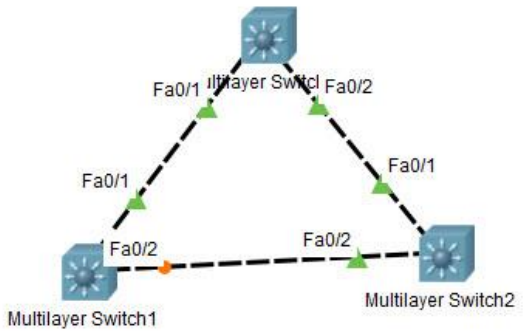
Spanning Tree Protocol:

- STP Stand for Spanning Tree Protocol.
- STP is work in Switch to avoid loop in switch's or in other words we can say the spanning Tree protocol is a network protocol that builds a loop-free logical topology for Ethernet networks.
- STP is Open Standard.
- STP works when multiple switches are used with redundant links.
- By default it is enable in CISCO Switches.
- STP will help us to create a loop free topology by blocking certain interfaces.
- Redundant link can creates network loops that flood down frames in the network.
- STP automatically removes layer 2 switching loops by shutting down redundant links.
- To finds a redundant link, it uses an algorithm, known as Spanning-tree algorithm (STA).
- STP used STA to prevent layer 2 loops.
- Spanning Tree Algorithm detecting layer 2 loops and blocks it until first one link goes down or disconnected.
- Spanning Tree Protocols use BPDU (bridge protocol data unit) in every 2 second for preventing layer 2 loops.

Let see with Example:

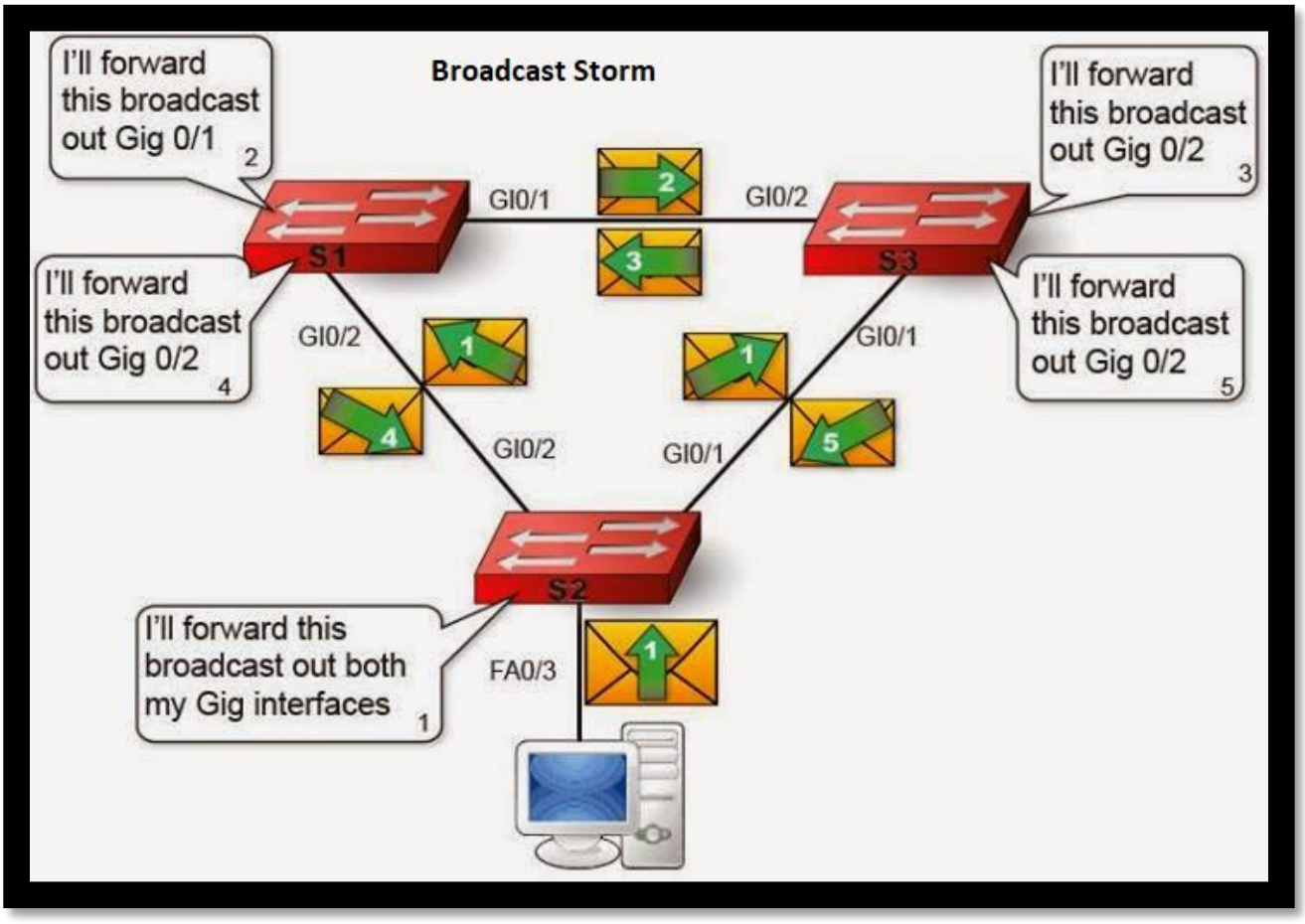


Without STP we have the following issues.

1. Broadcast Storm
2. MAC Database Instability
3. Multiple Frame Transmission

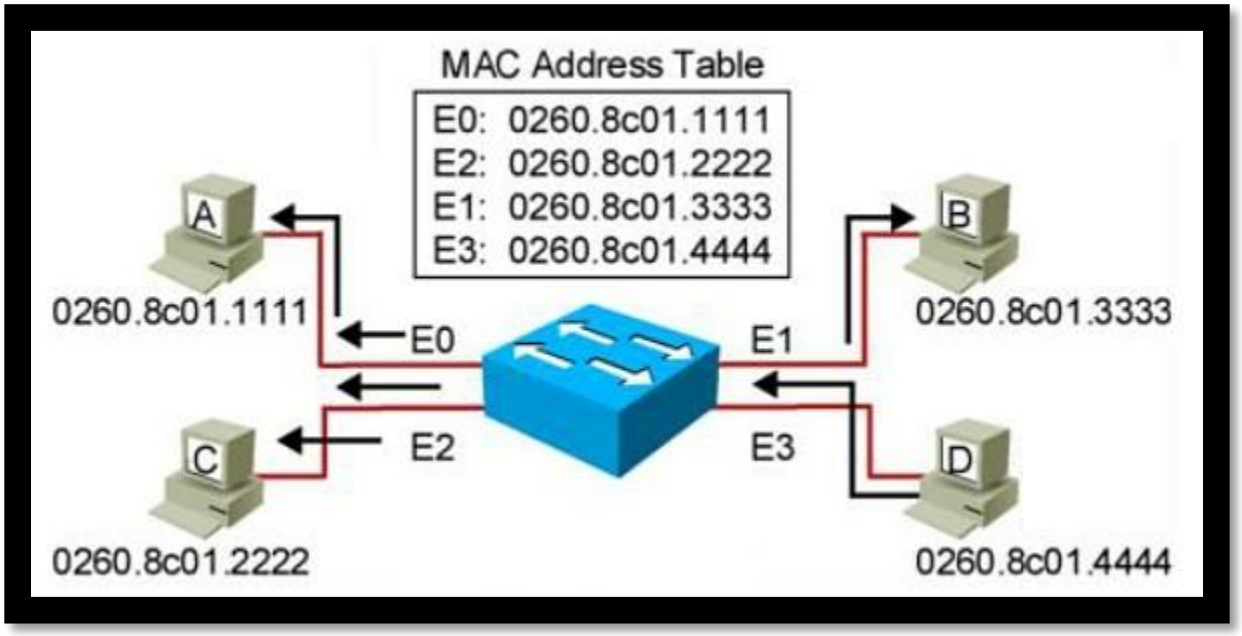
Broadcast Storm:

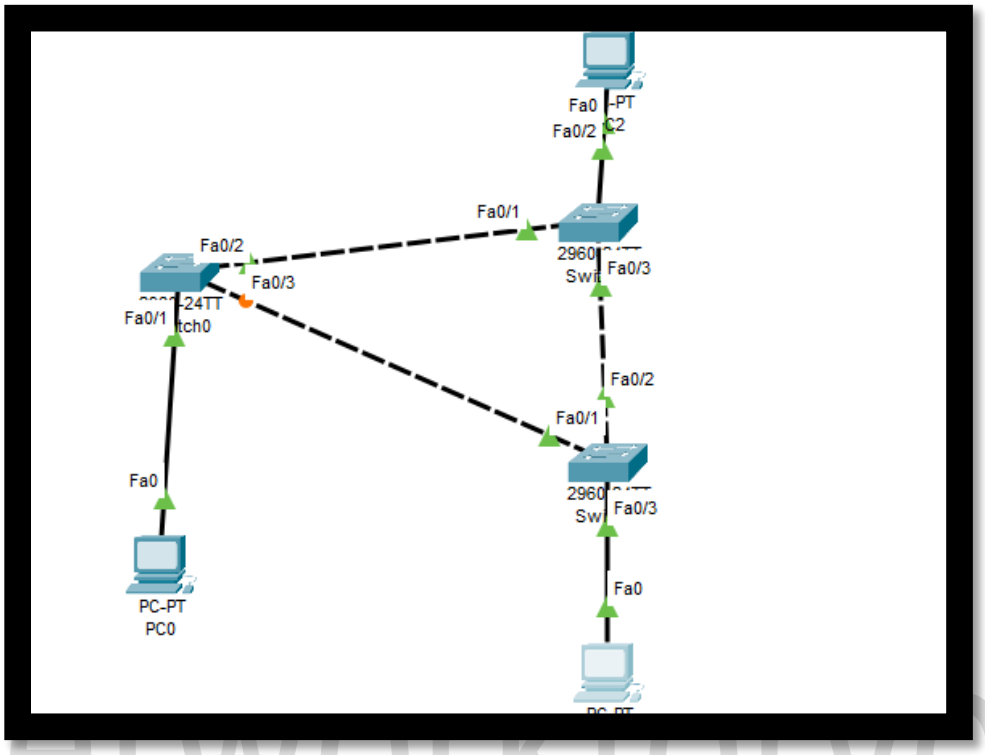
- When switch receives broadcast frame, it continues broadcasting them.
- The Switches broadcasting them again to its other interfaces.
- Broadcasting will keep going on forever until we shut down the network.
- This Process is known as Broadcast storm of switches.
- Broadcast storm consumes the entire bandwidth of the network.
- Broadcast storm denies bandwidth for normal network traffic.



MAC Database Instability:

- MAC tables are built by examining the source MAC address on a packet received.
- The source MAC address is tied to the interface it was received on.
- If loop occurs in the network then same source MAC address could be seen on more than one Interface.
- So MAC table will be unstable that is instability of MAC table causes copies of same frame to be delivered to multiple interfaces.
- MAC Instability results multiple copies of a frame arrive on different interface of switch.





Multiple Frame Transmission:

- Multiple copies of unicast frames may be delivered to destination host.
- Multiple copies of the same frame can cause unrecoverable errors.

Switch Priority:

- By default, all Cisco Switches has a Bridge Priority or Switch Priority value of 32,768.
- Bridge Priority value decides which Switch can become Root Bridge (Root Switch).
- Switch with lowest Bridge Priority (Switch Priority) Value will become the Root Switch.

Let see How STP is working.

- STP Selecting Root Bridge.
- STP Selecting Root Port.
- STP Selecting Designated port and non-Designated port.

Selecting the Root Bridge:

- The bridge with the lowest Bridge ID.
- Bridge ID = Priority + MAC address of the switch.
- All Switches priority is 32768+1 = 32769
- All Switches have same priority then they will compare MAC address.
- All Switches exchange information that is called BPDU (Bridge Protocol Data Units).
- Switches Send BPDU every 2 second.
- To Check we will use command : sh spanning-tree
- From the all switches in the network one is elected as Root Bridge. And all the remaining switches will be considered as Non root Bridge.

```
SW1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0060.2F97.B2E3
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.5882.71C6
              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
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
```

Non-Root Bridge:

- Except Root Bridge, all remaining switches of network are considered as Non-Root Bridges.
- Non-Root Bridges receive updates from Root Bridge & update their STP databases relatively.

Port Priority:

- Each port of a Switch has a Port Priority value associated with it, 128 by default.
- Gi0/1 128.20 P2P: Gi0/1 is the interface 128 is default value and 20 is port number.
- P2P means Point-to-point (Full Duplex) and Shr means Shared (Half Duplex) like hub.

