instituto superior de engenharia de lisboa

Redes de Internet / Internet Networks
Practical Lesson No. 3: RSTP and PVST

Context

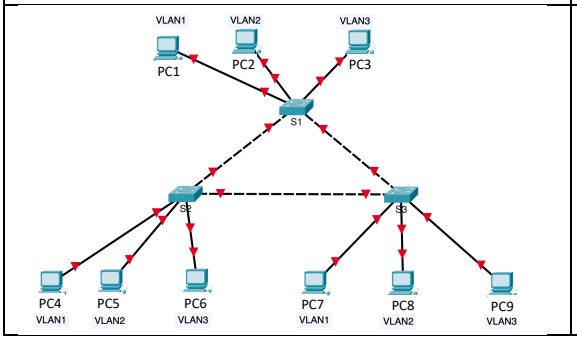
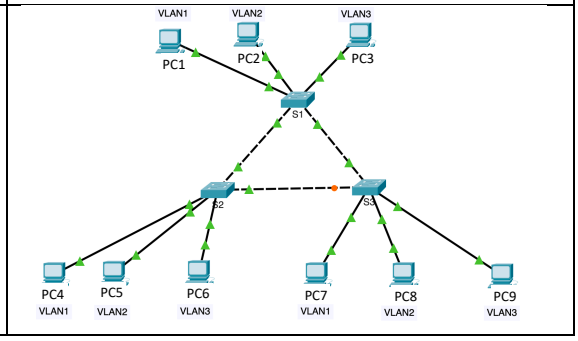
This activity aims to configure: VLANs and trunk connections, Rapid Spanning Tree PVST+, optimize bridge priorities by VLAN. Finally, it also aims to optimize the network by configuring PortFast and BPDU Guard on peripheral ports.

Objectives

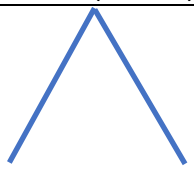
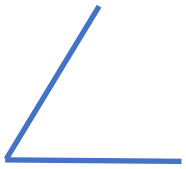
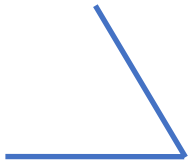
- Part I: Configure VLANs + PVST + Load balancing
- Part II: Configure PortFast and BPDU Guard
- Part III: Configure Rapid Spanning Tree PVST mode
- Part IV: Configure MST mode

Part I – Configuring PVST + Load Balancing

Using Packet Tracer, implement the following network topology containing three VLANs that share common links. You can find the base topology at the link. Verify that the MAC addresses of the switches respect the order MAC1 (0001.96E7.69DB) < MAC2 (000D.BD77.2A40) < MAC3(00D0.58D6.233D), so by default switch 1 is elected as the root bridge, while the highest interface on switch 3 is blocked.

Before Convergence	After Convergence
	

If only VLAN 1 (default) existed, this topology would be inefficient because it would overload the links between S1 and S2 and between S1 and S3, leaving the link between S2 and S3 only for use in case of failure of the previous ones. Therefore, to optimize load distribution between segments, the intention is to implement three VLANs, each with its own active STP topology, following the illustrative diagram below to ensure traffic distribution between links:

VLAN 1 (default)	VLAN 2	VLAN 3
		

1 - Configuring VLANs and Trunk Ports

An Access port (CISCO nomenclature) or “untagged port” (general nomenclature) is a switch port that carries traffic to only one VLAN. A Trunk port (CISCO nomenclature) or “tagged port” (general nomenclature) is a switch port that can carry traffic to more than one VLAN.
When an Ethernet frame passes through a port in TRUNK mode, a VLAN tag is added to distinguish which frames belong to each of the configured VLANs. In contrast, ACCESS mode ports do not require a VLAN tag to be defined, as all incoming or outgoing Ethernet frames belong to the same VLAN. The native VLAN is also defined, which is a special VLAN that can pass through the TRUNK port without a VLAN tag being defined.

Step 1: Set the ports to TRUNK mode

In this step, we will configure the switch ports that should remain in TRUNK mode. The additional command “nonegotiate” forces the trunk mode connection to be permanent, preventing it from being dynamically negotiated.

