Chapter Two
Switch Concepts and Configuration

Outline

1. **Basic Switch Configuration**
2. **Security Concerns in LANs**
3. **Switch Port Security**
4. **VLANs**
5. **Inter-VLAN Routing**

Objectives

- Upon completion of this chapter, you will be able to answer the following questions:
  - What are the steps a switch takes after power is applied?
  - What is the function of the boot loader if the operating system is corrupt or missing?
  - How might the switch LEDs help with troubleshooting?
  - What are the steps taken to configure a Cisco switch with an IP address, subnet mask, and default gateway?
  - What interface is used to apply an IP address to a Cisco switch?
  - What functionality is available once a switch has an IP address and default gateway?
  - What type of customization can be applied to a switch port?
  - What tools can be used to troubleshoot a Layer 1 or 2 problem?
  - What steps are required to configure a switch for SSH access?

Objectives…

- What are some common security attacks that affect switches?
- What mitigation tools could be used on a Cisco switch to prevent or react to a security attack?
- What are best practices for switch security?
- What steps are required to configure switch security?
- What is the purpose of DTP?

1. Basic switch configuration

Introduction

- Switches are used to connect multiple devices on the same network.
- In a properly designed network, LAN switches are responsible for directing and controlling the data flow at the access layer to networked resources.
- Cisco switches are self-configuring and no additional configurations are necessary for them to function out of the box.
- However, Cisco switches run Cisco IOS, and can be manually configured to better meet the needs of the network.
- This includes adjusting port speed and bandwidth, as well as implementing security requirements.

1. Basic switch configuration

- Switches are one of the numerous devices installed onto the corporate network infrastructure.
- Configuring them can be fun and challenging.
- Knowing how switches normally boot and load an operating system is also important.
- **Switch Boot Sequence:-** After a Cisco switch is powered on, goes through the following boot sequence
  - ✓ POST (power-on self-test)
  - ✓ Run boot loader software
  - ✓ Boot loader does low-level CPU initialization
  - ✓ Boot loader initializes the flash file system
  - ✓ Boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.

Switch Boot Sequence …

In order to find a suitable IOS image, the switch goes through the following steps:

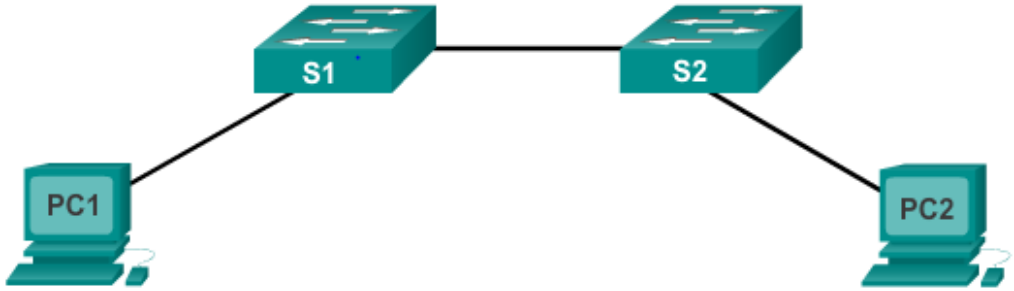
1. It attempts to automatically boot by using information in the BOOT environment variable
2. If this variable is not set, the switch performs a top-to-bottom search through the flash file system. It will load and execute the first executable file, if it can.
3. The IOS operating system then initializes the interfaces using the Cisco IOS commands found in the configuration file, startup configuration, which is stored in NVRAM.

Note: The BOOT environment variable is set using the boot System global configuration mode command. Use the show bootvar command to see to what the current IOS boot file is set.

Basic switch configuration

Let's focus on

- Creating a two PC network connected via a switch
- Setting a name for the switch
- Limiting access to the device configuration
- Configuring banner messages
- Saving the configuration

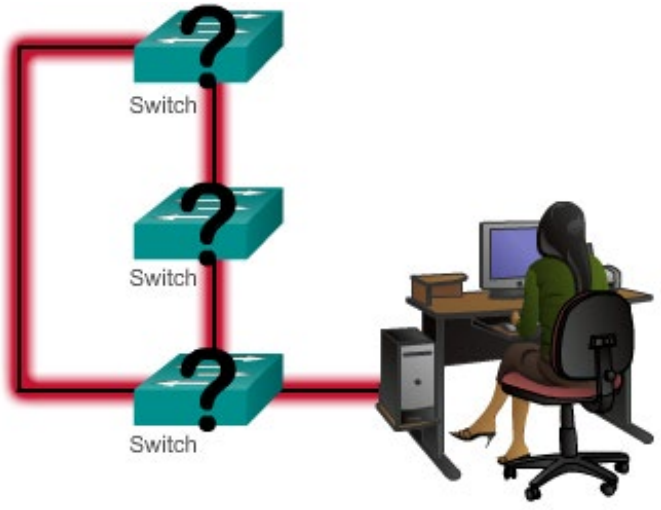


Device Names (Hostname)

Some guidelines for naming conventions are that names should:

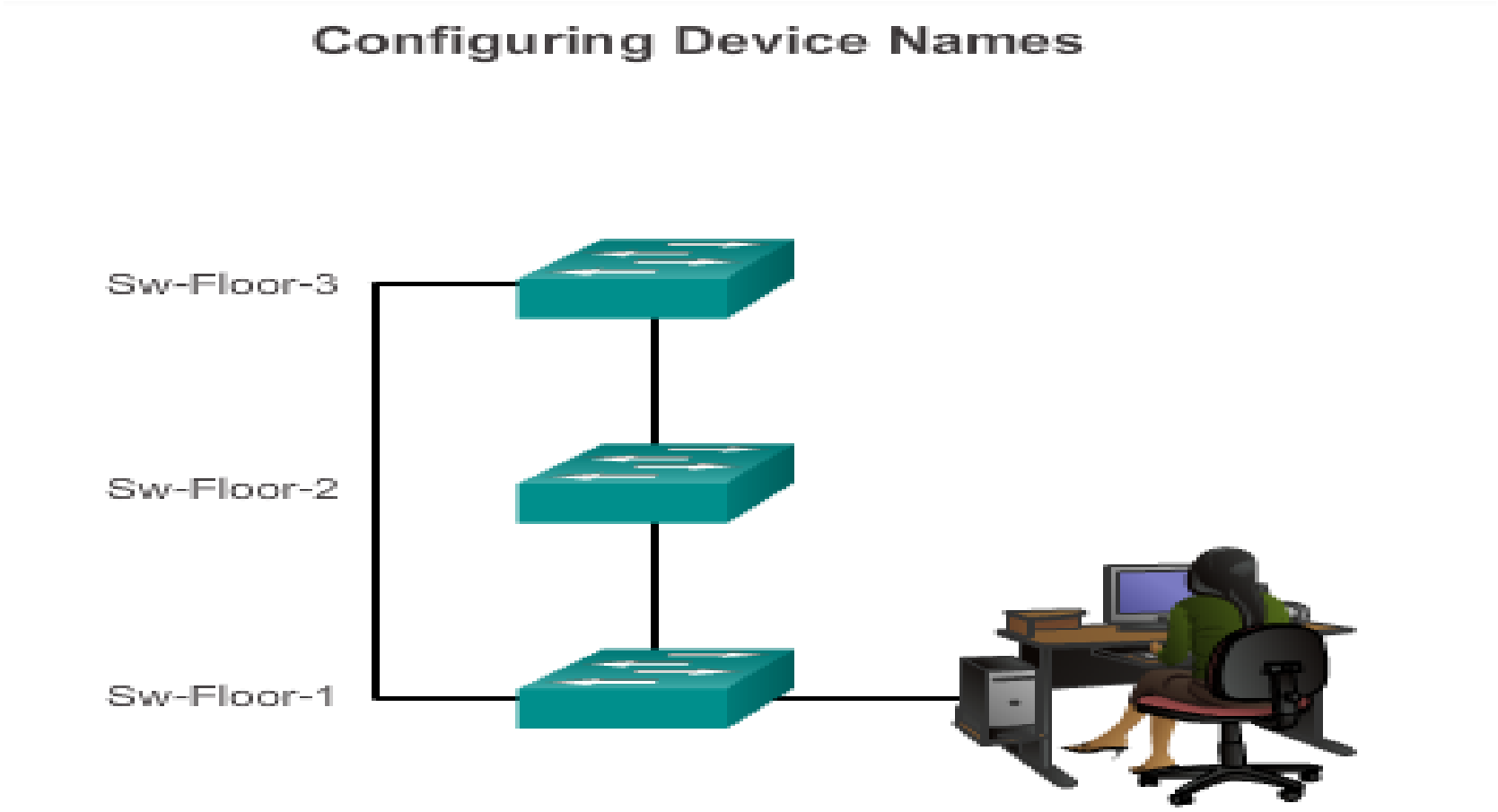
- Start with a letter
- Contain no spaces
- End with a letter or digit
- **Use only letters, digits, and dashes**
- Be less than 64 characters in length

Without names, network devices are difficult to identify for configuration purposes.

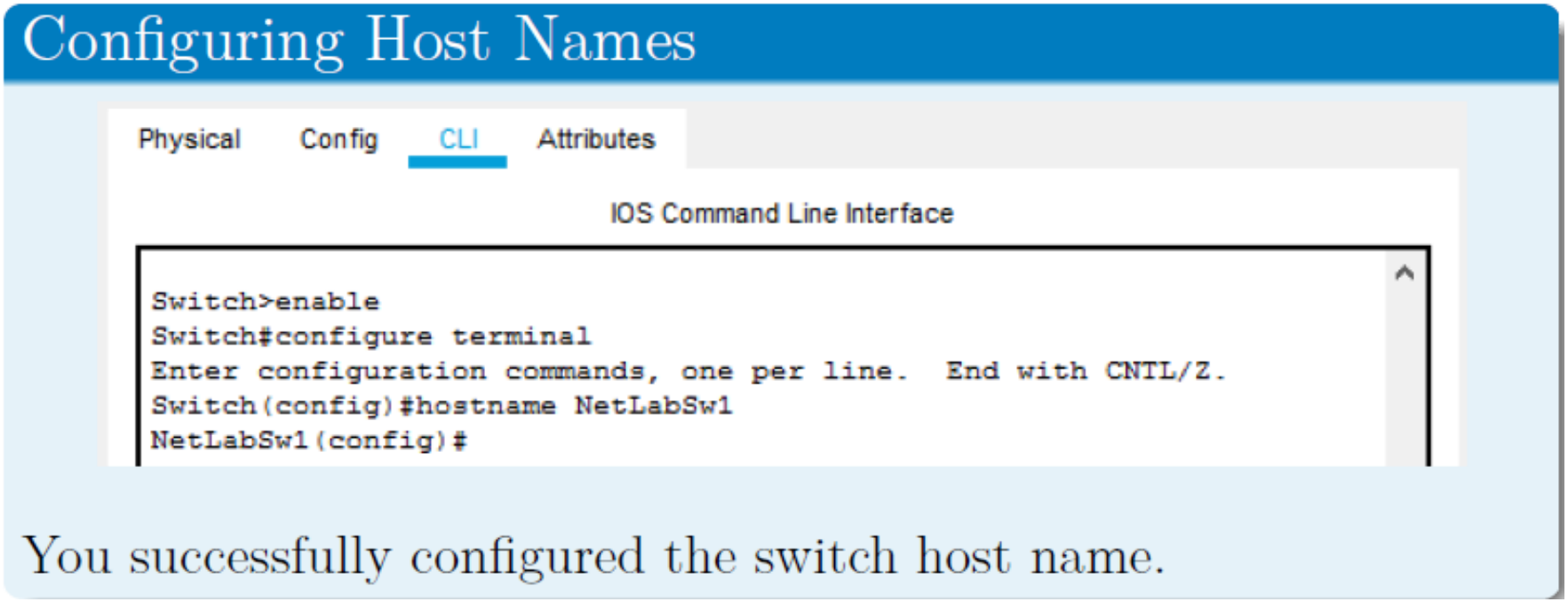


Device Names (Hostnames)…

- Hostnames allow devices to be identified by network administrators over a network or the Internet.



Configuring Host names



Limiting Access to Device Configurations

Securing Device Access

The passwords introduced here are:

- **Enable password** - Limits access to the privileged EXEC mode
- **Enable secret** - Encrypted, limits access to the privileged EXEC mode
- **Console password** - Limits device access using the console connection
- **VTY password** - Limits device access over Telnet

Securing Device Access

- Consider these key points when choosing passwords:
  - Use passwords that are more than eight characters in length.
  - Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences in passwords.
  - Avoid using the same password for all devices.
  - Avoid using common words such as **password** or **administrator**, because these are easily guessed

Note: In most of the labs in this course, we will be using simple passwords such as **cisco** or **class**.

Securing Privileged EXEC Access

- use the **enable secret** command, not the older **enable** password command
- **enable secret** provides greater security because the password is encrypted

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

Securing User EXEC Access…

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

- Console port must be secured
  - reduces the chance of unauthorized personnel physically plugging a cable into the device and gaining device access
- vty lines allow access to a Cisco device via Telnet
  - number of vty lines supported varies with the type of device and the IOS version

Service Password-Encryption command

- prevents passwords from showing up as plain text when viewing the configuration
- purpose of this command is to keep unauthorized individuals from viewing passwords in the configuration file
- once applied, removing the encryption service does not reverse the encryption

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable secret class
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show running-config
Building configuration...

Current configuration : 1127 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

Limiting Access to Device Configurations

Banner Messages

- Allows you to configure messages that anyone logging onto the switch sees.
- Important part of the legal process in the event that someone is prosecuted for breaking into a device.
- Wording that implies for a login is "welcome" or "invited" is not appropriate.
- Often used for legal notification because it is displayed to all connected terminals.
- Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.

MOTD Banner

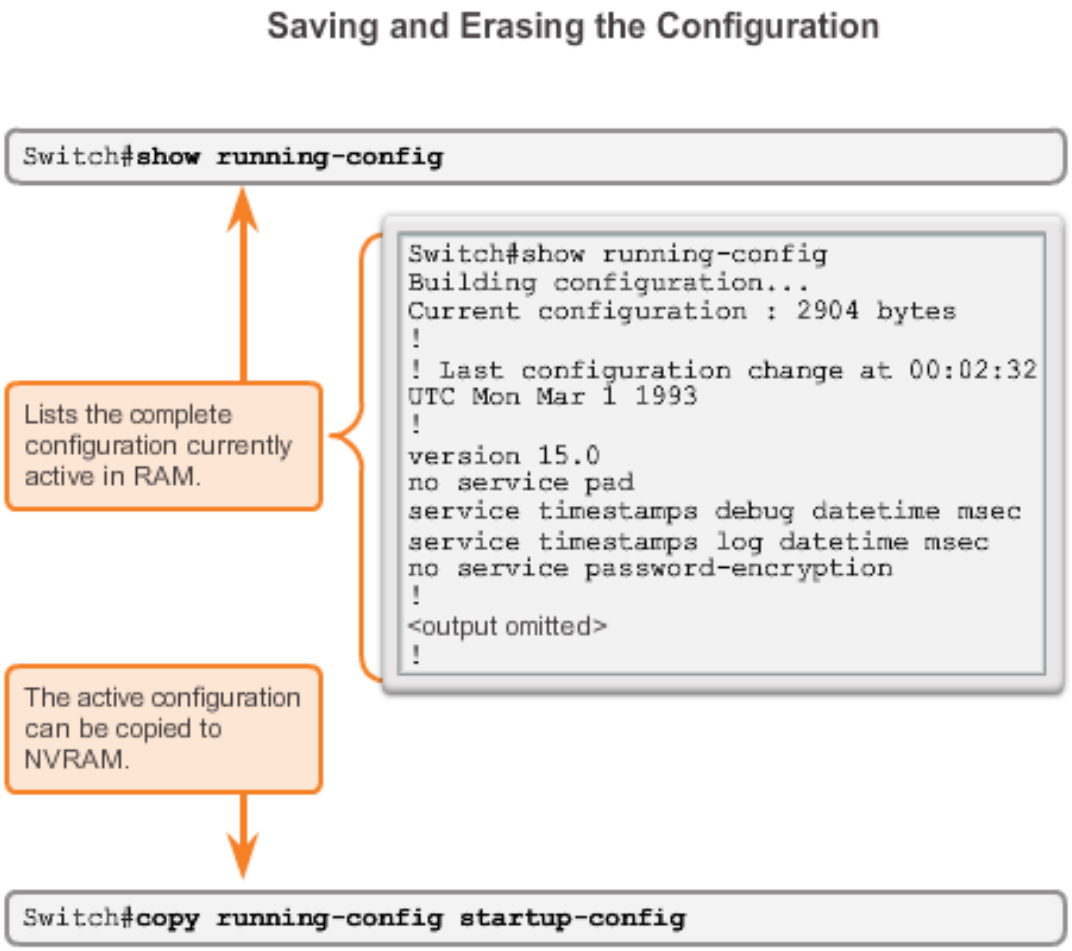
banner motd command...

```
NetLabSw1(config)#banner motd "This is a secure system. Authorized
Access Only!"
NetLabSw1(config)#exit
NetLabSw1#
```

MOTD Display

```
NetLabSw1 con0 is now available



Press RETURN to get started.









This is a secure system. Authorized Access Only!

NetLabSw1>
```

Configuration Files



- Switch# **reload**
  - –System configuration has been modified. Save? [yes/no]: **n**
  - –Proceed with reload? [confirm]
- Startup configuration is removed by using the **erase startup-config**
  - –Switch# **erase startup-config**
- On a switch you must also issue the **delete vlan.dat**
  - – Switch# **delete vlan.dat**
  - – Delete filename [vlan.dat]?
  - –Delete flash:vlan.dat? [confirm]

Preparing for Basic Switch Management

- In order to remotely manage a Cisco switch, it needs to be configured to access the network
- An IP address and a subnet mask must be configured
- If managing the switch from a remote network, a default gateway must also be configured
- The IP information (address, subnet mask, gateway) is to be assigned to a switch SVI (switch virtual interface)
- Although these IP settings allow remote management and remote access to the switch, they do not allow the switch to route Layer 3 packets.

