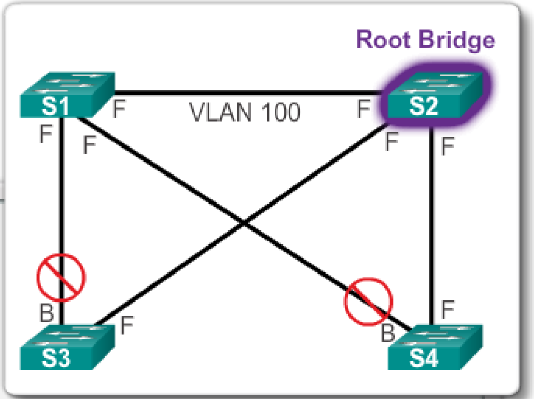
Expected Topology versus Actual Topology



STP Configuration Issues

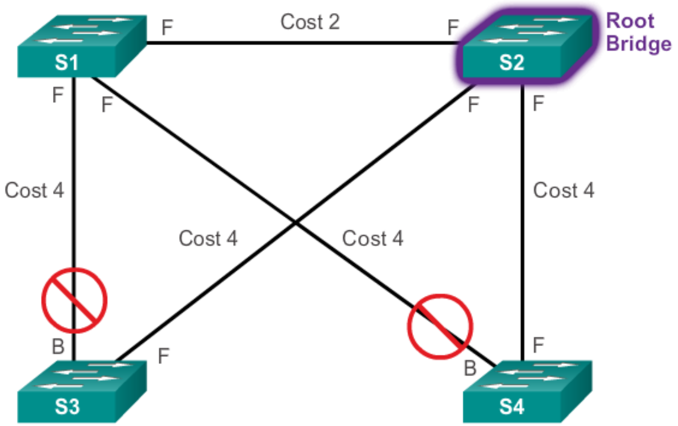
Overview of Spanning Tree Status

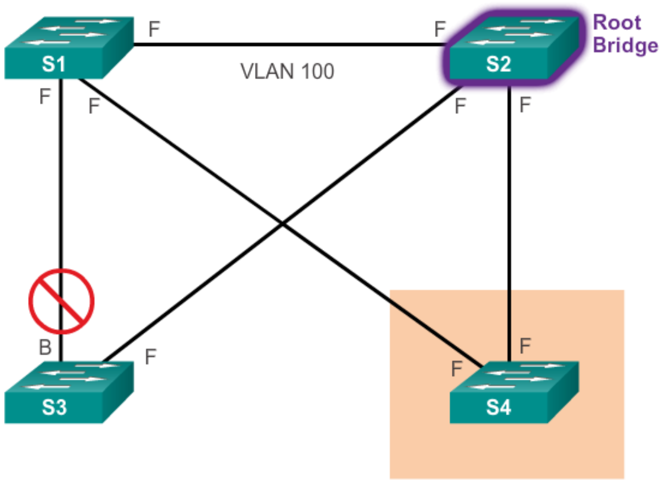
```
S1# show spanning-tree vlan 100

VLAN0100
 Spanning tree enabled protocol rstp
 Root ID     Priority     28772
             Address      0000.0c9f.3127
             Cost         2
             Port         88 (TenGigabit9/1)
             Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID   Priority     28772 (priority 28672 sys-id-ext 100)
             Address      0000.0cab.3724
             Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time   300

Interface      Role Sts Cost      Prio.Nbr Type
---------      -------------      -----------------------------
Gi3/1          Desg FWD 4         128.72   P2p
Gi3/2          Desg FWD 4         128.80   P2p
Te9/1          Root FWD 2         128.88   P2p
```