Spanning Tree Port Roles:

Designated Port:

- A non – root port, which is forwarding away from the root switch.
- Switch can have multiple designated ports & marked as forwarding port.
- For root bridges all switch ports are designated ports.
- In Cisco Switches a Root Port can never be a designated port.

Non-Designated Port:

- Non-designated port having higher port cost than the designated port.
- Spanning Tree Protocol marks non-designated port as the blocking port.
- Non-designated port not forward any frames and used to remove loops.
- If any change in topology, the same port may become a designated port.
- The non-designated port of is a Cisco switch port that is blocked.
- A non-designated port of switch is not a root port or a designated port.

Root Port:

- The Root port is the port that directly connects to the Root Bridge
- The Root Port is the port which has least cost to reach root switch.
- The Root port is the port that is closest to the root bridge.
- Every non-root bridge must have a root port connect to root switch.
- Only one Root Port on non-root Switch and no Root Port in root bridge.
- A Root Port has the least cost from the "Switch" to the Root Bridge.
- The Root ports forward traffic toward the root bridge.

Alternate Port:

- Alternative port moves to the forwarding state if any change in topology.
- Alternate port is a best alternate path to the root bridge or Switch.

Forwarding Ports:

- It also has two type designated ports and Root ports.

Blocking Ports:

- It is also called Non-Forwarding ports

Selecting the Root Port:

- Shortest path to the root bridge (Every non root bridge looks the best way to go root bridge) Least cost (speed).
- Typical Costs of different Ethernet networks.

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

STP Port states

1. Listening 15 sec.
2. Learning 15 sec.
3. Blocking 20 sec.
4. Forwarding No limits
5. Disable No limits

Listening State:

- After blocking state, Root Port or Designated Port will move to listening state.
- During listening state, port discards frames received from attached network segment.
- During listening state port discards frames switched from another port for forwarding.
- After 15 seconds, the switch port moves from the listening state to the learning state.

Learning State:

- Only root port & designated ports enter into learning state from listening.
- A Cisco Switch port change to learning state after the listening state.
- During the learning state, the port is listening for and processing BPDUs.
- In the learning state, the port begins to process the user frames.
- In the learning state, the port start updating the MAC address table.
- Data or user frames are not forwarded to the destination port of switch.
- After 15 seconds, switch port moves from learning state to forwarding state.

Forwarding State:

- In this state, the switch listens and processes both BPDUs and user frames.
- Port in forwarding state forwards frames across attached network segment.
- In forwarding state, port will process BPDUs & update its MAC Address table.
- Data frames are forwarded to destination, Forwarding State is normal state.
- The Data and configuration messages are passed through the port or link.

Blocking State:

- When we power on a Switch, the switch puts all of its ports in this state.
- The Switch Ports will go into a blocking state at the time of election process.
- In Blocking state, the switch only listens and processes the BPDUs only.
- Switch port in blocking state does not participate in frame forwarding.
- Port in blocking state discards frames received from attached network segment.
- During blocking state, port only listening & processing BPDUs on its interfaces.
- After 20 seconds, Switch port changes from the blocking state to listening state.

Disabled State:

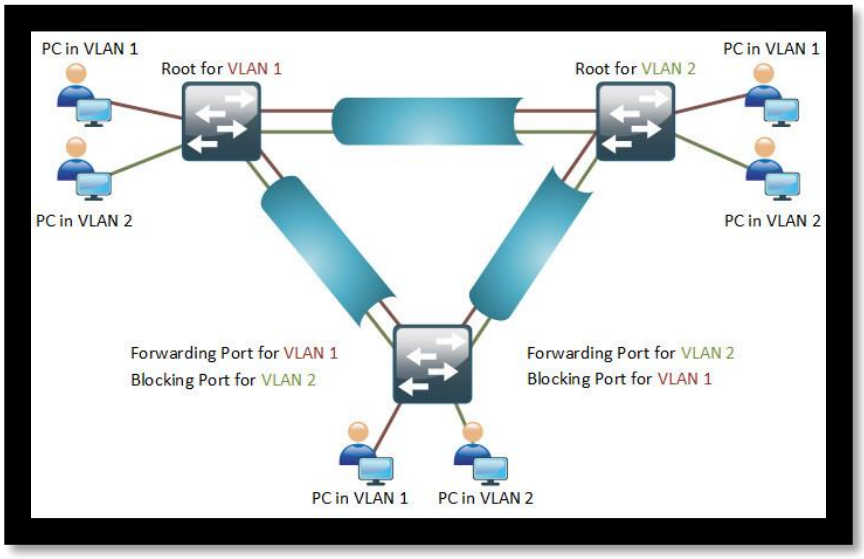
- A port in the disabled state does not participate in frame forwarding.
- A port in the disabled state does not participate in operation of STP.
- A port in the disabled state is considered non-operational.
- This state applies to all ports which are either manually shut down.
- All unplugged ports or interface also remain in Disabled state.