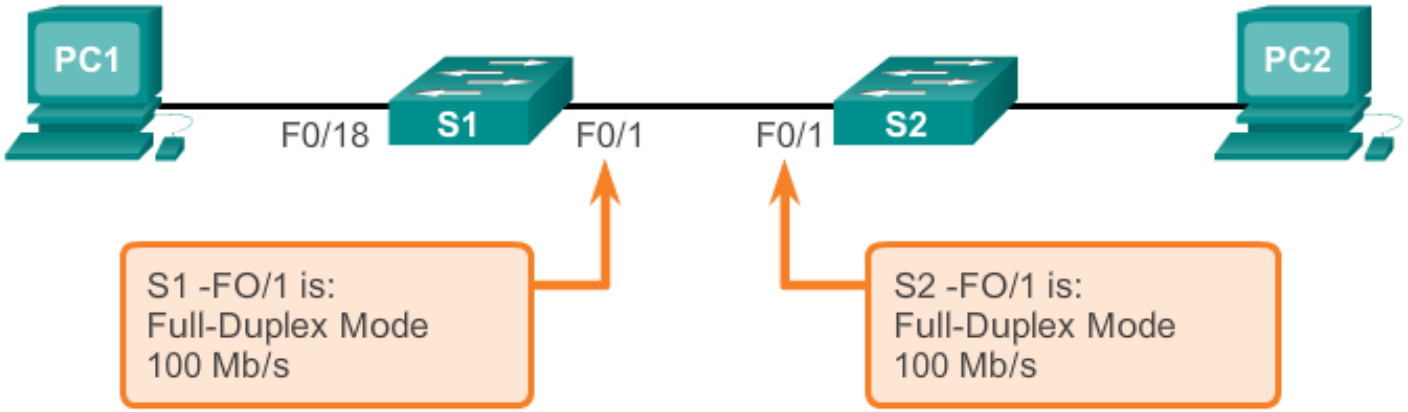
Preparing for Basic Switch Management

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode for the SVI.	S1(config)# **interface vlan99**
Configure the management interface IP address.	S1(config-if)# **ip address 172.17.99.11**
Enable the management interface.	S1(config-if)# **no shutdown**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Configure the default gateway for the switch.	S1(config)# **ip default-gateway 172.17.99.**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Configure Switch Ports at the Physical Layer

Configure Duplex and Speed



Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface fastethernet 0/1**
Configure the interface duplex.	S1(config-if)# **duplex full**
Configure the interface speed.	S1(config-if)# **speed 100**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Configure Switch Ports

Verifying Switch Port Configuration

Verification Commands

Cisco Switch IOS Commands	
Display interface status and configuration.	S1# **show interfaces [interface-id]**
Display current startup configuration.	S1# **show startup-config**
Display current operating config.	S1# **show running-config**
Displays info about flash filesystem.	S1# **show flash**
Displays system hardware & software status.	S1# **show version**
Display history of commands entered.	S1# **show history**
Display IP information about an interface.	S1# **show ip [interface-id]**
Display the MAC address table.	S1# **show mac-address-table**

Configure Switch Ports

Network Access Layer Issues

Display interface status and statistics.

```
S1# show interface FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast
Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec,
<...output omitted...>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0
  throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 multicast, 0 pause input
  0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
  8 output errors,1790 collisions,10 interface resets
  0 unknown protocol drops
  0 babbles, 235 late collision, 0 deferred
<output omitted>
```

Network Access Layer Issues

Parameter	Description
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Input errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
CRC	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	Number of messages retransmitted because of an Ethernet collision.
Late collisions	Jammed signal could not reach to ends.

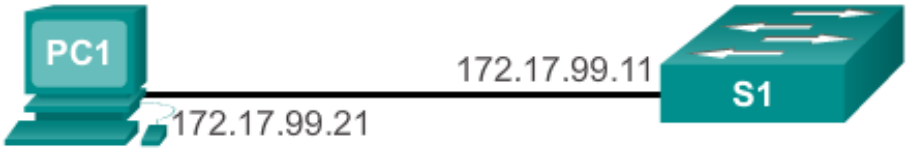
Secure Remote Access

SSH Operation

- Secure Shell (SSH) is a protocol that provides a secure (encrypted) command-line based connection to a remote device
- SSH is commonly used in UNIX-based systems
- Cisco IOS also supports SSH
- A version of the IOS software including cryptographic (encrypted) features and capabilities is required in order to enable SSH on Catalyst 2960 switches
- Because its strong encryption features, SSH should replace Telnet for management connections
- SSH uses TCP port 22 by default. Telnet uses TCP port 23

Secure Remote Access

SSH Operation

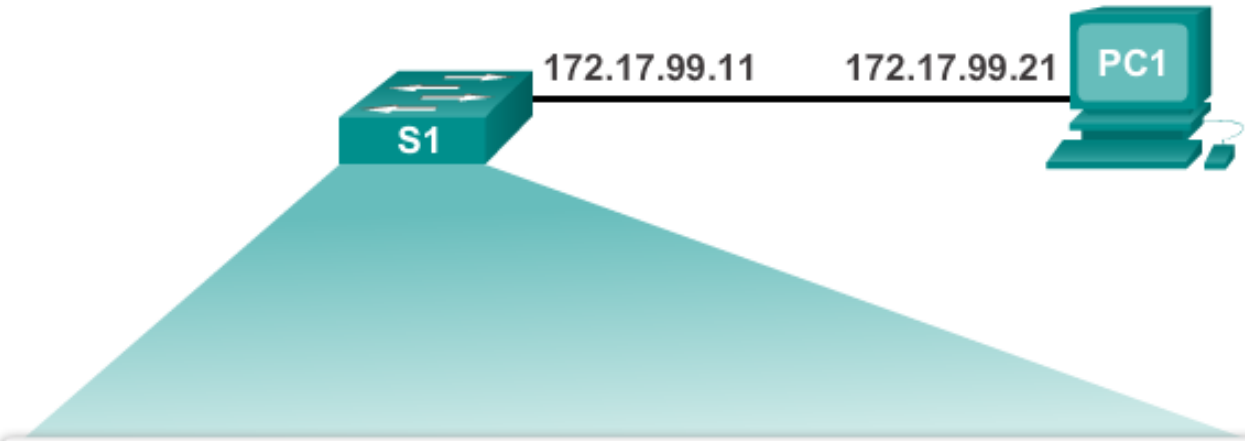


172.17.99.11 - PuTTY

```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

Secure Remote Access

Configuring SSH




```
S1 # configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```

Security Concerns in LANs

- Switches automatically populate their **CAM (Content Addressable Memory)** tables by watching traffic entering their ports
- Switches will forward traffic trough all ports if it can't find the destination MAC in its CAM table
- Under such circumstances, the switch acts as a hub.
- Unicast traffic can be seen by all devices connected to the switch
- An attacker could exploit this behavior to gain access to traffic normally controlled by the switch by using a PC to run a MAC flooding tool.
- Such tools is a program created to generate and send out frames with bogus source MAC addresses to the switch port.

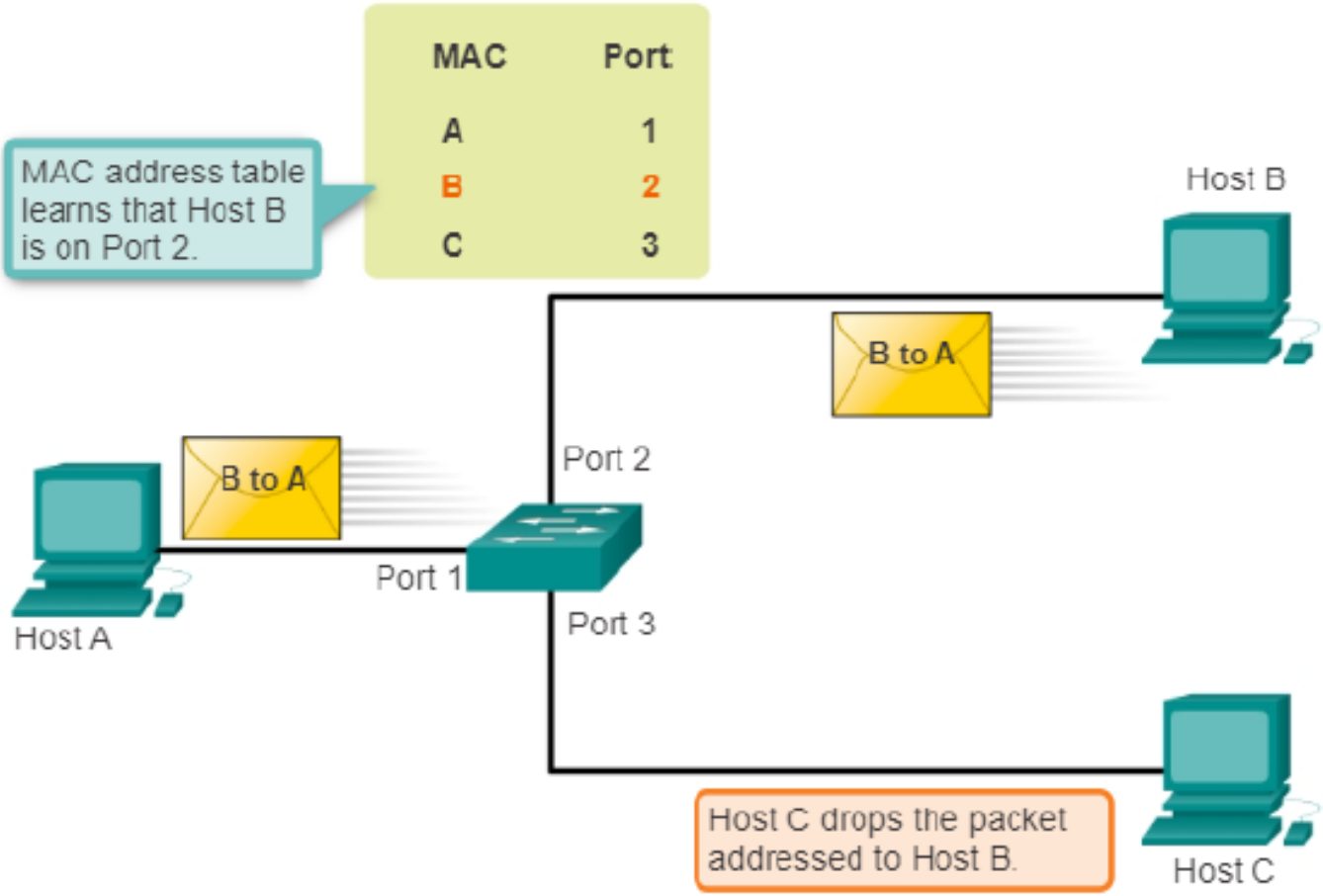
Security Concerns in LANs

MAC Address Flooding

- Such tool is a program created to generate and send out frames with bogus source MAC addresses to the switch port
- As these frames reach the switch, it adds the bogus MAC address to its CAM table, taking note of the port the frames arrived
- Eventually the CAM table fills out with bogus MAC addresses
- The CAM table now has no room for legit devices present in the network and therefore will never find their MAC addresses in the CAM table.
- All frames are now forwarded to all ports, allowing the attacker to access traffic to other hosts

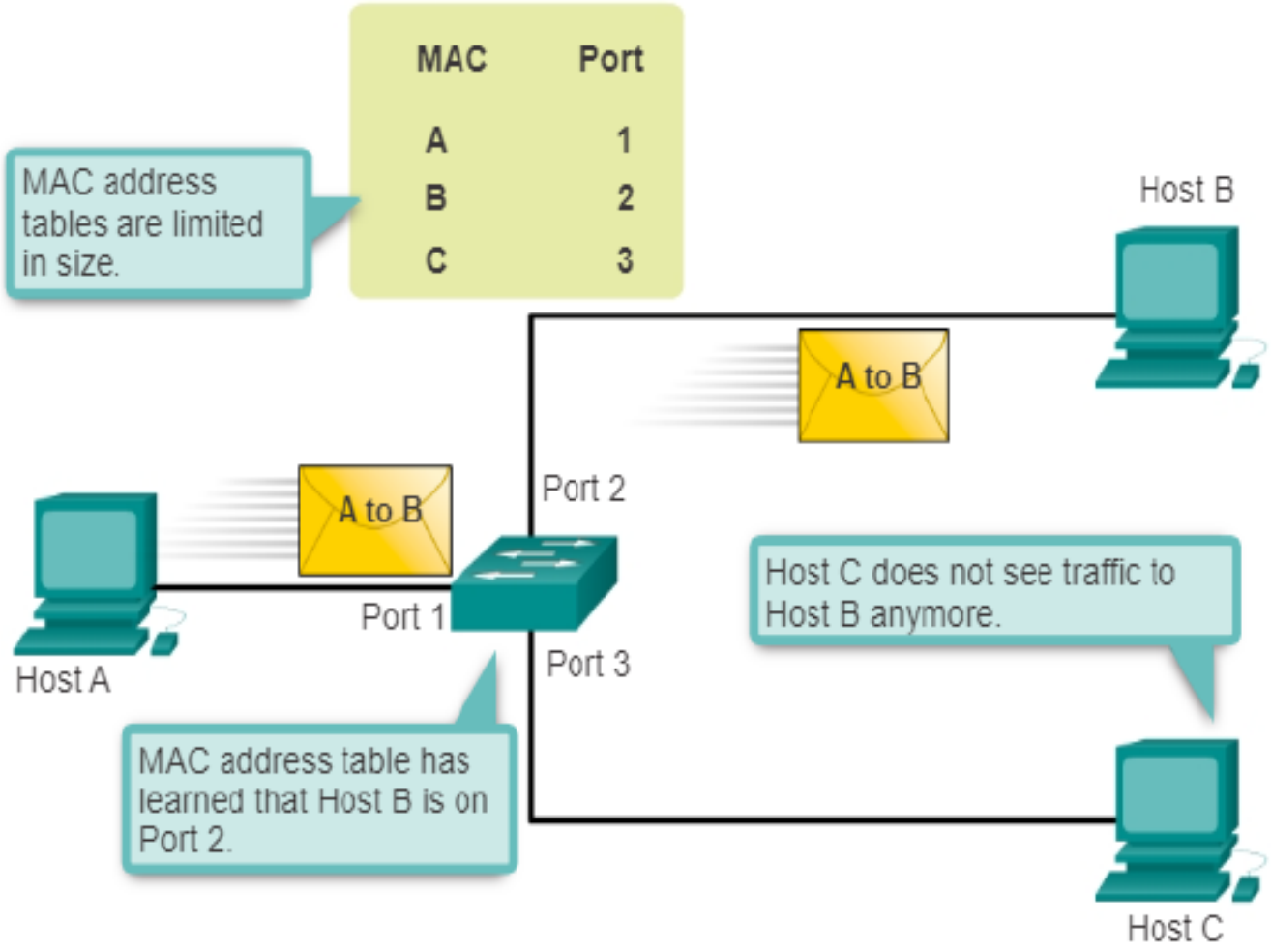
MAC Address Flooding….