Switch 1 Configuration:

```
S1(config)# interface range g0/1-2
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# end
```

```
S1# show interfaces trunk
```

```
S1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1
Gig0/2      1

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      none
Gig0/2      none
```

Switch 2 Configuration:

```
S2(config)# interface range g0/1-2
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport nonegotiate
S2(config-if-range)# end
```

```
S2# show interfaces trunk
S2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1
Gig0/2      1

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      none
Gig0/2      none
```

Switch 3 Configuration:

```
S3(config)# interface range g0/1-2
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport nonegotiate
S3(config-if-range)# end
```

```
S3# show interfaces trunk
S3#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1
Gig0/2      1

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      none
Gig0/2      none
```

Step 2: Configuring user ports in access mode

The switches connected to the PCs are configured in ACCESS mode. The three ports are then activated using the shutdown command.

Switch 1 Configuration:

```
S1(config)# interface range f0/1-3
S1(config-if-range)# switchport mode access
S1(config-if-range)# no shutdown
```

Switch 2 Configuration:

```
S2(config)# interface range f0/1-3
S2(config-if-range)# switchport mode access
S2(config-if-range)# no shutdown
```

Switch 3 Configuration:

```
S3(config)# interface range f0/1-3
S3(config-if-range)# switchport mode access
S3(config-if-range)# no shutdown
```

Step 3: Defining VLANs

Now use the following commands to create the three desired VLANs on all switches: VLAN 1 (default), VLAN 2, and VLAN 3.

Switch 1 Configuration:

```
S1(config)# vlan 1
S1(config-vlan)# vlan 2
S1(config-vlan)# vlan 3
S1(config-vlan)# end
```

```
S1# show vlan brief
```

```
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, Fa0/11, 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
2    VLAN0002                          active
3    VLAN0003                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Switch 2 Configuration:

```
S2(config)# vlan 1
S2(config-vlan)# vlan 2
S2(config-vlan)# vlan 3
S2(config-vlan)# end
```

```
S2# show vlan brief
```

```
S2#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, Fa0/11, 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
2    VLAN0002                          active
3    VLAN0003                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Switch 3 Configuration:

```
S3(config)# vlan 1
S3(config-vlan)# vlan 2
S3(config-vlan)# vlan 3
S3(config-vlan)# end
```

```
S3# show vlan brief
```

```
S3#sh vlan br

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
2    VLAN0002                          active
3    VLAN0003                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Step 3: Associating VLANs with switch ports

The ports must be associated with the VLANs according to the initial figure with the topology description. The example below illustrates the configuration for switch 1.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 1
S1(config-if)# interface f0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 2
S1(config-if)# interface f0/3
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 3
```

Step 4: Check the VLAN settings

Use the show vlan brief command on all switches to verify that all VLANs are correctly defined.

S1# **show vlan brief**

```
S1#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, 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
2    VLAN0002                         active    Fa0/2
3    VLAN0003                         active    Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

S2# **show vlan brief**

```
S2#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, 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
2    VLAN0002                         active    Fa0/2
3    VLAN0003                         active    Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

S3# **show vlan brief**

```
S3#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, 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
2    VLAN0002                         active    Fa0/2
3    VLAN0003                         active    Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Step 5: Optimize bridge priorities

To prevent the same physical link from being blocked for all three VLANs, the bridge priorities should be optimized so that the Root Bridge (RB) for each of VLANs 1, 2, and 3 is Switch 1, Switch 2, and Switch 3, respectively. First, you should check the current priority status of each bridge in each VLAN using the “show spanning-tree vlan x priority y” command:

S1(config)# **show spanning-tree vlan 1**

```
S1#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.96E7.69DB
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.96E7.69DB
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

As you can see, S1 is the root bridge for VLAN 1, which means that all of its interfaces are designated ports. The cost is used by STP to determine the best path to the root bridge. Paths with lower costs are preferred. Interfaces with higher bandwidth have lower costs, which is reflected in the cost value. Fa0/1 has a cost of 19, associated with a Fast Ethernet interface (100 Mbps). Gi0/1 and Gi0/2 have a cost of 4, associated with Gigabit Ethernet interfaces (1 Gbps).

Timer Summary:

• Hello Time: 2 seconds to send BPDUs and check connectivity.
• Max Age: 20 seconds wait before discarding outdated BPDUs.
• Forward Delay: 15 seconds in Listening and Learning states to ensure that the topology is stable before forwarding packets. When a port changes state (for example, after a topology change), it first spends 15 seconds in the Listening state and then 15 seconds in the Learning state to ensure network stability before it begins forwarding packets.