Type of STP:

Type of STP				
Protocol	**Standard**	**Resources Need**	**Convergence**	**Numbers of Trees**
STP	802.1D	Low	Slow	One
PVST+	CISCO	High	Slow	One for Every VLAN
RSTP	802.1W	Medium	Fast	One
Rapid PVST+	CISCO	Very High	Fast	One for Every VLAN
MST	802.1S	Medium or High	Fast	One for Multiple Vlans

PVST+:

- PVST+ stands for Per VLAN Spanning Tree Plus (PVST+).
- PVST+ is a CISCO Implementation of STP.
- Per-VLAN Spanning Tree+ (PVST+) is an extension of the PVST standard.
- PVST+ supports DOT1Q trucking encapsulation while PVST not support.
- PVST+ Provide each VLAN have its own Spanning Tree Protocol topology.
- PVST is usually the default spanning tree protocol on CISCO Switches.
- PVST+ takes 30 to 50 seconds to transit from blocking state to forwarding state.



RPVST+:

- RPVST+ stands for Rapid Per-VLAN Spanning Tree Plus.
- Rapid PVST+ is an enhanced version of the PVST+ version.
- Rapid PVST+ allows for faster spanning Tree calculations and convergence.
- RSTP is typically able to respond less than 10 seconds of a physical link failure.
- Rapid PVST+ defines three port states Discarding, Learning and Forwarding.
- We can enable RSTP by using command: spanning-tree mode rapid-pvst

STP	RSTP
Disabled	Discarding
Blocking	Discarding
Listening	Discarding
Learning	Learning
Forwarding	Forwarding

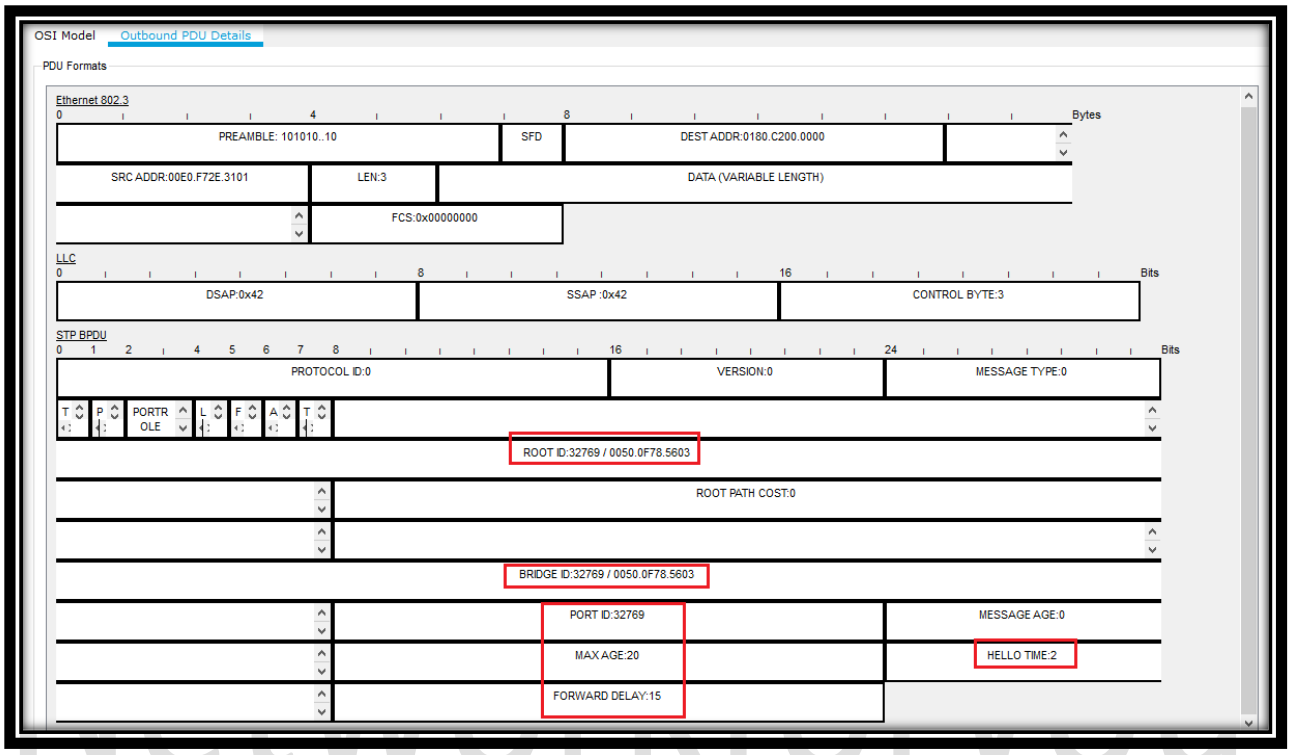
```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     0001.64B9.1217
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.64B9.1217
              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
```