- Switch records MAC address



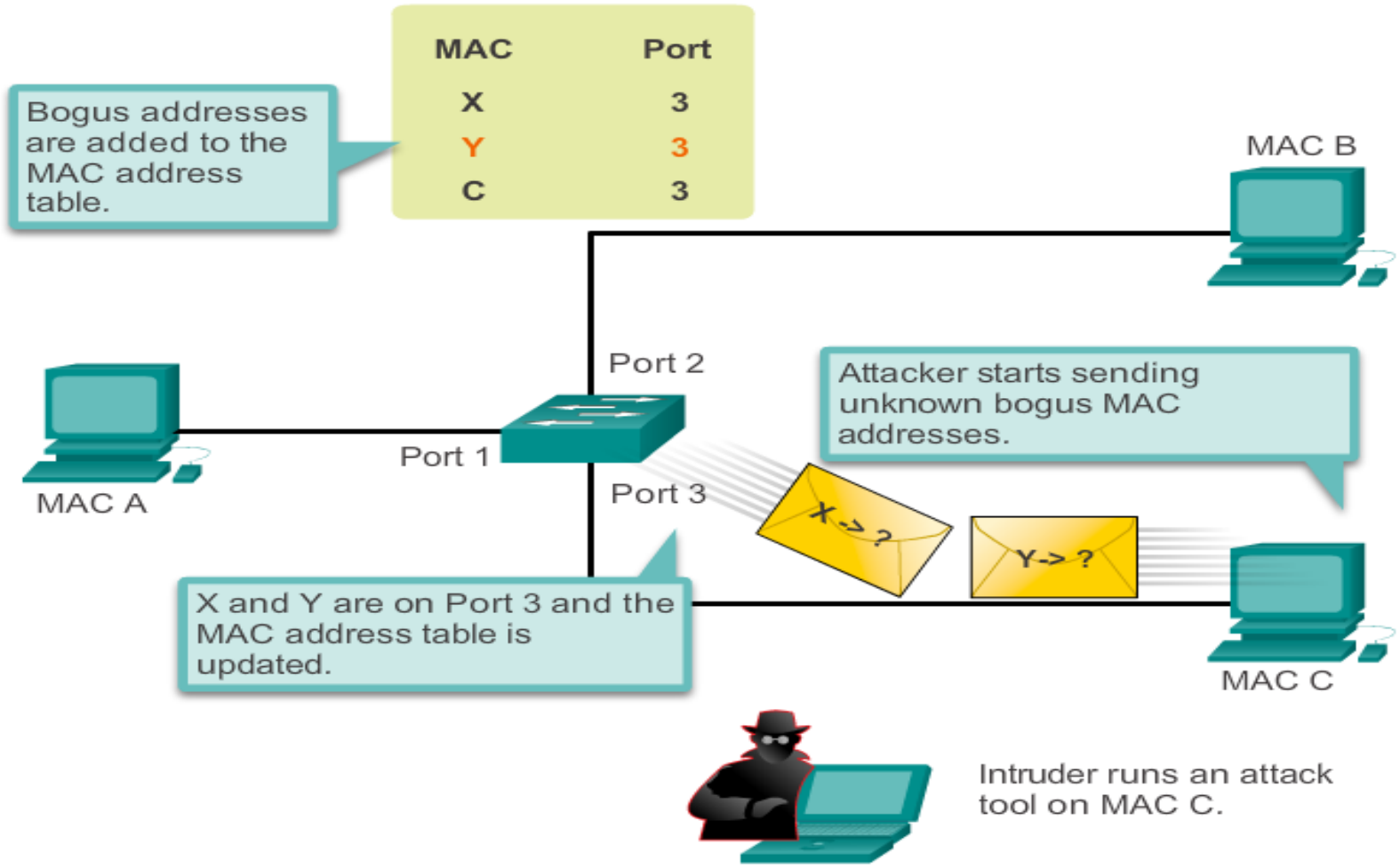
MAC Address Flooding….

- Switch Uses MAC Address Table to Forward Traffic



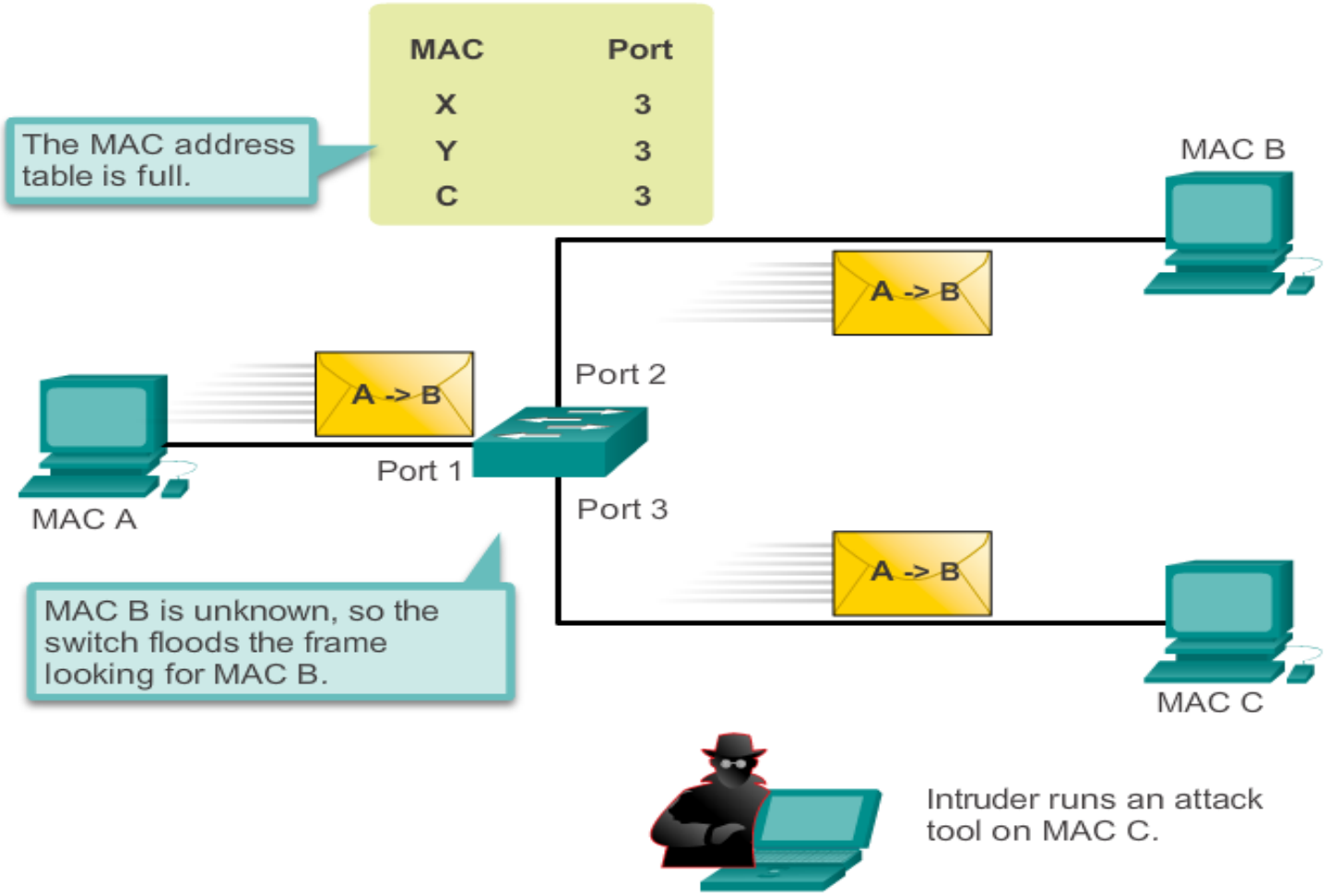
MAC Address Flooding….

- Attacker flooding the CAM table with bogus entries



MAC Address Flooding….

- The switch now behaves as a hub



Security Best Practices

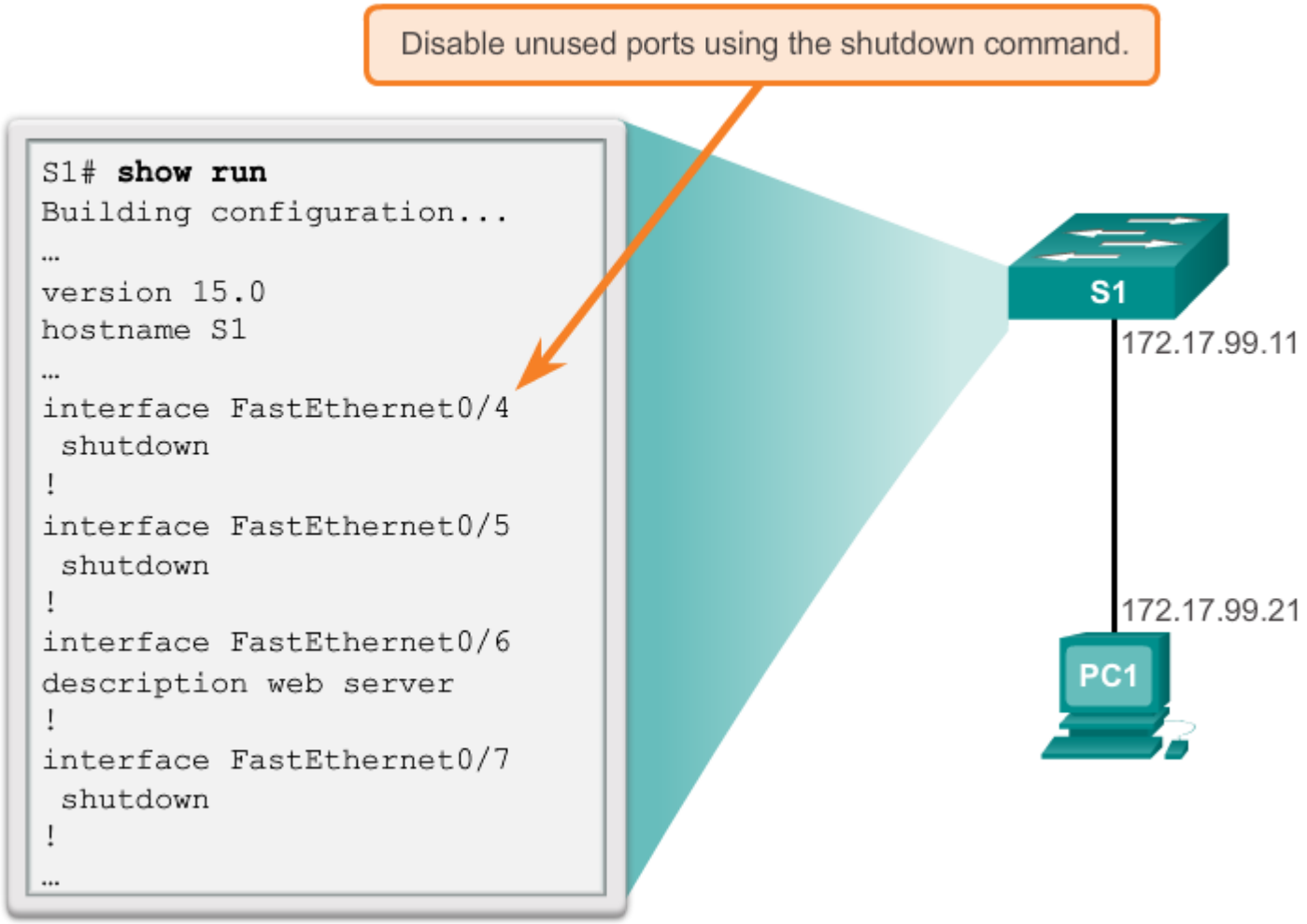
10 Best Practices

- Develop a written security policy for the organization
- Shut down unused services and ports
- Use strong passwords and change them often
- Control physical access to devices
- Use HTTPS instead of HTTP
- Perform backups operations on a regular basis.
- Educate employees about social engineering attacks
- Encrypt and password-protect sensitive data
- Implement firewalls.
- Keep software up-to-date

Switch Port Security

Secure Unused Ports

- Disable Unused Ports is a simple yet efficient security guideline



Switch Port Security

Port Security: Operation

- Port security limits the number of valid MAC addresses allowed on a port
- The MAC addresses of legitimate devices are allowed access, while other MAC addresses are denied
- Any additional attempts to connect by unknown MAC addresses will generate a security violation
- Secure MAC addresses can be configured in a number of ways:
  - Static secure MAC addresses
  - Dynamic secure MAC addresses
  - Sticky secure MAC addresses

Types of Secure MAC address

1. Static secure MAC addresses

- Statically configured on a switch port
- Stored in an address table and in the running configuration

2. Dynamic Secure MAC Address

- Learned dynamically from the traffic that is sent through the switch port
- Kept only in an address table and not in the running configuration

3. Sticky secure MAC addresses

- Can be manually configured or dynamically learned
- Kept in an address table and in the running configuration

Switch Port Security

Port Security: Violation Modes

- IOS considers a security violation when either of these situations occurs:
  - The maximum number of secure MAC addresses for that interface have been added to the CAM, and a station whose MAC address is not in the address table attempts to access the interface.
  - An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.
- There are three possible action to be taken when a violation is detected:
  - Protect
  - Restrict
  - Shutdown

Action to be taken when a violation is detected

1. Protect

- This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses when over the allowed MAC address limit
- When configured with this mode, no notification action is taken when traffic is dropped

2. Restrict

- This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses when over the allowed MAC address limit
- When configured with this mode, a syslog message is logged, a SNMP trap is sent, and a violation counter is incremented when traffic is droppedSwitch

Action to be taken when a violation is detected

3. Shutdown

- This mode is the default violation mode; when in this mode, the switch will automatically force the switch port into an error disabled state when a violation occurs.
- While in this state, the switch port forwards no traffic.
- The switch port can be brought out of this error disabled state by issuing the error disable recovery cause CLI command or by disabling and re-enabling the switch port

Switch Port Security

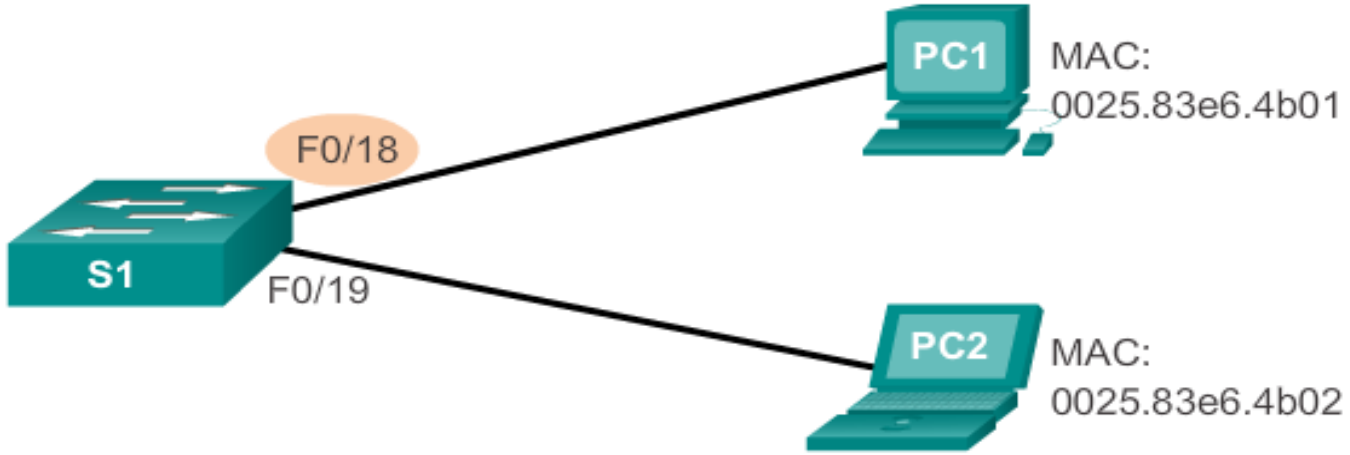
- **Port Security: Configuring**
- Dynamic Port Security Defaults

Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

Switch Port Security

Port Security: Configuring

- Configuring Dynamic Port Security

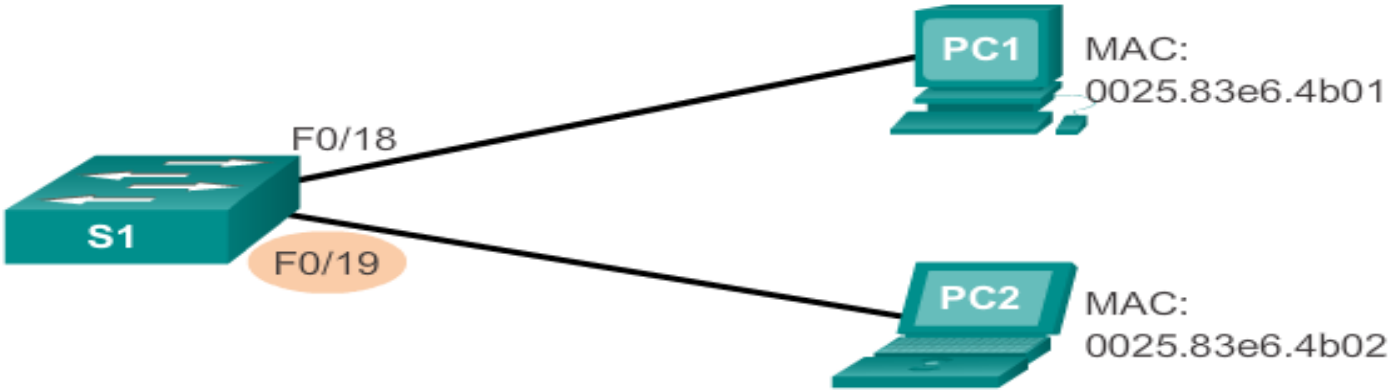


Cisco IOS CLI Commands	
S1(config)#**interface fastethernet 0/18**	Specify the interface to be configured for port security.
S1(config-if)#**switchport mode access**	Set the interface mode to access.
S1(config-if)#**switchport port-security**	Enable port security on the interface.

Switch Port Security

Port Security: Configuring

- Configuring Port Security Sticky



Cisco IOS CLI Commands	
S1(config)#**interface fastethernet 0/18**	Specify the interface to be configured for port security.
S1(config-if)#**switchport mode access**	Set the interface mode to access.
S1(config-if)#**switchport port-security**	Enable port security on the interface.
S1(config-if)#**switchport port-security maximum 50**	Set the maximum number of secure addresses allowed on the port.
S1(config-if)#**switchport port-security mac-address sticky**	Enable sticky learning.

