1-4(C). Spanning Tree Config

In the 2016 Wendell Odom Cert. Guide, this material is found in the first part of Chapter 3.

MODE

Cisco switches usually run PVSTP (normal 802.1D plus per-VLAN topologies and portfast) by default. It is sometimes called PVST+. In the configuration command, it's called "pvst."

```
S2(config)# spanning-tree mode pvst
```

This is the default, but still shows in the running-config. Some "show" commands call it "IEEE."

CHANGING ROOT SWITCH CHOICE

Without any further configuration, all switches will have the same priority, leaving the root bridge to be elected based on the lowest (earliest) MAC address. So, unless you want your root switch to be a relic from the 1900s in some forgotten wiring closet, change the BID by changing the priority (per-VLAN only).

```
SW(config)# spanning-tree vlan 11 priority 32768
```

Can directly set to a multiple of 4096 (32768 default) or use command below

```
SW(config)# spanning-tree vlan 11 root [primary | secondary]
```

Secondary sets priority to 28,672 (one notch down from default)
Primary sets priority to 24,576 or one notch down from that of the current root switch (if not self), whichever is lower.

CHANGING ROOT PORT CHOICE

Change the port cost of a trunking interface. This changes the root cost over that path.

```
SW(config-if)# spanning-tree  [ vlan 11 ] cost 10
```

Can use a combination of commands with and without vlan to have specific and "everyone else"

Default Port Costs—Cisco sets cost based on a port's actual speed, not its capability.

SPEED	10 Mbps	100 Mbps	1 Gbps	10 Gbps
COST	100	19	4	2

Port Priority (Range 0…255, default 128, lower better)—To break ties (same root cost) between parallel links between the same two switches, assuming you didn't want to have different port costs, which would cascade root cost changes downstream if your chosen link went down, you can change the port priority (on the upstream side).

```
SW(config-if)# spanning-tree vlan 10 port-priority 112
```

Note: Port cost is set on the downstream side (added to port cost in received hello), Port priority is set on the upstream side.

ADJUSTMENT	WHERE SET	SCOPE
Port Cost	Downstream end of Link	Affects cumulative path cost downstream
Port Priority	Upstream (Nearer Root Switch)	Local

SHOW SPANNING-TREE

```
1  S2# show spanning-tree vlan 1
2  VLAN0001
3    Spanning tree enabled protocol ieee
4    Root ID     Priority    32769
5                Address     000c.85ca.e280
6                Cost        19                      Cumulative root cost over path
7                Port        7 (FastEthernet0/7)     This is our port number
8                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
9
10   Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
11               Address     000d.29f3.f380
12               Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
13               Aging Time 300
14
15 Interface           Role Sts Cost      Prio.Nbr Type
16 ------------------- ---- --- --------- -------- --------------------------------
17 Fa0/7               Root FWD 19        128.7    P2p
18 Fa0/8               Altn BLK 19        128.8    P2p
19 Fa0/9               Altn BLK 19        128.9    P2p
20 Fa0/10              Altn BLK 19        128.10   P2p
21 Fa0/11              Desg FWD 19        128.11   P2p
22 Fa0/12              Desg FWD 19        128.12   P2p
```

This command puts everything in one place, but it's a confusing combination of information about the root switch and your own.

The Root Switch—The timers (hello, max age, etc.) are configured (or default) on all switches, but the ones actually used by all switches are propagated from the root switch once it's chosen.

- The root switch's ID (priority and MAC) [lines 4 and 5].

  Because we're running Cisco's per-VLAN version of STP, the priority of 32769 is actually a combination of the configured (or in this case default) priority of 32768 and the VLAN ID.

- The cumulative cost to the root [line 6]. On a root switch, this says "This bridge is the root."
- Which of our local ports leads to the root switch [lines 7] (unless we *are* the root switch.) We could also look for the which of our ports is labeled as the root port [line 17, column 2].