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

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      1         0        0          0          1

---------------------- -------- --------- -------- ---------- ----------
1 vlans                       1         0        0          0          1
```

BPDU (Bridge Protocol Data Units):

- Bridge Protocol Data Units (BPDUs) are messages exchanged between the switches.
- BPDUs frames contain info about switch ID, originating switch port & MAC address.
- BPDUS frames also contain info regarding switch port priority, switch port cost etc.
- Bridge Protocol Data Units (BPDUs) frames are sent out as multicast messages regularly.
- BPDUS frames use the multicast destination MAC address which is 01:80:c2:00:00:00.
- When BPDUs are received, the Switch uses a mathematical formula called the STA.
- Spanning Tree Algorithm (STA) know when there is a Layer 2 Switch loop in network.
- Spanning Tree Algorithm determines which of redundant ports needs to be shut down.
- Three types of BPDUs are Configuration BPDU, Topology Change Notification (TCN) BPDU and Topology Change Notification Acknowledgment (TCA).
- Basic purpose of BPDUs & Spanning Tree Algorithm is to avoid Layer 2 Switching loops.
- Basic purpose of BPDUs and Spanning Tree Algorithm to avoid Layer 2 Broadcast storms.
- Configuration BPDUs are used to elect the Root Bridges, root ports, and designated ports.
- When topology change occurs, Switch send TCN BPDU out its root port, destined for Root.
- TCN contains no information about the change – it only indicates that a change occurred.
- By responding with a TCN with the Topology Change Acknowledgement (TCA) flag set.

- Once Root Bridge receives the TCN, it will send out a configuration BPDU to all switches.



Spanning Tree Timers:

STP timers are hello timer, forward delay timer and max age timer.

Hello Time:

- Hello Time, defines interval Root Bridge send out configuration BPDUs.
- The Default Spanning Tree Protocol (STP) hello timer is 2 seconds.
- STP hello timer can be adjust to any value between 1 and 10 seconds.

Forward Delay:

- Forward delay timer is time interval spent in listening & learning state.
- The Forward Delay is the length of the Listening and the Learning states.
- Default Spanning Tree Protocol (STP) forward delay timer is 15 seconds.
- STP forward delay timer can be adjust to any value between 4 & 30 seconds.

Maximum Age:

- The Spanning Tree Maximum Age timer often referenced as MaxAge.
- If the port no longer receives the BPDUs after the Max Age time has elapsed.
- Switch assumes that topology change must have occurred & BPDU is aged out.
- By default, Spanning Tree Protocol Maximum Age timer is set to 20 seconds.
- The STP max age timer can be tune to any value between 6 and 40 seconds.

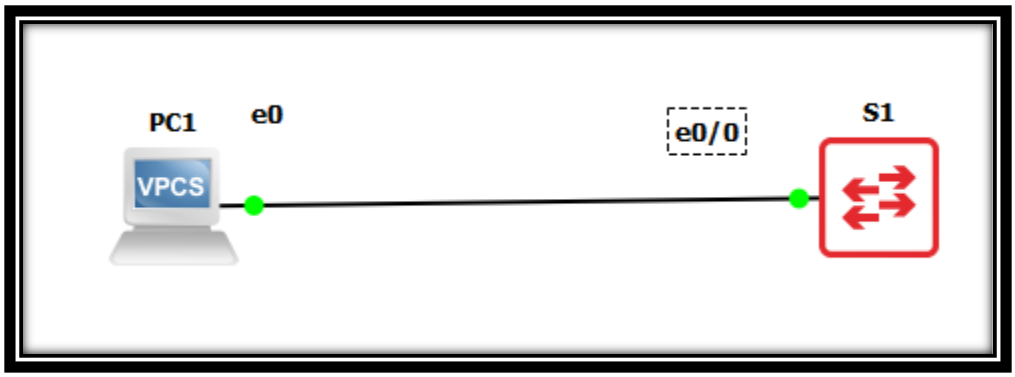