Switch Port Security

Port Security: Verifying

- Verifying Port Security Sticky


```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```

Switch Port Security

Port Security: Verifying

- Verifying Port Security Sticky – Running Config


```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Switch Port Security…

Port Security: Verifying

- Verifying Port Security Secure MAC Addresses


```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports    Remaining Age
                                                          (mins)
----    -----------       ----                -----    -------------
1       0025.83e6.4b01    SecureDynamic       Fa0/18       -
1       0025.83e6.4b02    SecureSticky        Fa0/19       -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port
```

Switch Port Security

Ports In Error Disabled State

- A port security violation can put a switch in error disabled state
- A port in error disabled is effectively shut down
- The switch will communicate these events through console messages

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

Switch Port Security

Ports In Error Disabled State

- The show interface command also reveals a switch port on error disabled state

```
S1# show interface fa0/18 status
Port Name  Status         Vlan  Duplex  Speed   Type
Fa0/18     err-disabled   1     auto    auto    10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security                 : Enabled
Port Status                   : Secure-shutdown
Violation Mode                : Shutdown
Aging Time                    : 0 mins
Aging Type                    : Absolute
SecureStatic Address Aging    : Disabled
Maximum MAC Addresses         : 1
Total MAC Addresses           : 0
Configured MAC Addresses      : 0
Sticky MAC Addresses          : 0
Last Source Address:Vlan      : 000c.292b.4c75:1
Security Violation Count      : 1
```