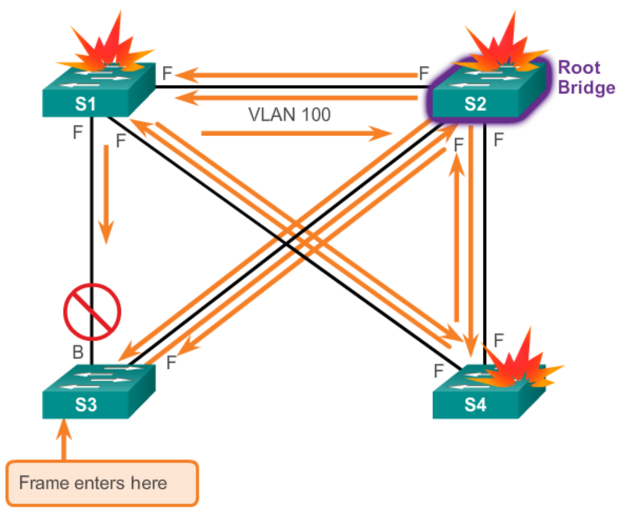


Spanning-Tree Failure Consequences

- STP erroneously moves one or more ports into the forwarding state.
- Any frame that is flooded by a switch enters the loop.







STP Configuration Issues

Repairing a Spanning Tree Problem

- One way to correct spanning-tree failure is to manually remove redundant links in the switched network, either physically or through configuration, until all loops are eliminated from the topology.
- Before restoring the redundant links, determine and correct the cause of the spanning-tree failure.
- Carefully monitor the network to ensure that the problem is fixed.