S2(config)# **show spanning-tree vlan 2**

```
S2#show spanning-tree vlan 2
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID     Priority    32770
              Address     0001.96E7.69DB
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32770  (priority 32768 sys-id-ext 2)
              Address     000D.BD77.2A40
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

S3(config)# **show spanning-tree vlan 3**

```
S3# sh spanning-tree vlan 3
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    32771
              Address     0001.96E7.69DB
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32771  (priority 32768 sys-id-ext 3)
              Address     00D0.58D6.233D
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Altn BLK 4         128.26   P2p
```

Next, we want to change the priority of each bridge from the default value to the new value 24576. This can be done in two ways, as shown here for the configuration of “Switch 1”:

```
S1(config)# spanning-tree vlan 1 root primary
ou
S1(config)# spanning-tree vlan 1 priority 24576
```

After properly configuring each of the bridges, verify that all LEDs are “green” in the new active topology. Confirm the port configuration with the “show spanning-tree vlan x” command on each of the bridges. The existence of an active topology per VLAN has the benefit of allowing “Load Sharing” between the various physical links, although it has the downside of higher CPU and memory usage.

```
S1(config)# show spanning-tree vlan 1
```

```
S1#sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0001.96E7.69DB
              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     0001.96E7.69DB
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

```
S2(config)# show spanning-tree vlan 2
```

```
S2#sh spanning-tree vlan 2
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID     Priority    24578
              Address     000D.BD77.2A40
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24578  (priority 24576 sys-id-ext 2)
              Address     000D.BD77.2A40
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

S3(config)# **show spanning-tree vlan 3**

```
S3# sh spanning-tree vlan 3
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    24579
              Address     00D0.58D6.233D
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24579  (priority 24576 sys-id-ext 3)
              Address     00D0.58D6.233D
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

Additional Notes on Spanning Tree Priority and Root Bridge Optimization

Electing the root bridge based on the MAC address should be avoided, as this can result in suboptimal network performance, since the oldest switch with the lowest MAC address will be chosen.

To avoid this situation, it may be convenient to manually choose a root bridge on the network. To do this, you must manually configure a root bridge value or manually designate it as the root bridge with the root primary command. This will set the bridge priority to 24576, which is lower than the default priority.

If the root bridge fails, another core switch must be designated as the secondary root bridge. To do this, use the root secondary command. This will set the bridge priority to 28672, which is lower than the default priority but higher than the primary root. If the primary switch fails, the switches will elect a new root bridge, which will be the secondary switch, assuming the role of the new root bridge.

Step 6: Intra VLAN Routing

For this step, we suggest considering the following IP addressing scheme:

VLAN	Endereço IP /Gateaway	Máscara
1	192.168.1.0 / 192.168.1.254	255.255.255.0
2	192.168.2.0 / 192.168.2.254	255.255.255.0
3	192.168.3.0 / 192.168.254	255.255.255.0
PC1	192.168.1.1	255.255.255.0
PC2	192.168.2.1	255.255.255.0
PC3	192.168.3.1	255.255.255.0
PC4	192.168.1.2	255.255.255.0
PC5	192.168.2.2	255.255.255.0
PC6	192.168.3.2	255.255.255.0
PC7	192.168.1.3	255.255.255.0
PC8	192.168.2.3	255.255.255.0
PC9	192.168.3.3	255.255.255.0

Configuring the default gateway on the root bridge of each VLAN:

S1(config)# **interface vlan 1**
S1(config-if)# **ip address 192.168.1.254 255.255.255.0**
S1(config-if)# **no shutdown**

S1(config)# **interface vlan 2**
S1(config-if)# **ip address 192.168.2.254 255.255.255.0**
S1(config-if)# **no shutdown**

S1(config)# **interface vlan 3**
S1(config-if)# **ip address 192.168.3.254 255.255.255.0**
S1(config-if)# **no shutdown**

S1(config-if)# **exit**

Configure the IP addresses and their respective default gateways on each PC using the IP Config module in Packet Tracer. Check for connectivity within each VLAN between the various PCs using the “ping” application via the command prompt.