Switch Port Security

Ports In Error Disabled State

- A shutdown/no shutdown interface command must be issued to re-enable the port

```
S1(config )#interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```

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.

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.

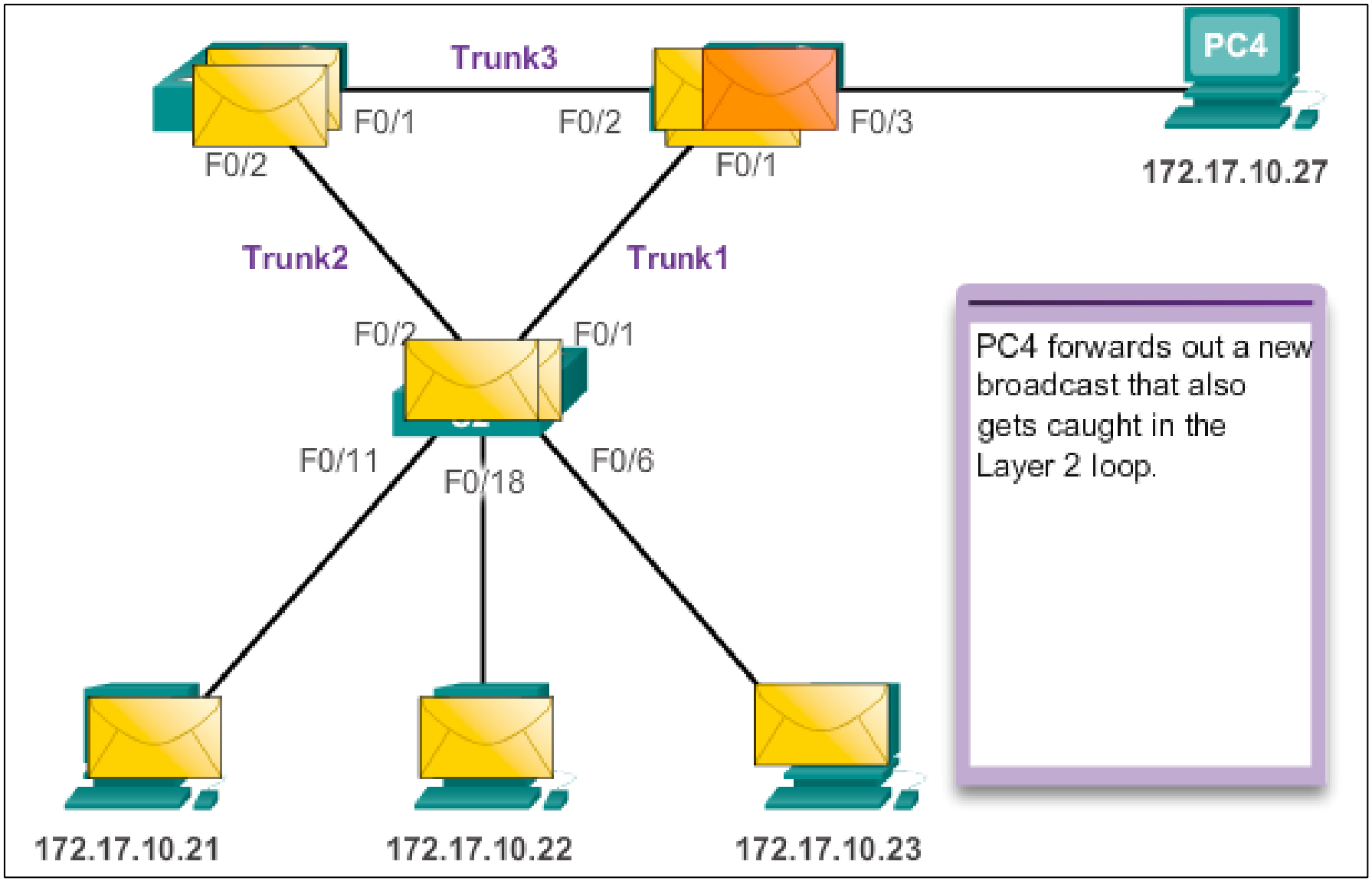
Issues with Layer 1 Redundancy…

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.

Issues with Layer 1 Redundancy…

Broadcast Storm



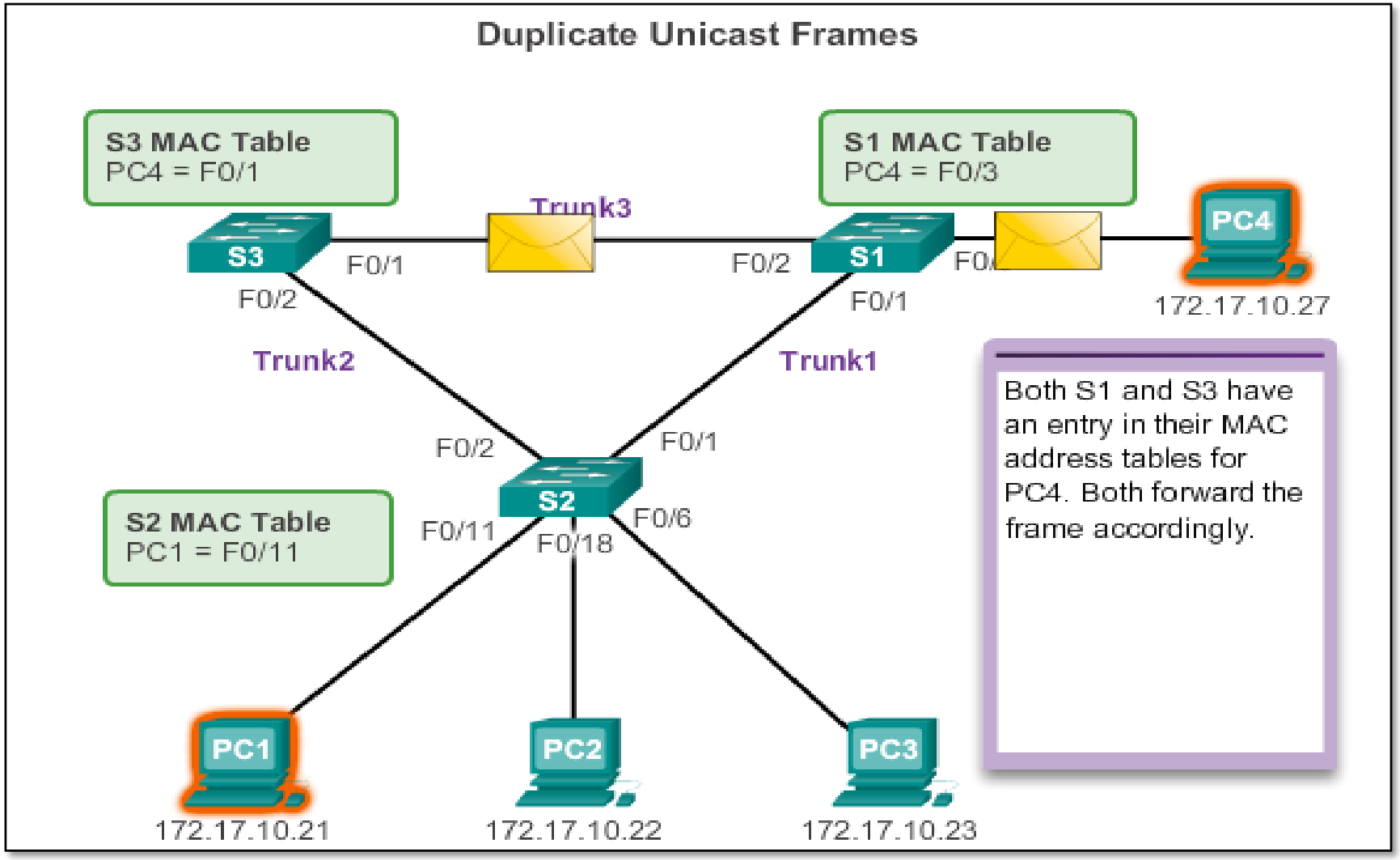
Issues with Layer 1 Redundancy:

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.

Issues with Layer 1 Redundancy….

Duplicate Unicast Frames



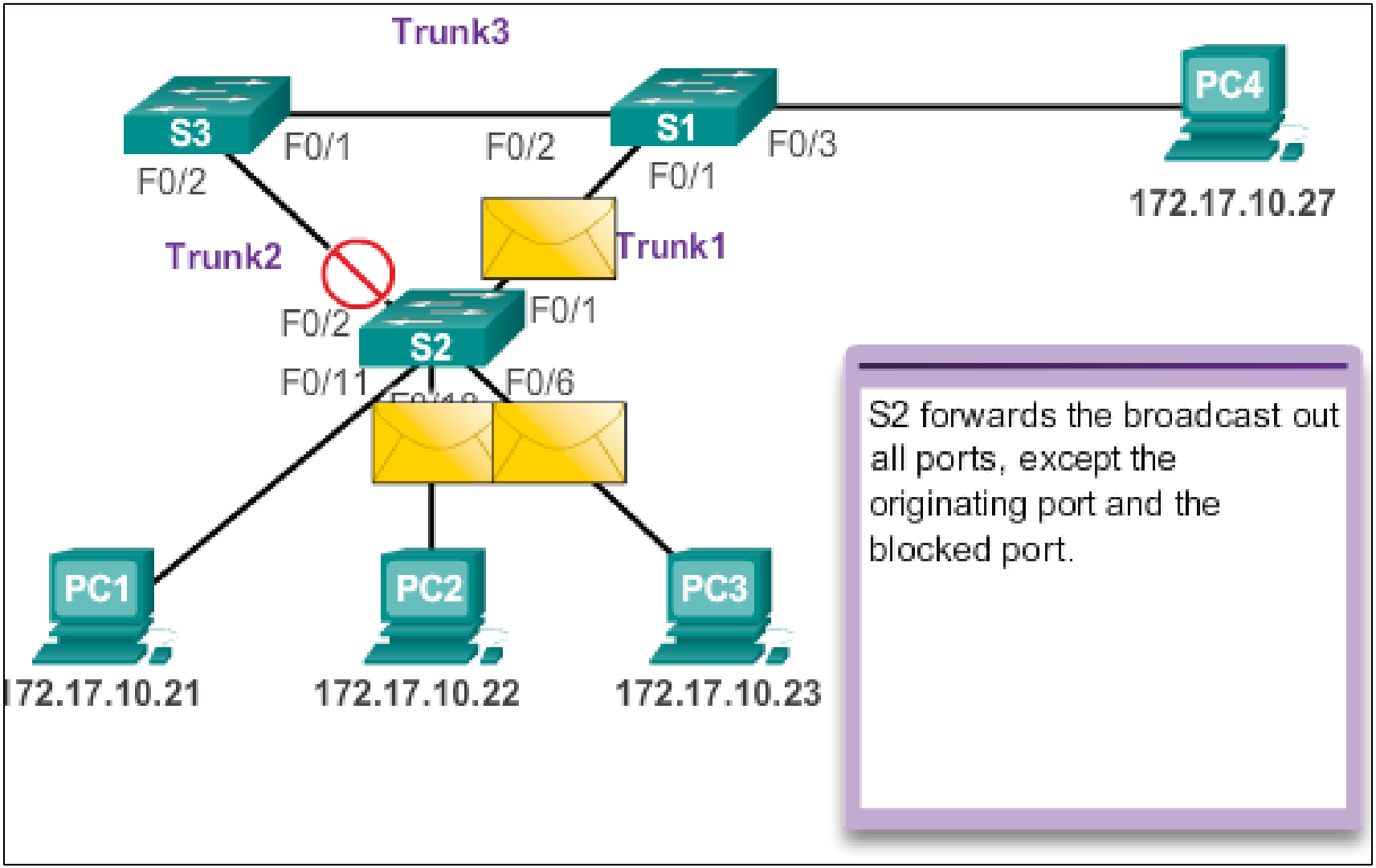
Spanning Tree Algorithm

Introduction

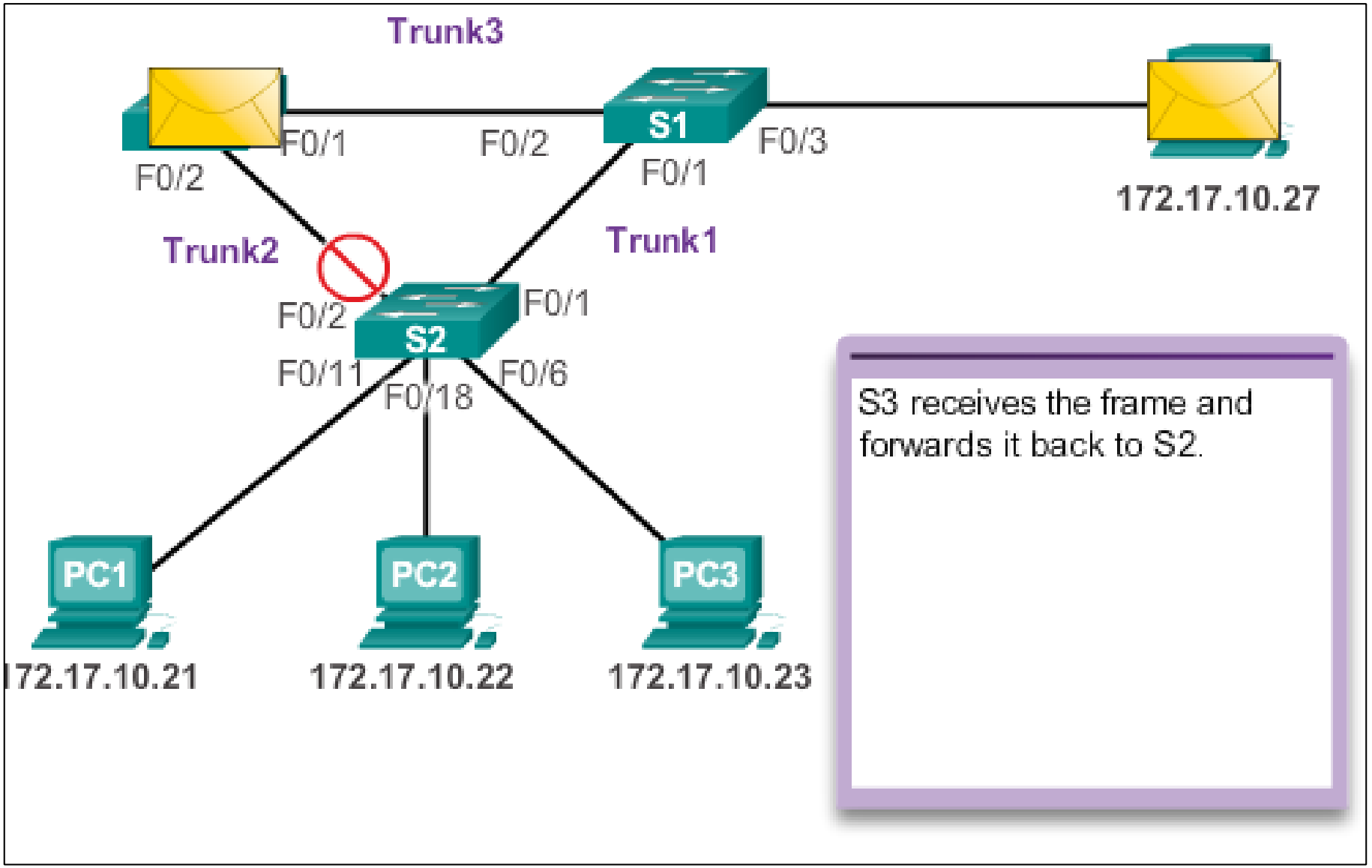
- STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.
- A port is considered blocked when user data is prevented from entering or leaving that port.
- This does not include bridge protocol data unit (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.

Spanning Tree Algorithm

Introduction

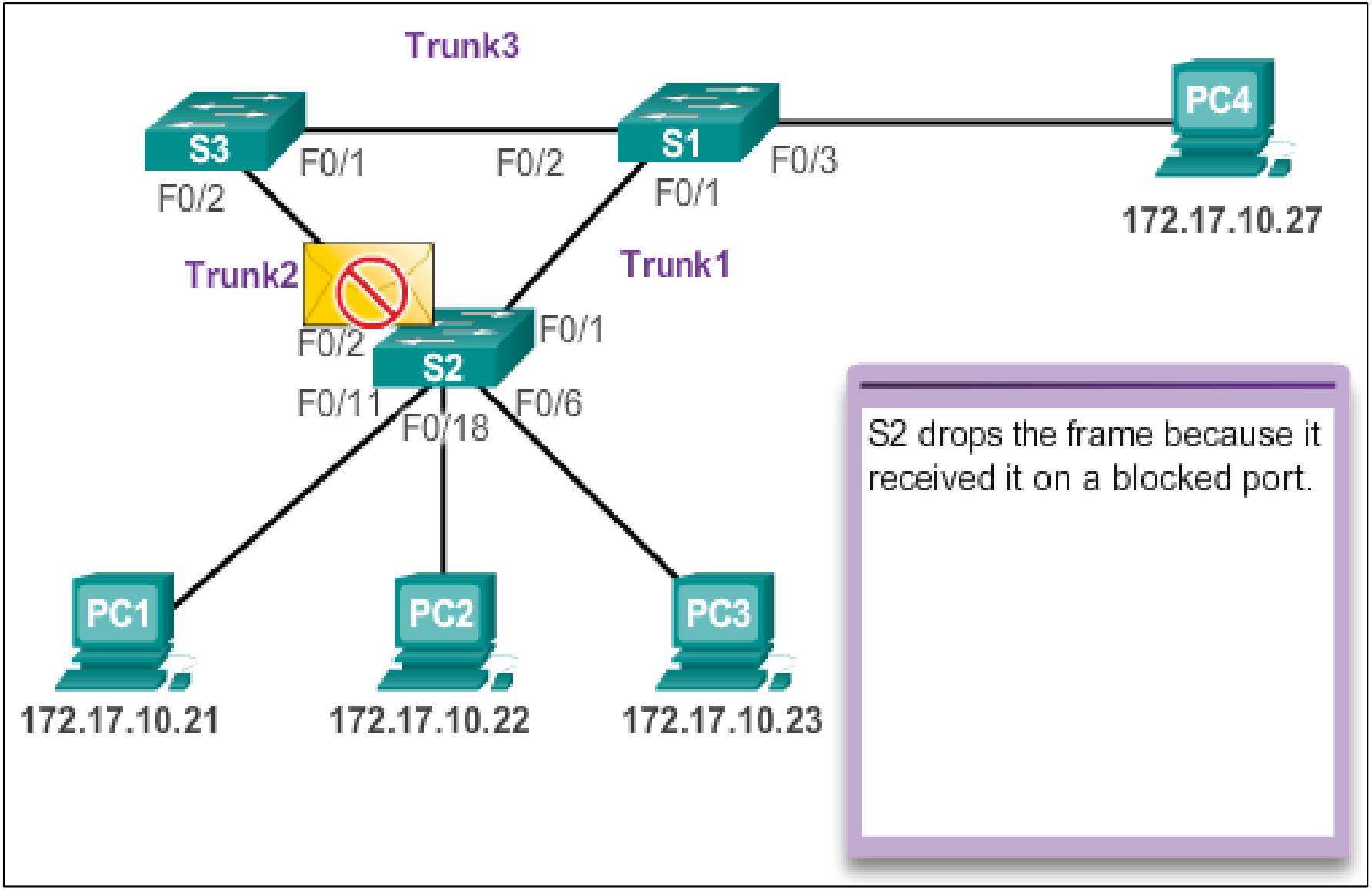


STP Operation
Spanning Tree Algorithm: Introduction

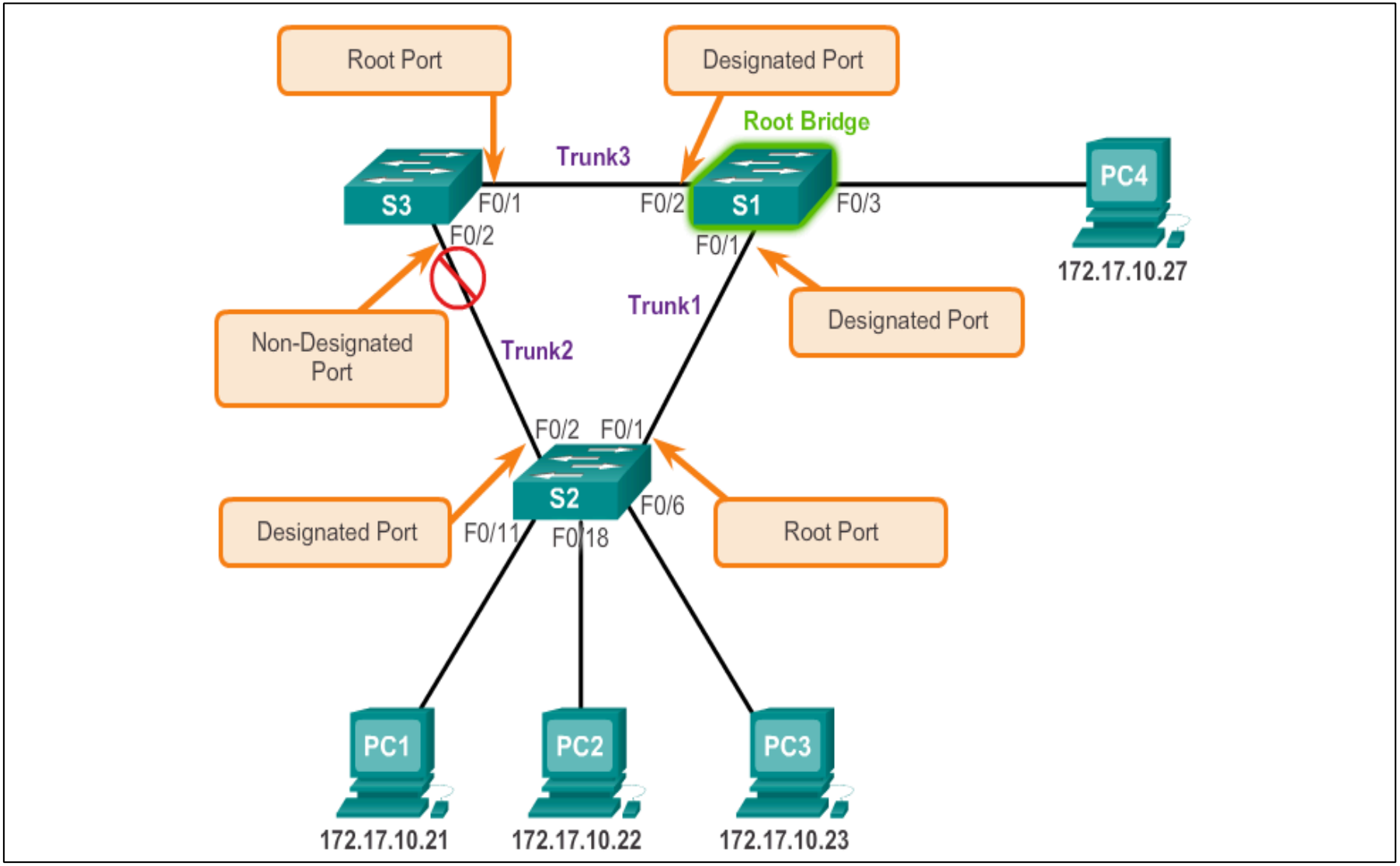


S3 receives the frame and forwards it back to S2.

STP Operation
Spanning Tree Algorithm: Introduction



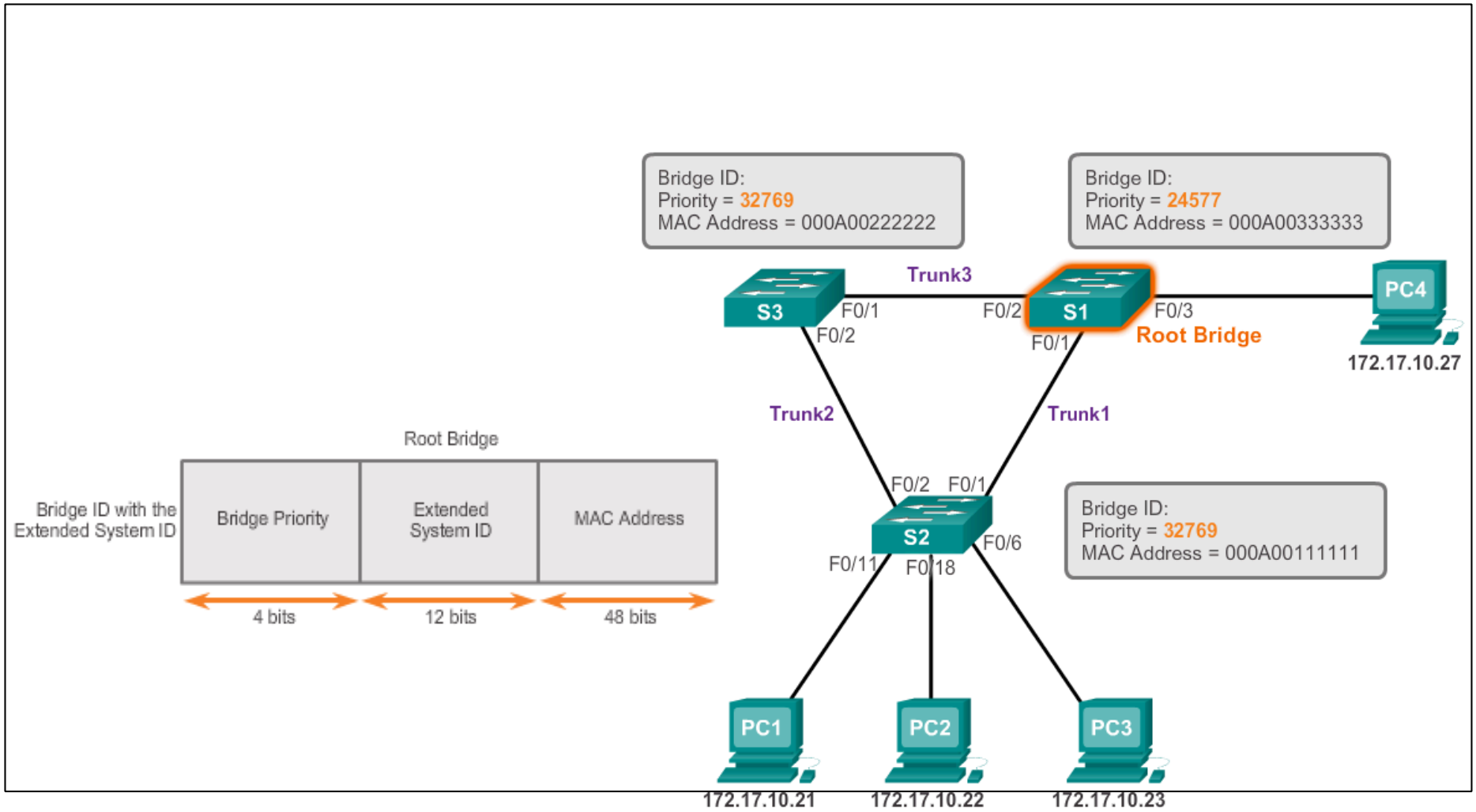
STP Operation
Spanning Tree Algorithm: Port Roles



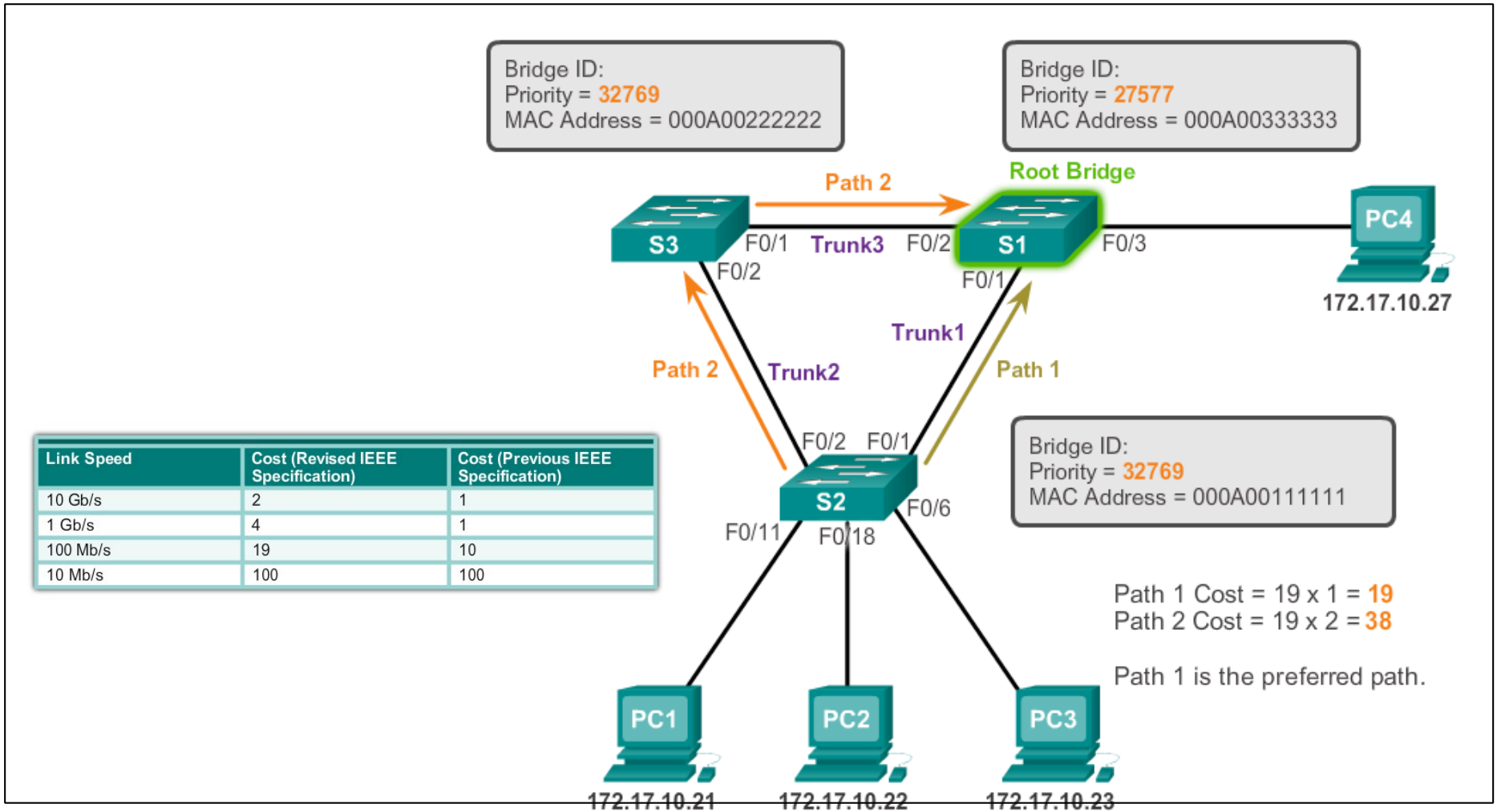
Spanning Tree Algorithm: Port Roles

- **Root -** Ports on non-root switches with the best cost path to root bridge. These ports forward data to the root bridge.
- **Designated** - Ports on root and designated switches. All ports on the root bridge will be designated.
- **Blocked** - All other ports to bridges or switches are in a blocked state. Access ports going to workstations or PCs are not affected.

STP Operation
Spanning Tree Algorithm: Root Bridge

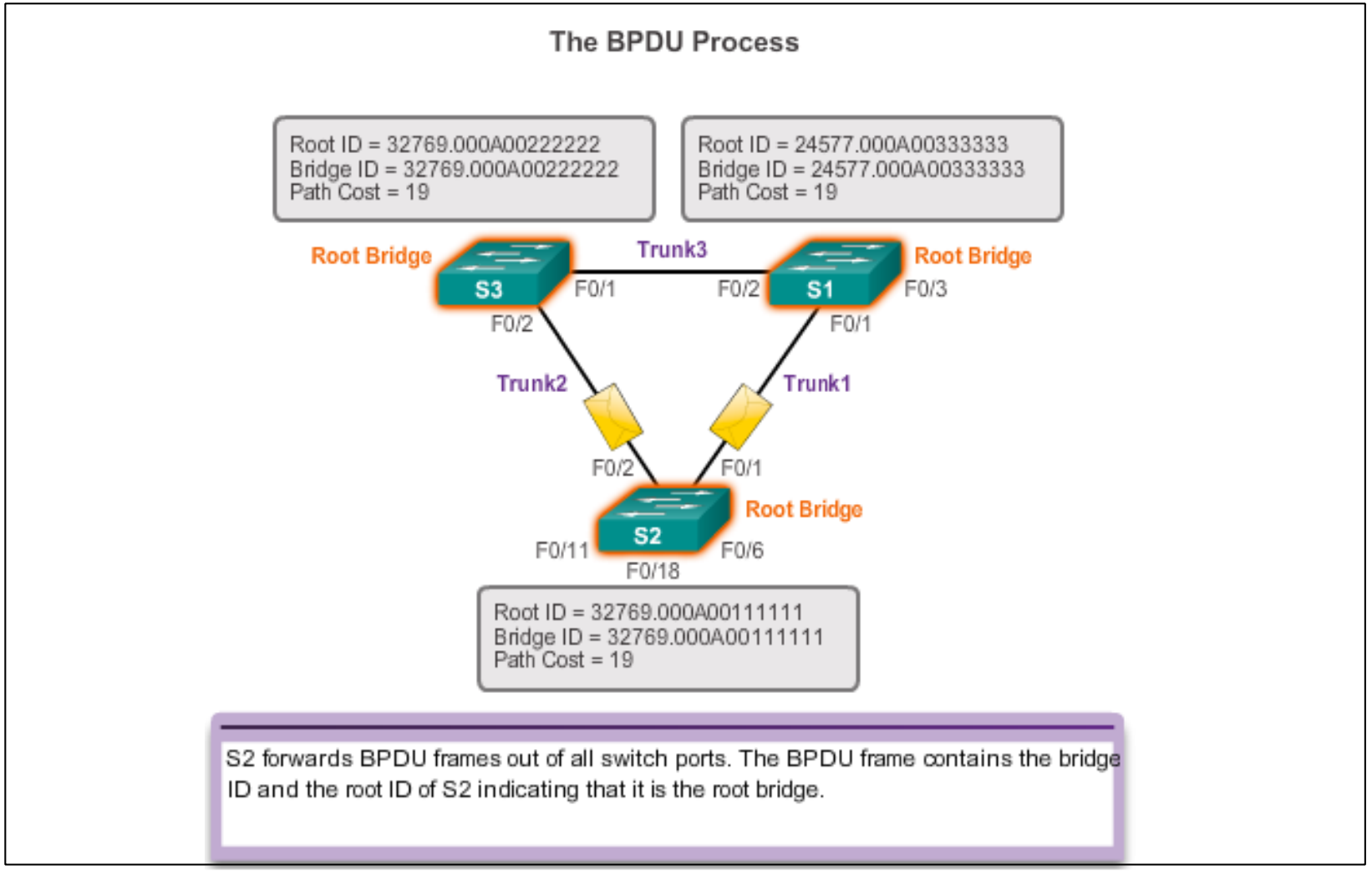


STP Operation
Spanning Tree Algorithm: Path Cost

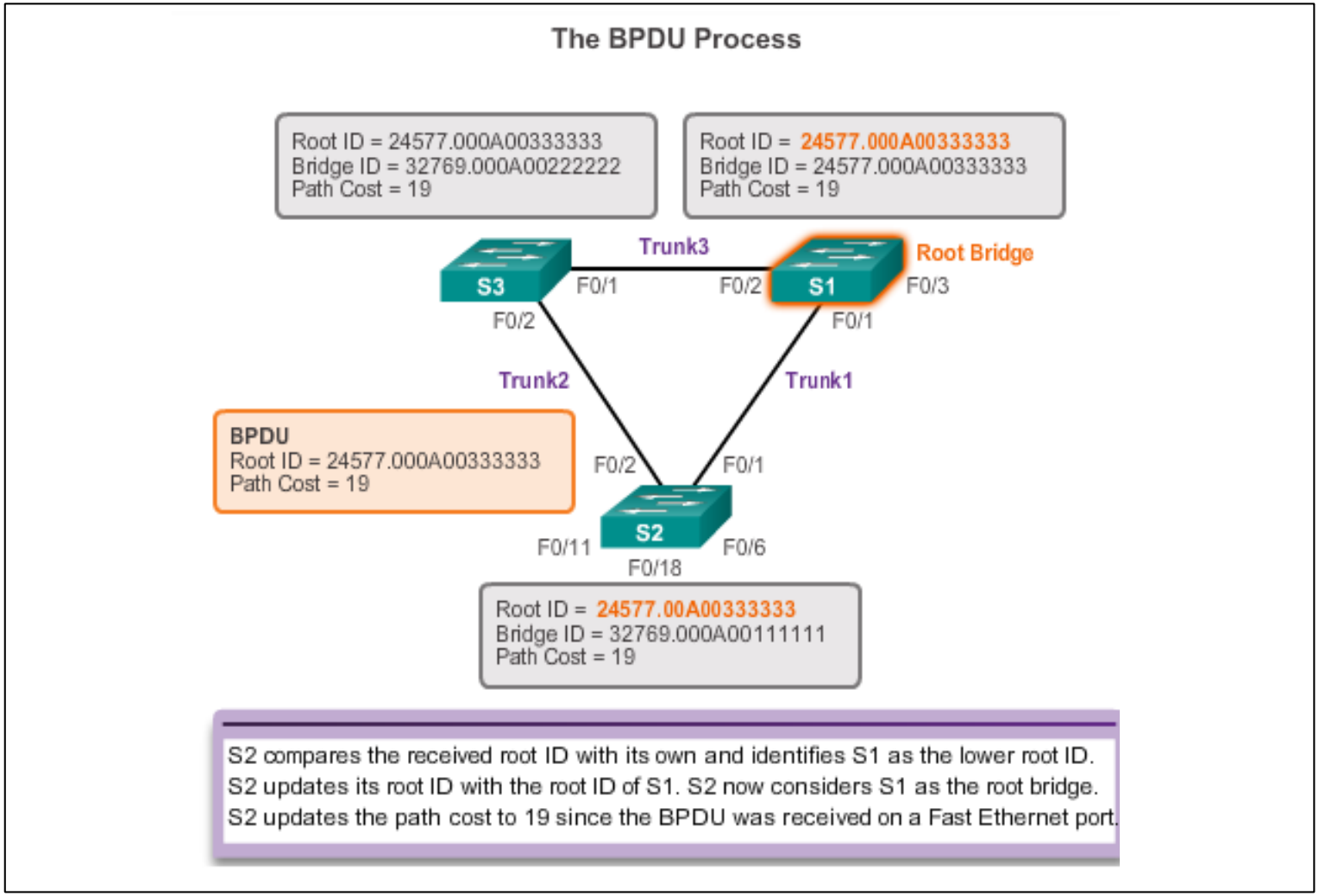


Link Speed	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

STP Operation
BPDU Propagation and Process



STP Operation
BPDU Propagation and Process



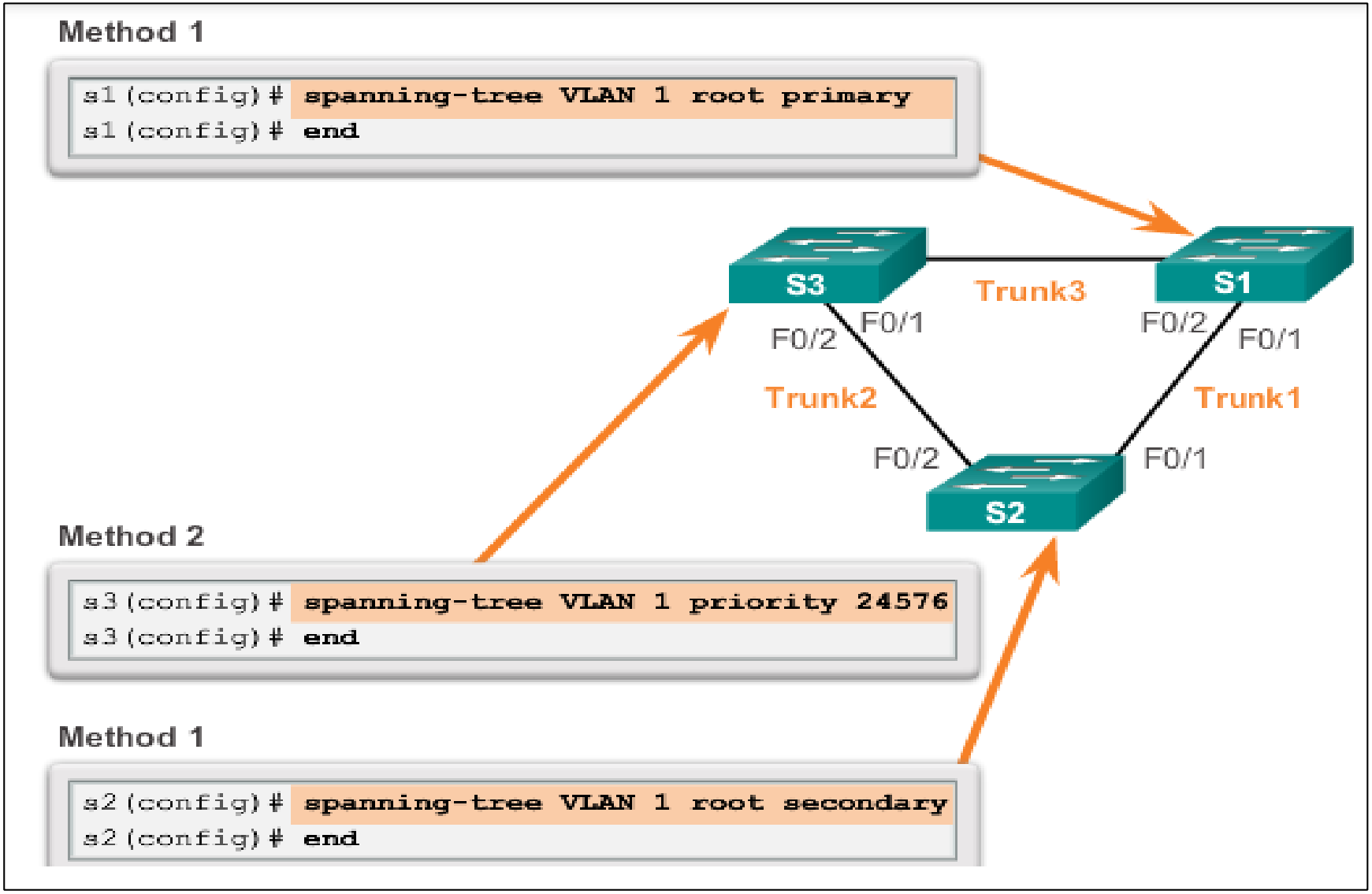
List of Spanning Tree Protocols

- 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

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



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#
```