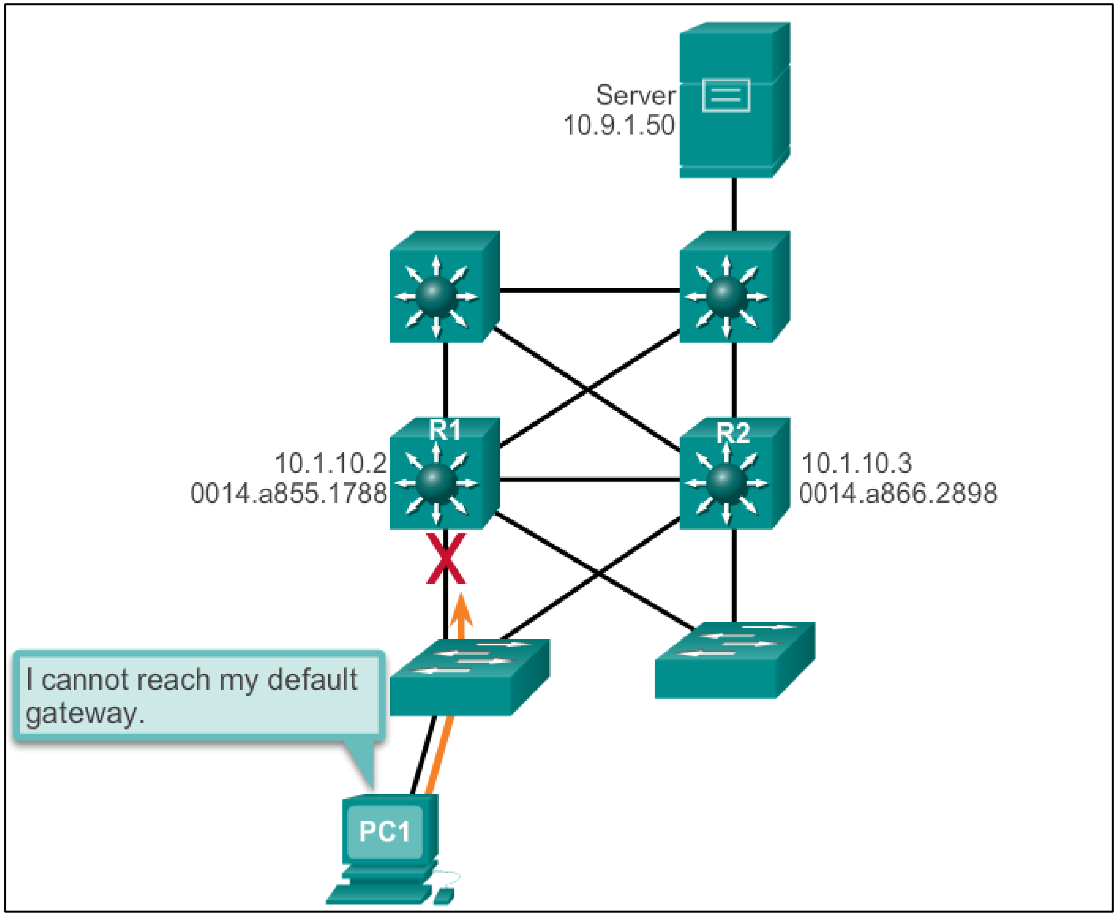
2.4 First-Hop Redundancy Protocols

Cisco | Networking Academy®
Mind Wide Open™

Concept of First-Hop Redundancy Protocols

Default Gateway Limitations

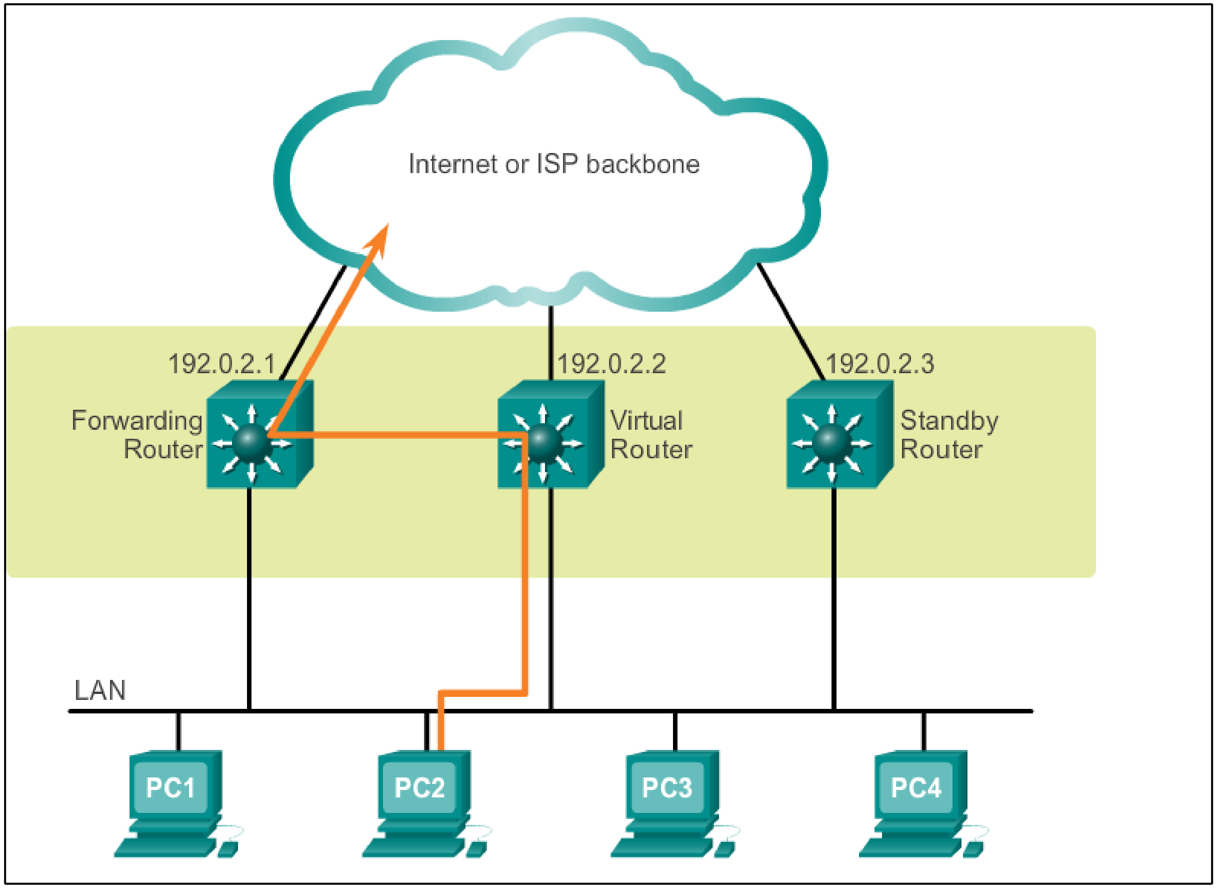
- If the default gateway cannot be reached, the local device is unable to send packets off the local network segment.
- Even if a redundant router exists that could serve as a default gateway for that segment, there is no dynamic method by which these devices can determine the address of a new default gateway.