Example VLAN1:

PC1->PC4;

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC1->PC7

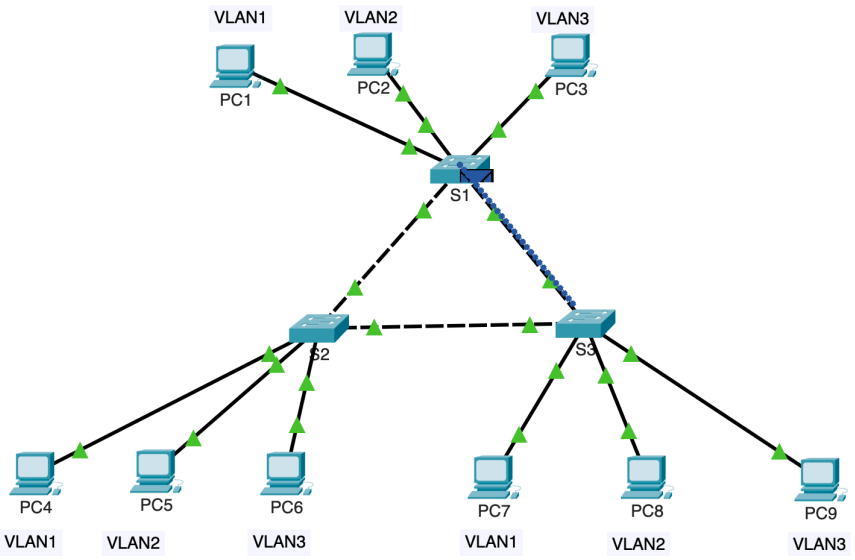
```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Repeat the exercise with the packet tracer simulation module, selecting only ICMP packets. Test sending ICMP packets between PCs belonging to the same VLANs. For example, send an ICMP packet from PC7 to PC4 and observe the direction of packet propagation, where you should see that, for example, for VLAN 1, the lower link is blocked. Verify that the desired behavior occurs in all configured VLANs.



Note: verify that there is no inter-VLAN routing in this configuration.

Part II: Configure PortFast and BPDU Guard

This section aims to illustrate two features that increase the convergence speed of the active topology and enhance network security.

> Additional notes on Port Fast and BPDU Guard
>
> PortFast causes a port to enter the forwarding state almost immediately, drastically reducing the time spent in the Listening and Learning states. This minimizes the time required for the server or workstation to come online. Configure PortFast on the S2 interfaces connected to PCs.
>
> BPDU Guard protects the Spanning Tree Protocol (STP) topology from threats related to the sending of BPDUs. It should be enabled on ports that should not receive BPDUs from connected devices (e.g., printers). When PortFast is configured on access ports, it accelerates the transition to the STP Forwarding state. End devices (workstations, servers, printers, etc.) should not generate BPDUs, which are normally exchanged between switches.
>
> To prevent loops, BPDU Guard blocks interfaces preventively. It prevents external influences from affecting the Spanning Tree domain. BPDU Guard is disabled by default, but is highly recommended on all ports with the PortFast function enabled. When a BPDU is received, the port is disabled and its status is set to Errdisable (equivalent to the “shutdown” state). BPDU Guard can be enabled globally or per interface, requiring the port to be manually reactivated after it has been disabled.

Step 1: PortFast configuration

The following example illustrates the activation of PortFast on the three access ports configured with the respective PCs.
S1(config)# **interface range f0/1-3**
S1(config-if-range)# **spanning-tree portfast**

Step 2: Configuring BPDU Guard

As a protective measure to prevent BPDU exchange with elements behind a port configured with PortFast, the BPDU Guard feature is enabled, as illustrated for “Switch 1”:

```
S1(config)# interface range f0/1-3
S1(config-if-range)# spanning-tree bpduguard enable
```

Step 3: Verify the configuration

Use the show run command to view and validate the entire configuration.
Example:

```
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
!
interface FastEthernet0/1
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 3
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Part III: Configuring Rapid Spanning Tree Mode PVST

The Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) can be seen as an evolution of the standard 802.1D. The 802.1D terminology remains basically the same and most parameters are unchanged. In most cases, RSTP performs better than Cisco's proprietary extensions without any additional configuration. 802.1w can also revert to 802.1D to ensure port-level interoperability with legacy bridges. On Cisco equipment, only a proprietary version of RSTP is available, called Rapid PVST (Rapid Per-VLAN Spanning Tree).

Port States

There are only three port states left in RSTP that correspond to the three possible operational states. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.