Rapid PVST+ Configuration
Spanning Tree Mode

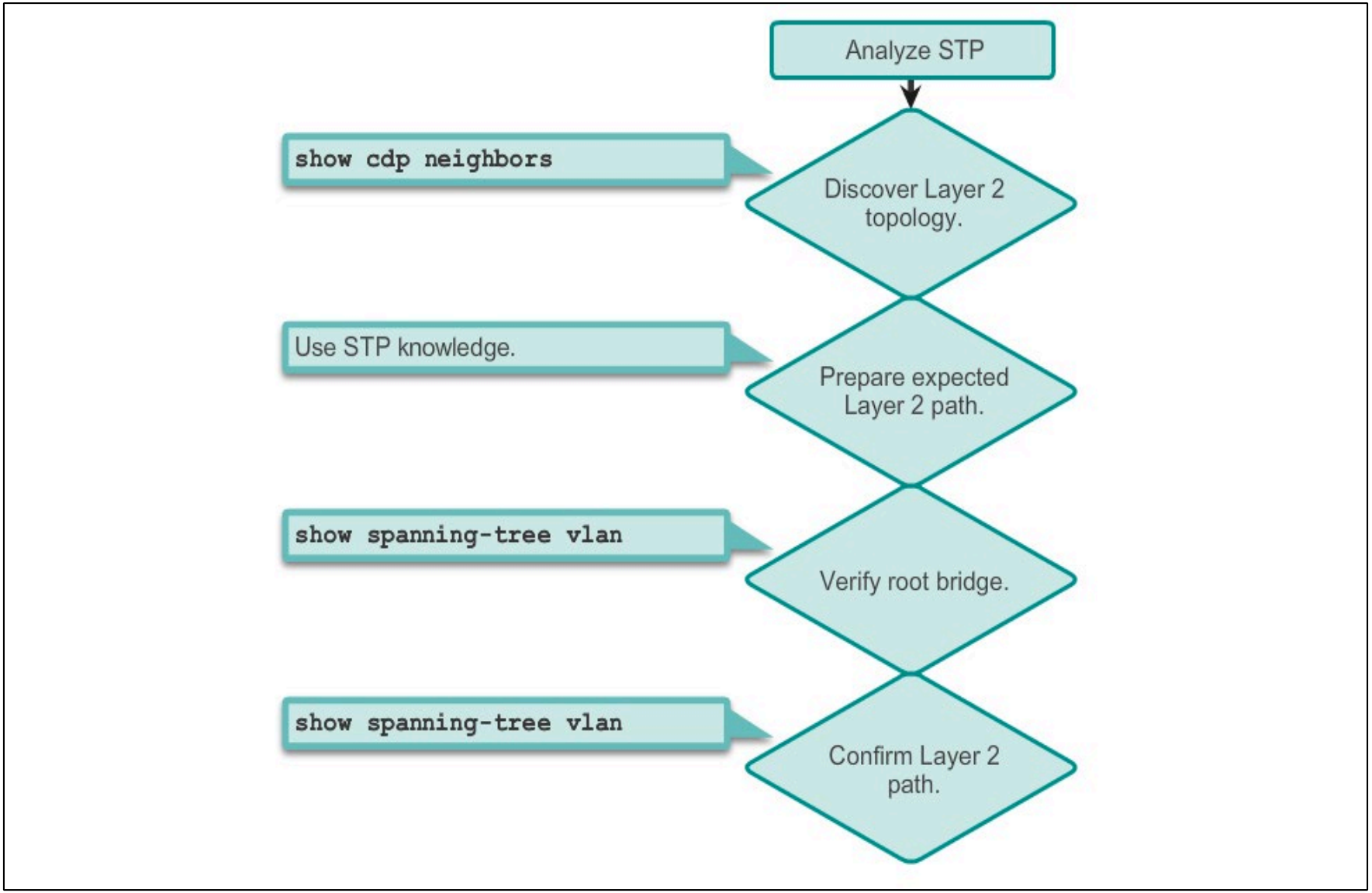
Rapid PVST+ is the Cisco implementation of RSTP. It supports RSTP on a per-VLAN basis.

```
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

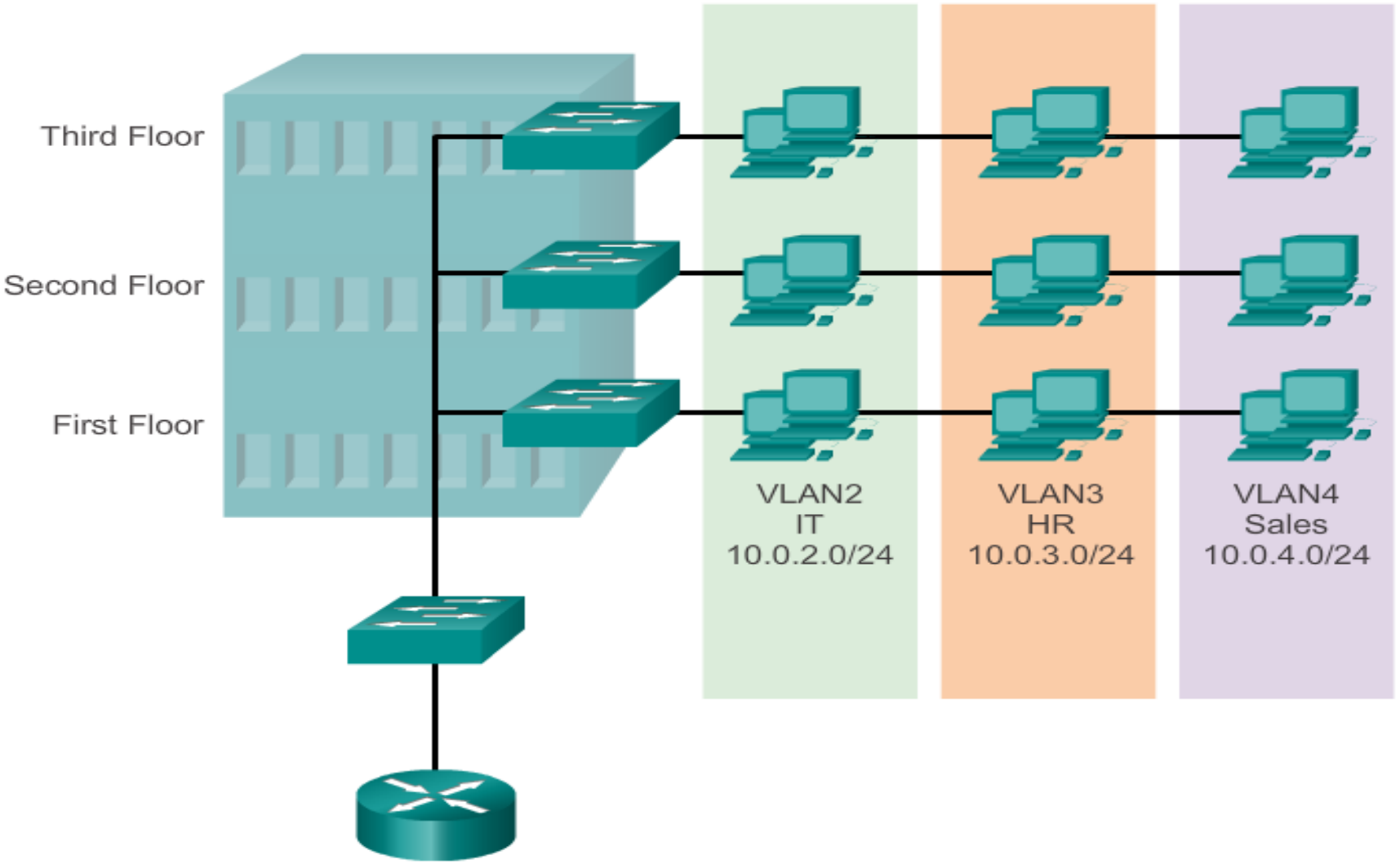
Analyzing the STP Topology



Overview Of VLANs
VLAN Configuration

- VLAN (virtual LAN) is a logical partition of a layer 2 network
- Multiple partition can be created, allowing for multiple VLANs to co-exist
- Each VLAN is a broadcast domain, usually with its own IP network
- VLANS are mutually isolated and packets can only pass between them through a router
- The partitioning of the layer 2 network takes inside a layer 2 device, usually a switch.
- The hosts grouped within a VLAN are unaware of the VLAN's existence

Overview Of VLANs
VLAN Definitions



Overview Of VLANs

Benefits of VLANs

- ✓ Security
- ✓ Cost reduction
- ✓ Better performance
- ✓ Shrink broadcast domains
- ✓ Improved IT staff efficiency
- ✓ Simpler project and application management

Types of VLANs

- Data VLAN
- Default VLAN
- Native VLAN
- Management VLAN

Overview Of VLANs
Types of VLANs

VLAN 1