Our Own Switch Configuration [lines 3, 10-22]

- Our own switch's bridge ID (priority and MAC) [lines 10 and 11]

  Here, the command breaks out our bridge priority and VLAN ID (called says-id-ext). The priority can be adjusted (per-clan only) with the command

  ```
  SW(config)# spanning-tree vlan 1 priority 32768
  ```

Our Own Interface Configurations

- Port Costs [lines 17-22, column 4]. These can be adjusted per-VLAN or for all VLANs

  ```
  SW(config-if)# spanning-tree  [ vlan 1 ] cost 10
  ```

- Port Priorities [lines 17-22, column 5]. These can be adjusted per-VLAN or for all VLANs

  ```
  SW(config-if)# spanning-tree [ vlan 1 ] port-priority 112
  ```

Spanning Tree Effects on Our Interfaces—The resulting tree

- Roles and States [lines 17-22, Columns 2-3]

SHOW SPANNING-TREE [VLAN 1] ROOT

```
                                        Root    Hello Max Fwd
Vlan                Root ID             Cost    Time  Age Dly  Root Port
---------------- ------------------- --------- ----- --- ---  ------------
VLAN0001         32769 000c.85ca.e280        19    2   20  15  Fa0/7
```

This tells about the root switch from the perspective of the switch we're on. The root port is *our* port number and the root cost is cumulative, not our own configured port cost. You'll see one line of output for each VLAN (different VLANs can be configured with different root switches).

SHOW SPANNING-TREE [VLAN 1] BRIDGE

```
                                                Hello  Max  Fwd
Vlan                    Bridge ID                Time  Age  Dly  Protocol
---------------- ---------------------------------- -----  ---  ---  --------
VLAN0001         32769 (32768,   1) 000d.29f3.f380    2    20   15  ieee
```

This is about our own switch's configuration. Again, one line per VLAN.

TROUBLESHOOTING

```
S1(config)# debug spanning-tree events
```
Issues a log message every time the topology changes.
```
S1(config)# undebug all
```
Turn it off when you're done.

PORTFAST

STP is slow… very slow. For switchports used by hosts, it doesn't have to be. Access ports can be declared portfast to immediately transition from blocking to forwarding when a PC is connected, skipping listening and learning. This avoids a host waiting 30 seconds after a NIC becomes active.

```
S2(config-if)# spanning-tree portfast
S2(config-if)# spanning-tree bpduguard enable
```
Dangerous to use portfast on a port where a switch might connect, so always use bpduguard too

BPDU GUARD

Several problems can arise if an uninformed or malicious person attaches their own switch to a LAN running STP.

- An STP-capable switch with a low priority could become root, creating an inefficient tree
- A cheap non-STP switch could create loops
- An attacker could attach an STP-capable switch to multiple ports, configure it to become the root switch, and route large amounts of traffic through their switch for eavesdropping.

Cisco's BPDU guard can be enabled on any switchports where other switches should never be attached. If a BPDU is heard on that port, the switch will disable the port (status=err-disabled). Enabling BPDU guard on the same ports where portfast is enabled prevents loops if a switch *is* ever attached there, by killing the port before a loop occurs.

Verifying Portfast

```
SW# show spanning-tree interface fa0/4 portfast
```

Shows for each VLAN whether enabled. Port must be up for portfast to show as enabled

```
S1# show spanning-tree interface fa0/5 detail
 Port 5 (FastEthernet0/5) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.5.
   Designated root has priority 24577, address 000c.85ca.e280
   Designated bridge has priority 24577, address 000c.85ca.e280
   Designated port id is 128.5, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 371, received 0
```

GLOBAL PORTFAST & BPDU GUARD

Portfast and Bpduguard can also be enabled switch-wide and then turned off on individual ports.

```
SW(config)#spanning-tree portfast default
SW(config)#spanning-tree portfast bpduguard default
SW(config-if)#spanning-tree { portfast | bpduguard } disable
```

Summary

GLOBAL	ONE INTERFACE
spanning-tree portfast default no spanning-tree portfast default	spanning-tree portfast spanning-tree portfast disable
spanning-tree portfast bpduguard default no spanning-tree portfast bpduguard default	spanning-tree bpduguard enable spanning-tree bpduguard disable

Global settings can be viewed using the "show spanning-tree summary" command. It's also a quick way to see if a switch has any blocking ports in a given VLAN.

```
S3# show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0002-VLAN0004
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    1         0        0          1          2
VLAN0002                    0         0        0          2          2
VLAN0003                    0         2        0          0          2
VLAN0004                    0         2        0          0          2
---------------------- -------- --------- -------- ---------- ----------
4 vlans                     1         4        0          3          8
```