STP (802.1D) Port State	RSTP (802.1w) Port State	Is Port Included in Active Topology?	Is Port Learning MAC Addresses?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Forwarding	Yes	Yes

Additional Notes on RSTP Operation

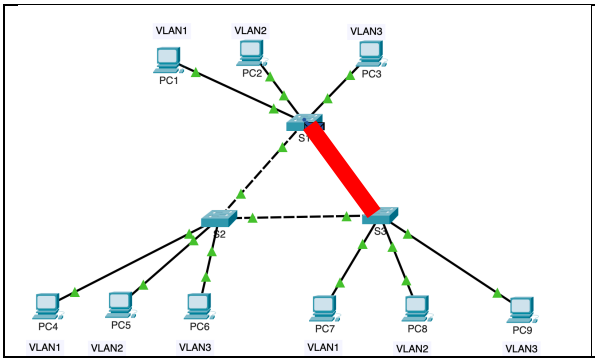
RSTP Operation is similar to STP. Like STP, in RSTP, Root Bridge is selected firstly. Then port roles are determined.

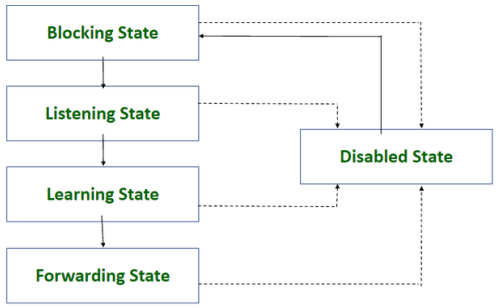
In RSTP there are two additional port roles:

- Alternate Port if it is connected to a port on different Switch
- Backup Port if it is connected to a port on the same Switch

Step 1: Check convergence times with PVST

Remove the marked link and verify that the time until PVST converges to the new active topology follows the process of BLK -> LSN (15s) -> LRN (15s) -> FWD, which takes about 30 seconds. Suggestion: test a ping -t between PC7 and PC1





Use the show spanning-tree command to observe the status of the ports, for example on switch 1, when the marked link is removed and replaced.

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Desg LSN 4         128.26   P2p
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------
Fa0/3            Desg FWD 19        128.3    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Root LRN 4         128.26   P2p
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------
Fa0/3            Desg FWD 19        128.3    P2p
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Root FWD 4         128.26   P2p
```

Step 2: Configure R-PVST+ mode

Use the spanning-tree mode command to configure the switches to set rapid PVST+ as the STP mode.

S1(config)# **spanning-tree mode rapid-pvst**

S2(config)# **spanning-tree mode rapid-pvst**

S3(config)# **spanning-tree mode rapid-pvst**

Step 3: Compare convergence times with RPVST

Using the original base topology, configure RPVST mode and test again the impact of removing the marked link, comparing the time until convergence to the new active topology. Verify that the transition from BLK to FWD is almost immediate, since RPVST does not consider the listening and learning states.

Part IV: Configuring MST Mode

The Multiple Spanning Tree Protocol (MST; IEEE 802.1S) combines the advantages offered by PVST, particularly in terms of load balancing, but with much greater efficiency in terms of bandwidth, memory, and CPU resource consumption, as there is not one active topology for each individual VLAN, but rather one for each group of VLANs, taking into account a control parameter.

- **STP** → IEEE 802.1D → CST: Common STP (Packet Tracer nok)
- **PVST+** →Per VLAN STP Plus → Cisco Proprietary (Packet Tracer ok)
- **RSTP** → IEEE 802.1W (Packet Tracer nok)
- **Rapid-PVST** → Cisco Proprietary (Packet Tracer ok)
- **MST** → IEEE 802.1S [RSTP] (Packet Tracer nok)

MST is not supported in Packet Tracer, but conceptually it is identical to PVST, assigning each group of VLANs a common family. MST mode configuration is done by regions that share a common configuration and are interpreted in a complex topology as a single switch. The parameterization of an "MST Region" comprises three fundamental parameters:
• NAME (name that identifies a set of parameters)
• REVISION (number that identifies a set of parameters)
• INSTANCE mapping (mapping of VLANs by switch -> e.g.: instance1 VLAN 1-30)

Configuration instructions

- switch(config)# **spanning-tree mode mst**
- switch(config)# **spanning-tree mst configuration**
- switch(config-mst)# **name NAME**
- switch(config-mst)# **revision NUMBER**
- switch(config-mst)# **instance NUMBER vlan VLAN-LIST**