```
Switch# show vlan brief

VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------
1    default              active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                    Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                    Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                    Gi0/1,  Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
```

- All ports assigned to VLAN 1 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

VLANs in a Multi-Switched Environment

VLAN Trunks

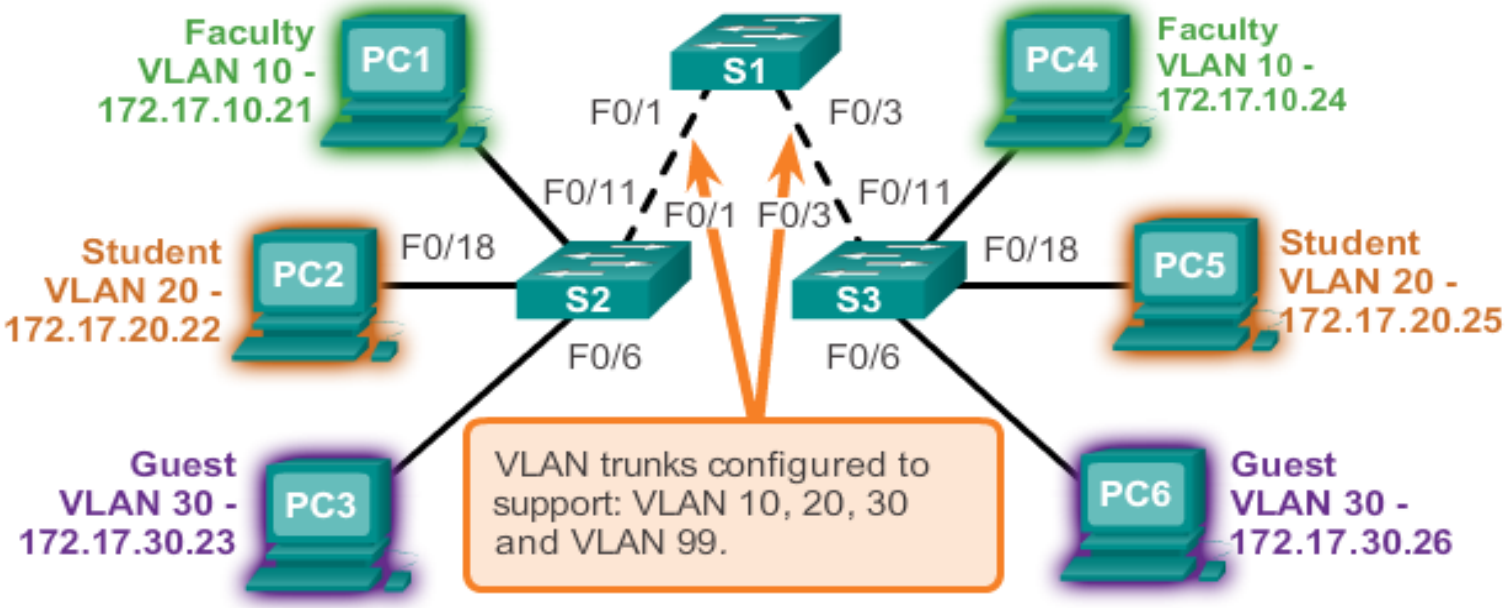
- A VLAN trunk carries more than one VLAN
- Usually established between switches so same-VLAN devices can communicate even if physically connected to different switches
- A VLAN trunk is not associated to any VLANs. Neither is the trunk ports used to establish the trunk link
- Cisco IOS supports IEEE802.1q, a popular VLAN trunk protocol

VLANs in a Multi-Switched Environment

VLAN Trunks

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.



VLANs in a Multi-Switched Environment

Controlling Broadcast Domains with VLANs

- VLANs can be used to limit the reach of broadcast frames
- A VLAN is a broadcast domain of its own
- Therefore, a broadcast frame sent by a device in a specific VLAN is forwarded within that VLAN only.
- This help controlling the reach of broadcast frames and their impact in the network
- Unicast and multicast frames are forwarded within the originating VLAN as well

VLANs in a Multi-Switched Environment…

Tagging Ethernet Frames for VLAN Identification

- Frame tagging is used to properly transmit multiple VLAN frames through a trunk link
- Switches will tag frames to identify the VLAN they belong. Different tagging protocols exist, with IEEE 802.1q being a very popular one
- The protocol defines the structure of the tagging header added to the frame
- Switches will add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports
- Once properly tagged, the frames can transverse any number of switches via trunk links and still be forward within the correct VLAN at the destination

VLAN Assignment

VLAN Ranges On Catalyst Switches

- The Catalyst 2960 and 3560 Series switches support over 4,000 VLANs
- These VLANs are split into 2 categories:
- **Normal Range VLANs**
  - VLAN numbers from 1 through 1005
  - Configurations stored in the vlan.dat (in the flash)
  - VTP can only learn and store normal range VLANs
- **Extended Range VLANs**
  - VLAN numbers from 1006 through 4096
  - Configurations stored in the running-config (in the NVRAM)
  - VTP does not learn extended range VLANs

VLAN Assignment
Creating a VLAN

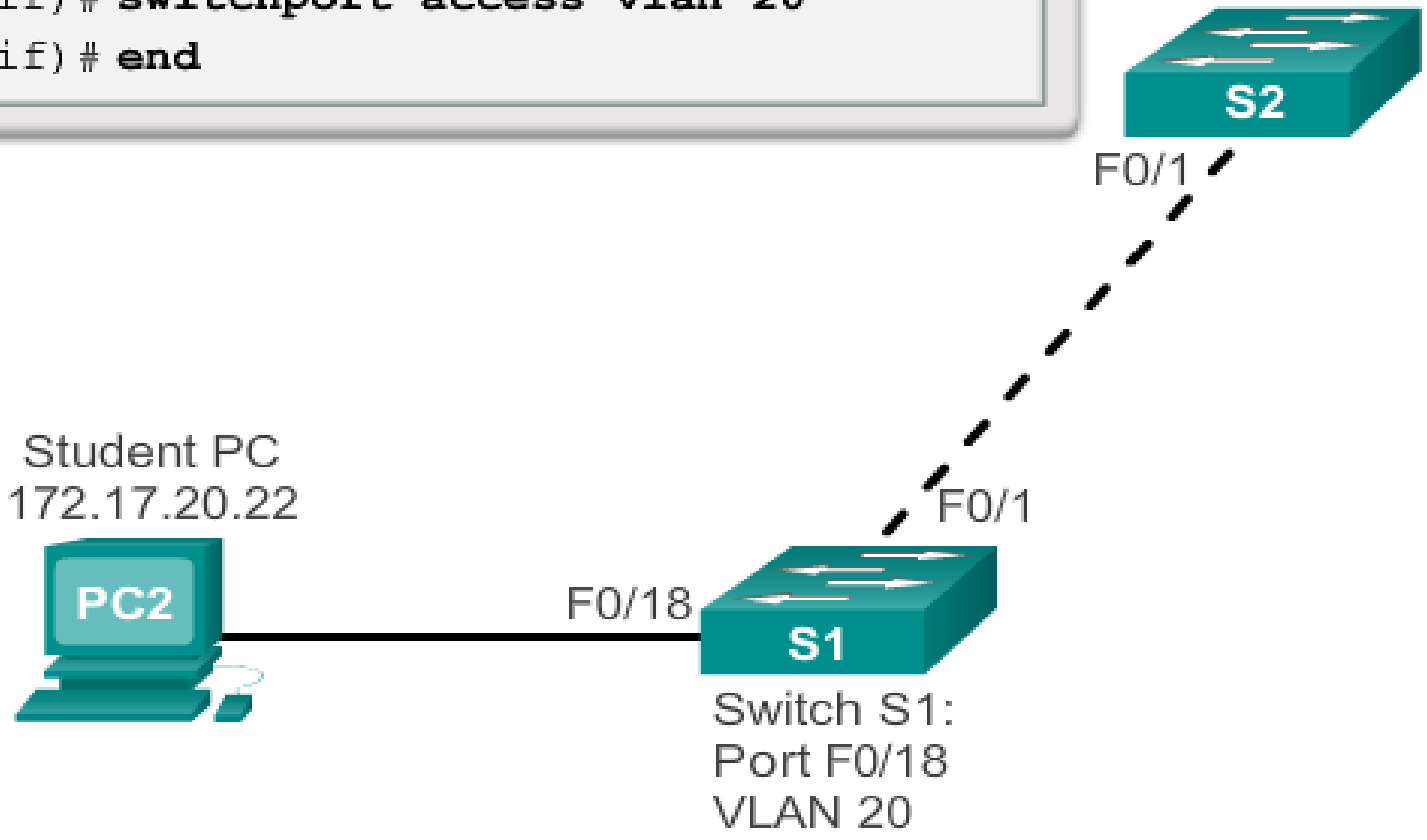
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan_id`
Specify a unique name to identify the VLAN.	`S1(config)# name vlan_name`
Return to the privileged EXEC mode.	`S1(config)# end`

VLAN Assignment
Assigning Ports To VLANs

Cisco Switch IOS Commands	
Enter global configuration mode.	S1 # **configure terminal**
Enter interface configuration mode for the SVI.	S1(config) # **interface** *interface_id*
Configure the management interface IP address.	S1(config) # **ip address 172.17.99.11**
Set the port to access mode.	S1(config-if) # **switchport mode access**
Assign the port to a VLAN.	S1(config-if) # **switchport access vlan** *vlan_id*
Return to the privileged EXEC mode.	S1(config-if) # **end**

VLAN Assignment
Assigning Ports To VLANs

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



VLAN Assignment
Changing VLAN Port Membership

```
S1(config)# int fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

VLAN Name                Status    Ports
---- ----------------- ------- -------------------------------
1    default              active  Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                  Gi0/1, Gi0/2
20   student              active
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

VLAN Assignment
Changing VLAN Port Membership

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name                Status     Ports
---- ------------------- ---------- -------------------------------
1    default             active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/12, Fa0/1
                                    Fa0/14, Fa0/15, Fa0/16, Fa0/
                                    Fa0/18, Fa0/19, Fa0/20, Fa0/
                                    Fa0/22, Fa0/23, Fa0/24, Gi0/
                                    Gi0/2
20   student             active     Fa0/11
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```

VLAN Assignment
Deleting VLANs

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name                 Status    Ports
---- ----------------     --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                    Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                    Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                    Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

VLAN Assignment
Verifying VLAN Information

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

S1# show vlan summary
Number of existing VLANs            : 7
Number of existing VTP VLANs        : 7
Number of existing extended VLANS   : 0

S1#
```

VLAN Assignment
Verifying VLAN Information

```
S1#show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

VLAN Assignment
Configuring IEEE 802.1q Trunk Links

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode for the SVI.	`S1(config )# interface interface_id`
Force the link to be a trunk link.	`S1(config)# switchport mode trunk`
Specify a native VLAN for untagged 802.1Q trunks.	`S1(config-if)# switchport trunk native vlan vlan_id`
Specify the list of VLANs to be allowed on the trunk link.	`S1(config-if)# switchport trunk allowed vlan vlan-list`
Return to the privileged EXEC mode.	`S1(config-if)# end`

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

VLAN Assignment
Resetting the Trunk To Default State

Resetting Trunk Link Example

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

VLAN Assignment
Resetting the Trunk To Default State

Return Port to Access Mode

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

VLAN Assignment

Verifying Trunk Configuration

Verifying Trunk Configuration

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Dynamic Trunking Protocol
Introduction to DTP

- Switch ports can be manually configured to form trunks
- Switch ports can also be configured to negotiate and establish a trunk link with a connected peer
- Dynamic Trunking Protocol (DTP) is a protocol to manage trunk negotiation
- DTP is a Cisco proprietary protocol and is enabled by default in Cisco Catalyst 2960 and 3560 switches
- If the port on the neighbor switch is configured in a trunk mode that supports DTP, it manages the negotiation
- The default DTP configuration for Cisco Catalyst 2960 and 3560 switches is dynamic auto

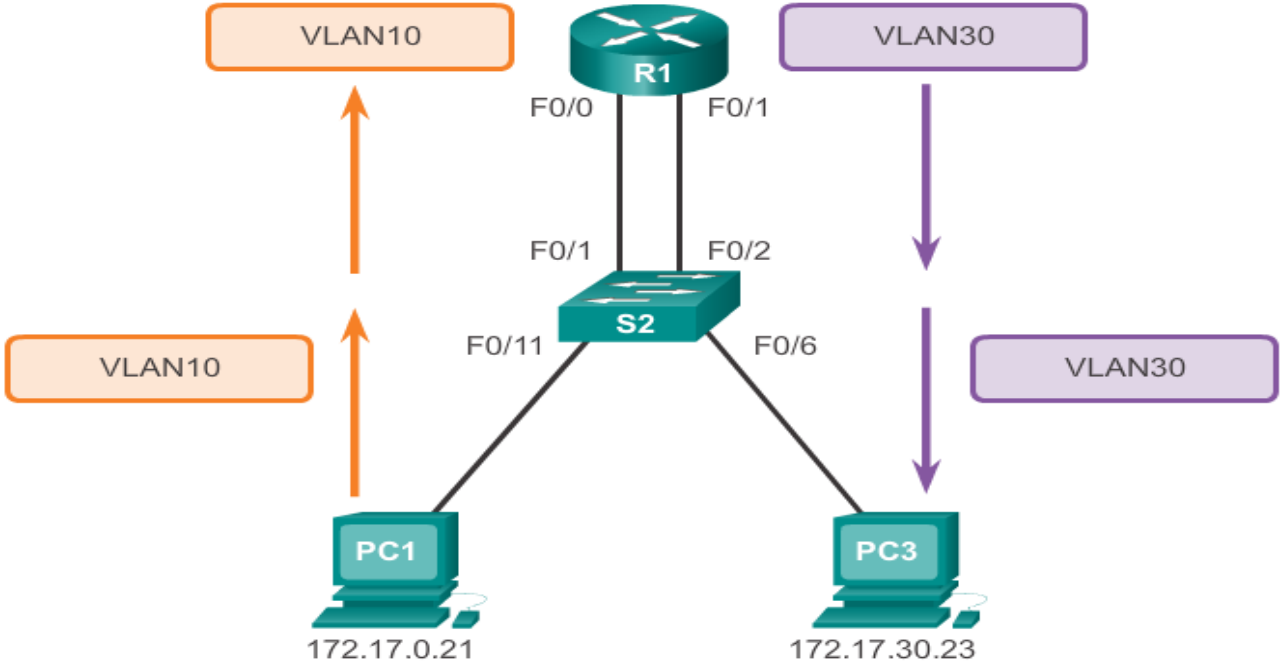
Dynamic Trunking Protocol
Negotiated Interface Modes

- Cisco Catalyst 2960 and 3560 support the following trunk modes:
  - ✓switchport mode dynamic auto
  - ✓switchport mode dynamic desirable
  - ✓switchport mode trunk
  - ✓switchport nonegotiate

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

Inter-VLAN Routing Operation
What is Inter-VLAN Routing?