Concept of First-Hop Redundancy Protocols

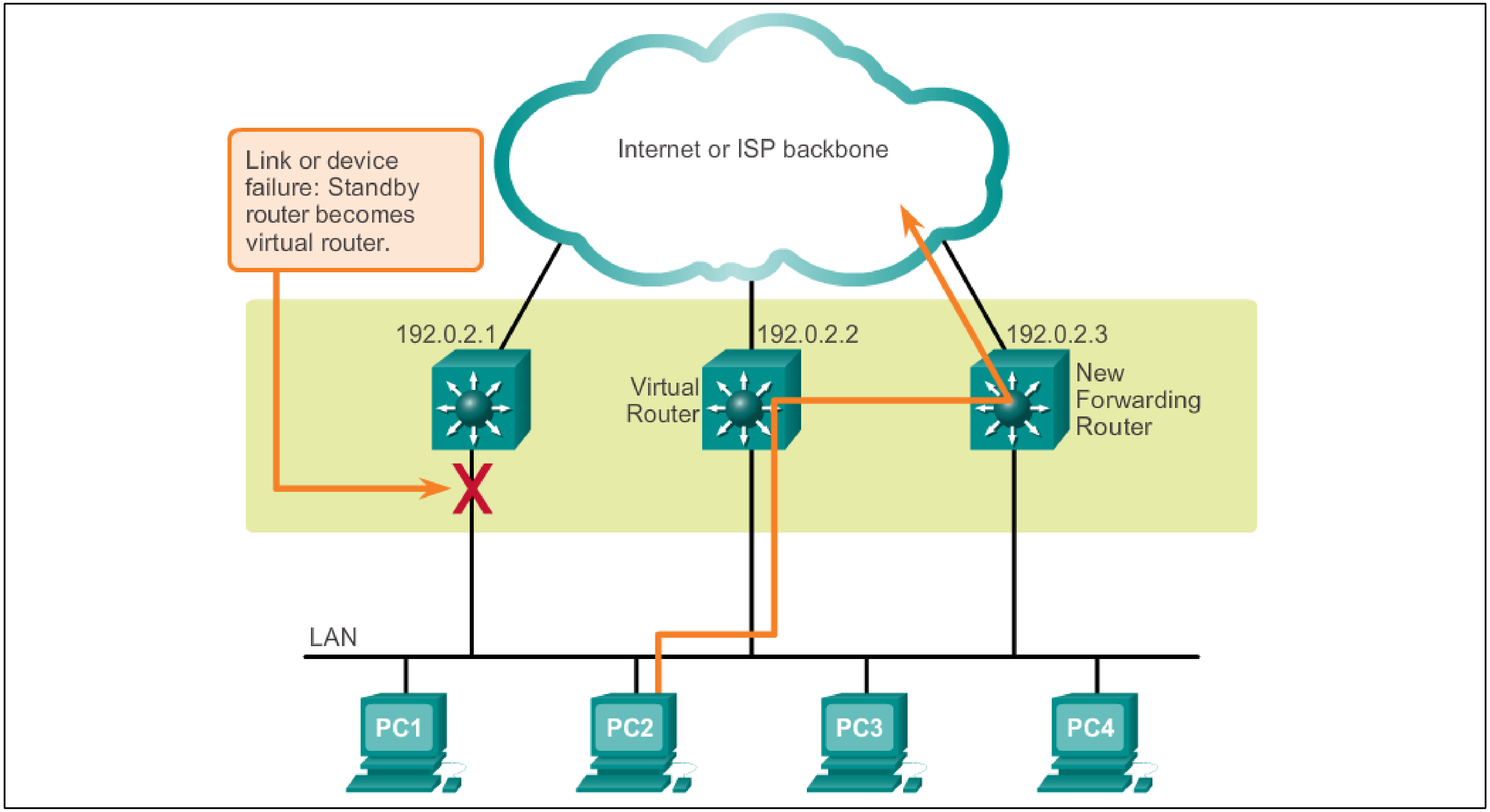
Router Redundancy

- Multiple routers are configured to work together to present the illusion of a single router to the hosts on the LAN.
- The ability of a network to dynamically recover from the failure of a device acting as a default gateway is known as first-hop redundancy.



Concept of First-Hop Redundancy Protocols

Steps for Router Failover



Varieties of First-Hop Redundancy Protocols

First-Hop Redundancy Protocols

- Hot Standby Router Protocol (HSRP)
- HSRP for IPv6
- Virtual Router Redundancy Protocol version 2 (VRRPv2)
- VRRPv3
- Gateway Load Balancing Protocol (GLBP)
- GLBP for IPv6
- ICMP Router Discovery Protocol (IRDP)

Varieties of First-Hop Redundancy Protocols

First-Hop Redundancy Protocols

First-Hop Router Redundancy Options

- HSRP defines a group of routers - one active and one standby.
- Virtual IP and MAC are shared between the two routers.
- To verify HSRP state, use the **`show standby`** command.
- HSRP is Cisco proprietary.
- VRRP is a standard protocol.

FHRP Verification

HSRP Verification

```
Router# show standby
Ethernet0/1 - Group 1
  State is Active
   2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
   Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
   Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
   Next hello sent in 1.412 secs
  Gratuitous ARP 14 sent, next in 7.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
   Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
Group name is "HSRP1" (cfgd)
Follow by groups:
Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.666)
Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.491)
  Group name is "HSRP1", advertisement interval is 34 sec
```

FHRP Verification

GLBP Verification

- Gateway Load Balancing Protocol (GLBP) is a Cisco proprietary solution to allow automatic selection and simultaneous use of multiple available gateways in addition to automatic failover between those gateways.

```
Router# show glbp
FastEthernet0/1 - Group 1
  State is Active
    1 state change, last state change 00:02:34
  Virtual IP address is 192.168.2.100
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.288 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is local
  Standby is 192.168.2.2, priority 100 (expires in 8.640 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    001e.7aa3.5e71 (192.168.2.1) local
    001e.7aa3.5f31 (192.168.2.2)
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:02:23
    MAC address is 0007.b400.0101 (default)
    Owner ID is 001e.7aa3.5e71
    Redirection enabled
Preemption enabled, min delay 30 sec
    Active is local, weighting 100
```

2.5 Summary

Cisco | Networking Academy®
Mind Wide Open™

Chapter 2: Summary

- IEEE 802.1D is implemented on Cisco switches on a per-VLAN basis in the form of PVST+. This is the default configuration on Cisco switches.
- RSTP, can be implemented on Cisco switches on a per-VLAN basis in the form of Rapid PVST+.
- With PVST+ and Rapid PVST+, root bridges can be configured proactively to enable spanning tree load balancing.
- First hop redundancy protocols, such as HSRP, VRRP, and GLBP provide alternate default gateways for hosts in the switched environment.

Cisco | Networking Academy®
Mind Wide Open™