- Layer 2 switches can't forward traffic between VLANs without the assistance of a router
- Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another using a router



Inter-VLAN Routing Operation
Legacy Inter-VLAN Routing

- In the past, actual routers were used to route between VLAN
- Each VLAN was connected to a different physical router interface
- Packets would arrive on the router through one through interface, be routed and leave through another
- Since the router interfaces were connected to VLANs and had IP addresses from that specific VLAN, routing between VLANs was achieved.
- Simple solution but not scalable. Large networks with large number of VLANs would require lots of router interfaces

Inter-VLAN Routing Operation
Router-On-A-Stick Inter-VLAN Routing

- The so called router-on-a-stick approach uses a different path to route between VLANs
- One of the router's physical interfaces is configured as a 802.1Q trunk port. Now that interface can understand VLAN tags
- Logical subinterfaces are then created. One subinterface per VLAN
- Each subinterface is configured with an IP address from the VLAN it represents
- VLAN members (hosts) are configured to use the subinterface address as a default gateway.
- Only one of the router's physical interface is used

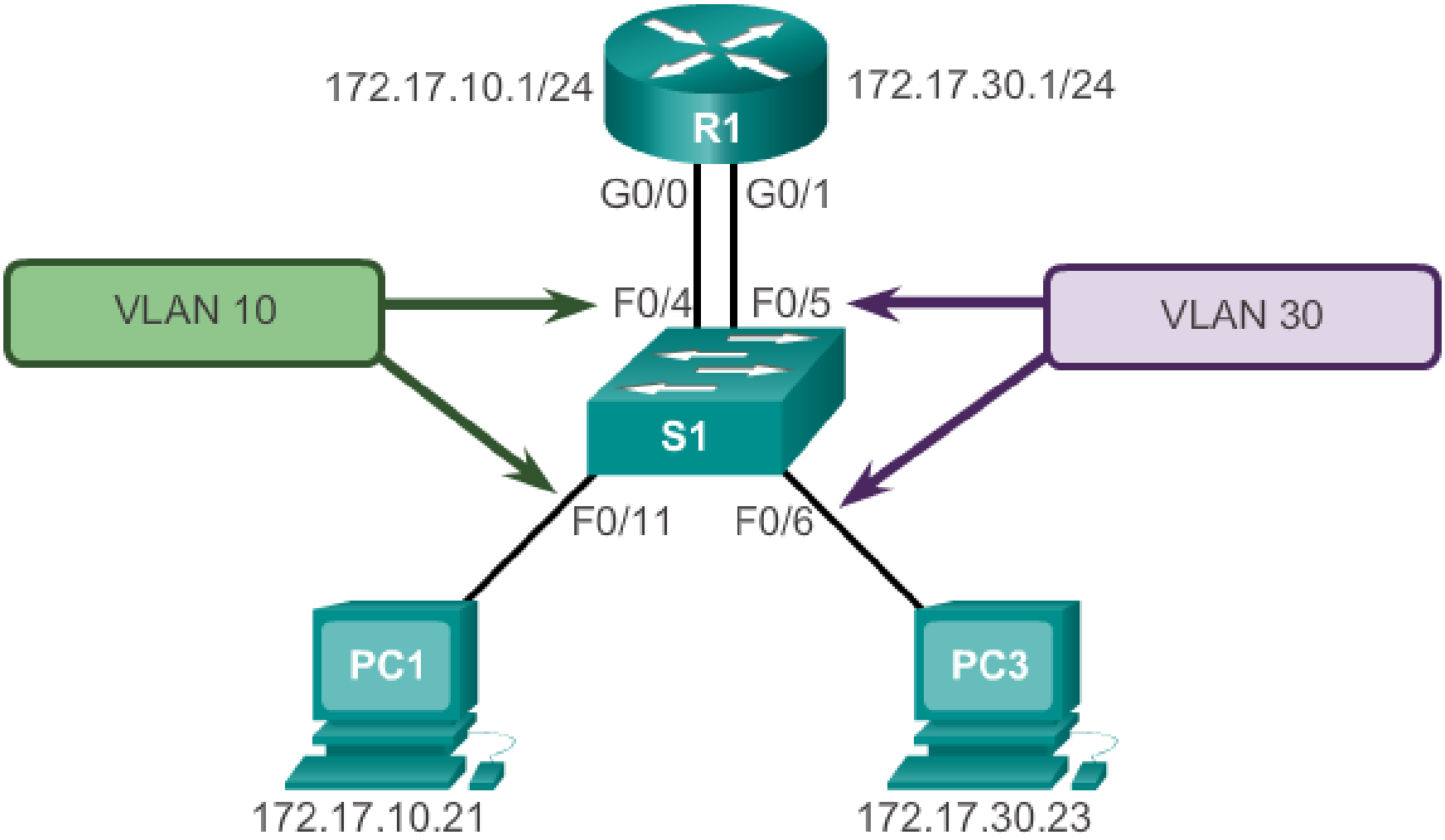
Inter-VLAN Routing Operation
Multilayer Switch Inter-VLAN Routing

- Multilayer switches can perform Layer 2 and Layer 3 functions. Routers are not required anymore
- Each VLAN existent in the switch is a SVI
- SVI are seen as layer 3 interfaces
- The switch understands network layer PDUs and therefore, it can route between its SVIs just as a router routes between its interfaces
- With a multilayer switch, traffic is routed internal to the switch device
- Very scalable solution

Configure Legacy Inter-VLAN Routing Preparation

- Legacy inter-VLAN routing requires routers to have multiple physical interfaces
- Each one of the router's physical interfaces is connected to a unique VLAN
- Each interface is also configured with an IP address for the subnet associated with the particular VLAN
- Network devices use the router as a gateway to access the devices connected to the other VLANs

Configure Legacy Inter-VLAN Routing Preparation



Configure Legacy Inter-VLAN Routing
Switch Configuration

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 30
S1(config-if)# end
*Mar 20 01:22:56.751: %SYS-5-CONFIG_I: Configured from console by
console
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

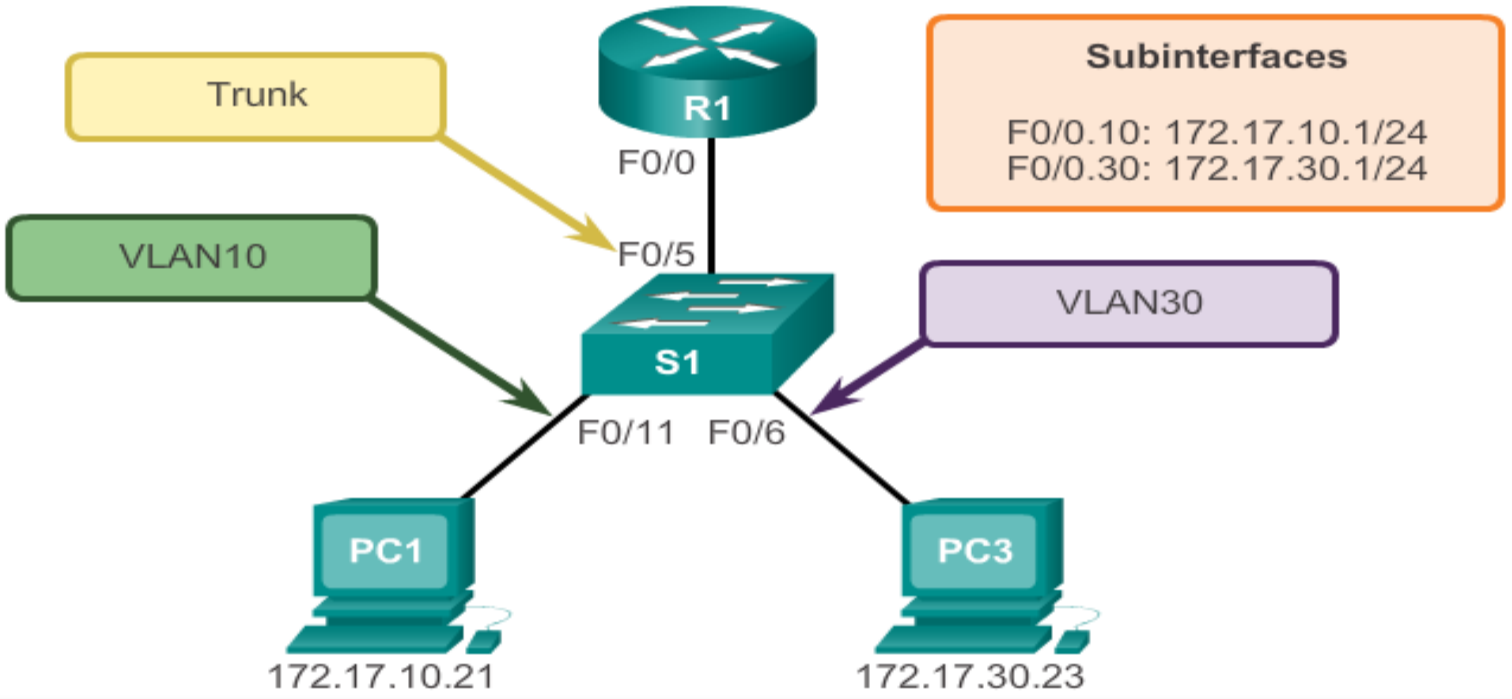
Configure Legacy Inter-VLAN Routing
Router Interface Configuration

```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)# end
R1# copy running-config startup-config
```

Configure Router-On-A-Stick
Preparation

- An alternative to legacy inter-VLAN routing is to use VLAN trunking and subinterfaces
- VLAN trunking allows a single physical router interface to route traffic for multiple VLANs
- The physical interface of the router must be connected to a trunk link on the adjacent switch
- On the router, subinterfaces are created for each unique VLAN on the networ
- Each subinterface is assigned an IP address specific to its subnet/VLAN and is also configured to tag frames for that VLAN

Configure Router-On-A-Stick
Switch Configuration




```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

Configure Router-On-A-Stick
Router Interface Configuration

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0, changed state to up
```

Configure Router-On-A-Stick
Verifying Subinterfaces

```
R1# show vlans
 <output omitted>
Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:    GigabitEthernet0/0.10

  Protocols Configured:  Address:      Received:   Transmitted:
          IP             172.17.10.1          11              18
<output omitted>
Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:    GigabitEthernet0/0.30

  Protocols Configured:  Address:      Received:   Transmitted:
          IP             172.17.30.1          11               8
<output omitted>
```

Configure Router-On-A-Stick
Verifying Routing

- Access to devices on remote VLANs can be tested using the **ping** command.
- The **ping** command sends an ICMP echo request to the destination address
- When a host receives an ICMP echo request, it responds with an ICMP echo reply
- Tracert is a useful utility for confirming the routed path taken between two devices

Inter-VLAN Configuration Issues
Switch Port Issues

- When using the legacy routing model, ensure that the switch ports that connect to the router interfaces are configured with the correct VLANs
- Use the **switchport access vlan 10** command to correct any errouneous VLAN port assignment
- Also ensure the router is connected to the correct switch port
- When using router-on-a-stick, ensure the switch port connected to the router is configured as a trunk link
- The **switchport mode trunk** command can be used to solve this problem

Inter-VLAN Configuration Issues
Verify Switch Configuration

```
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#
```

Inter-VLAN Configuration Issues
Verify Router Configuration

- With router-on-a-stick configurations, a common problem is assigning the wrong VLAN ID to the subinterface
- The **show interface** command can help detecting this problem
- If this is the case, use the **encapsulation dot1q <vlan id>** interface command to fix the problem

Inter-VLAN Configuration Issues
Verify Router Configuration

```
R1# show interface

<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

<output omitted>

R1#
R1# show run
Building configuration...
Current configuration : 505 bytes

<output omitted>

!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 100
 ip address 172.17.10.1 255.255.255.0
!
interface GigabitEthernet0/0.30
```

IP Addressing Issues
Verifying IP Address And Subnet Mask Configuration Issues

- To verify if the correct IP address is configured in the router, use the **show ip interface** command
- The **show running-config** can also be useful when troubleshooting router related problems
- Although configuring subinterface IDs to match the VLAN number makes it easier to manage inter-VLAN configuration, it is not a requirement. When troubleshooting addressing issues, ensure that the subinterface is configured with the correct address for that VLAN.

Layer 3 Switching Operation And Configuration
Introduction To Layer 3 Switching

- Layer 3 switches usually have packet-switching throughputs in the millions of packets per second (pps)
- All Catalyst switches support two types of Layer 3 interfaces:
  - **Routed Port**
  - **SVI**
- High-performance switches, such as the Catalyst 6500 and Catalyst 4500, are able to perform most of the router's functions
- But several models of Catalyst switches require enhanced software for specific routing protocol feature

Layer 3 Switching Operation And Configuration
Inter-VLAN Routing with SVIs

- Today routing has become faster and cheaper and can performed at hardware speed
- It can be transferred to core and distribution devices with little to no impact on network performance
- Many users are in separate VLANs, and each VLAN is usually a separate subnet
- This implies that each distribution switch must have IP addresses matching each access switch VLAN
- Layer 3 (routed) ports are normally implemented between the distribution and the core layer
- This model is less dependent on spanning-tree as there are no loops in the Layer 2 portion of the topology

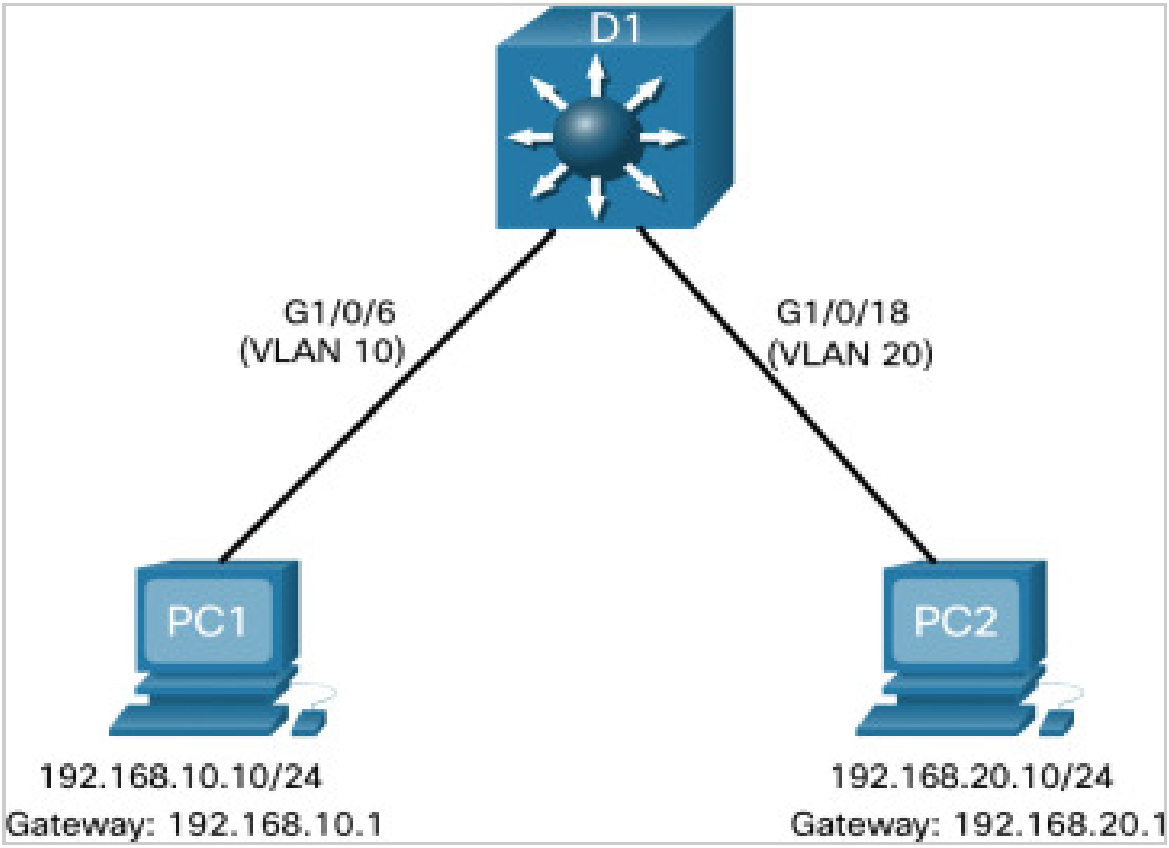
Layer 3 Switching Operation And Configuration
Inter-VLAN Routing with SVIs (cont)

- By default, an SVI is created for the default VLAN (VLAN1). This allows for remote switch administration
- Any additional SVIs must be created by the admin
- SVIs are created the first time the VLAN interface configuration mode is entered for a particular VLAN SVI
- The **interface vlan 10** entered by the first time creates an SVI named VLAN 10
- The VLAN number used corresponds to the VLAN tag associated with data frames on an 802.1Q encapsulated trunk
- Whenever the SVI is created, ensure that particular VLAN is present in the VLAN database

Layer 3 Switching Operation And Configuration
Inter-VLAN Routing with SVIs (cont)

- SVIs advantages include:
  - It is much faster than router-on-a-stick, because everything is hardware switched and routed.
  - No need for external links from the switch to the router for routing.
  - Not limited to one link. Layer 2 EtherChannels can be used between the switches to get more bandwidth.
  - Latency is much lower, because it does not need to leave the switch.

Inter-VLAN Routing with SVIs (cont)



Inter-VLAN Routing with SVIs (cont)

Step 1: Create the VLANs

- D1(config)#vlan 10
- D1(config-vlan)#name studdent
- D1(config-vlan)#vlan 20
- D1(config-vlan)#name Faculty

Step 2: Create the SVI VLAN interfaces

- D1(config)#interface vlan 10
- D1(config-if)#IP address 192.168.10.1 255.255.255.0
- D1(config-if)#no shutdown
- D1(config-if)#interface vlan 20
- D1(config-if)#interface IP address 192.168.11.1 255.255.255.0
- D1(config-if)#no shutdown

Inter-VLAN Routing with SVIs (cont)

Step 3: Configure access ports

- D1(config)#interface g1/0/6
- D1(config-if)# switchport mode access
- D1(config-if)# switchport access vlan 10
- D1(config) interface g1/0/18
- D1(config-if)# switchport mode access
- D1(config-if)# switchport access vlan 20

Step 4: Enable IP routing

D1(config)# IP routing