Commands	Description
show spanning-tree vlan 1	Display STP details
spanning-tree vlan 1 hello-time 5	Changing STP Hello time
spanning-tree vlan 1 forward-time 20	Changing STP Forward Delay time
spanning-tree vlan 1 max-age 40	Changing STP Maximum Age time

Port Fast:

- By passing the listening & learning states, go to forwarding mode.
- STP PortFast feature causes a port to enter forwarding state immediately.
- Port Fast port normally connect to end devices such as server, printer or PC.
- Do not enable portfast on an interface to another device which is hub/switch.
- If Port Fast feature port connect to a cisco switches, it may cause a loop.
- PVST+, Rapid PVST+, or MSTP Spanning tree all support Port Fast feature.
- Port Fast can be enable on interface level or globally on Cisco switch.
- When running globally it enable Portfast on interface that is edge port.

Enable Portfast Feature	We can check by debug
interface e0/0 spanning-tree portfast no shutdown	debug spanning-tree events

Lab Time:



PC Configuraiton:	Switch Configuration:
PC1> sh ip NAME : PC1[1] IP/MASK : 0.0.0.0/0 GATEWAY : 0.0.0.0 DNS : MAC : 00:50:79:66:68:00 LPORT : 10001 RHOST:PORT : 127.0.0.1:10002 MTU: : 1500 PC1> ip 192.168.1.2/24 192.168.1.1 Checking for duplicate address... PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1 PC1> sh ip NAME : PC1[1] IP/MASK : 192.168.1.2/24 GATEWAY : 192.168.1.1 DNS : MAC : 00:50:79:66:68:00 LPORT : 10001 RHOST:PORT : 127.0.0.1:10002 MTU: : 1500	interface e0/0 spanning-tree portfast no shutdown Or we can enable globally SW1(config)#spanning-tree portfast default Portfast can also be enabled globally for all interfaces running in access mode.

PC1> save Saving startup configuration to startup.vpc . done	

Without Port Fast:

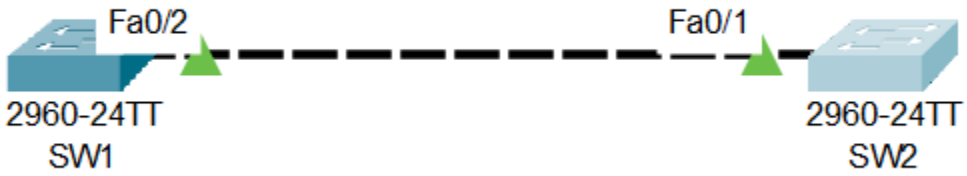
```
S1#debug spanning-tree events
Spanning Tree event debugging is on
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int e0/0
S1(config-if)#sh
S1(config-if)#
*Sep 25 16:54:33.795: STP: VLAN0001 we are the spanning tree root
*Sep 25 16:54:33.795: STP[1]: Generating TC trap for port Ethernet0/0
S1(config-if)#
*Sep 25 16:54:35.799: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Sep 25 16:54:36.806: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to dow
n
S1(config-if)#no sh
S1(config-if)#
*Sep 25 16:54:42.356: set portid: VLAN0001 Et0/0: new port id 8001
*Sep 25 16:54:42.356: STP: VLAN0001 Et0/0 -> listening
S1(config-if)#
*Sep 25 16:54:44.353: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Sep 25 16:54:45.353: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
S1(config-if)#
*Sep 25 16:54:57.362: STP: VLAN0001 Et0/0 -> learning
S1(config-if)#
*Sep 25 16:55:12.362: STP[1]: Generating TC trap for port Ethernet0/0
*Sep 25 16:55:12.362: STP: VLAN0001 Et0/0 -> forwarding
S1(config-if)#
```

With Port Fast:

```
S1(config)#int e0/0
S1(config-if)#sp
S1(config-if)#spanning-tree por
S1(config-if)#spanning-tree portfa
S1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on Ethernet0/0 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)#sh
S1(config-if)#n
*Sep 25 17:02:20.779: STP: VLAN0001 we are the spanning tree root
S1(config-if)#no
*Sep 25 17:02:22.785: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Sep 25 17:02:25.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
S1(config-if)#no sh
S1(config-if)#
*Sep 25 17:02:34.970: set portid: VLAN0001 Et0/0: new port id 8001
*Sep 25 17:02:34.970: STP: VLAN0001 Et0/0 ->jump to forwarding from blocking
S1(config-if)#
*Sep 25 17:02:36.975: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Sep 25 17:02:37.979: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
```

Spanning-Tree RootGuard:

- RootGuard will make sure you don't accept a certain switch as a root bridge.
- BPDUs are sent and processed normally but if a switch suddenly sends a BPDU with a superior bridge ID it won't accept it as the root bridge.



In this SW2 is root switch and we enable root guard in SW2 on interface f0/1

So when SW1 try to send superior bridge ID . SW2 will not accept it and block that port let see.

SW1 Configuration:	SW2 Configuration:
en config t hostname SW1 spanning-tree vlan 1 priority 0	en config t hostname SW2 interface FastEthernet0/1 spanning-tree guard root

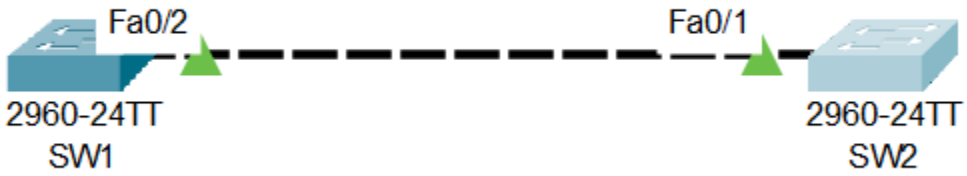
Spanning-Tree BPDUGuard:

- Spanning-Tree BPDUGuard is a security feature that protects a network from rogue switches.
- It does this by blocking BPDUs (Bridge Protocol Data Units) from unknown sources.
- If a switch receives a BPDU from an unknown source, it will immediately shut down the port that received the BPDU.
- This prevents the rogue switch from taking over the network.
- BPDUGuard is especially important in networks with multiple switches.
- If a rogue switch is connected to the network, it can send BPDUs that cause the other switches to reconfigure their spanning tree topology.
- This can lead to network loops and outages.

- To enable BPDUGuard, you need to configure it on each switch in the network. The configuration is usually very simple. For example, on a Cisco switch, you would use the following command:

Int f0/1

spanning-tree bpduguard enable



SW1 Configuration:	SW2 Configuration:
en config t hostname SW1	en config t hostname SW2 interface FastEthernet0/1 spanning-tree bpduguard enable

SW2(config)#spanning-tree portfast bpduguard default

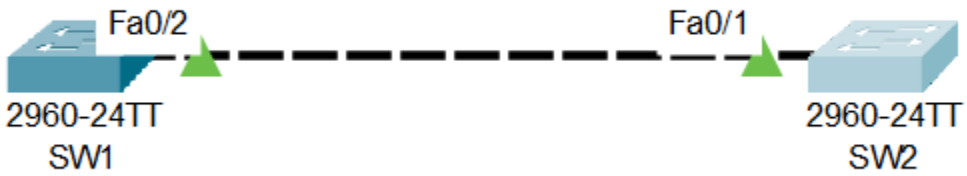
We can also use the spanning-tree portfast bpduguard default command. This will globally activate

BPDUguard on all interfaces that have portfast enabled.

BPDU Filter:

- **The spanning tree BPDU filter works similarly to BPDU Guard as it allows you to block malicious BPDUs.**
- The difference is that BPDUguard will put the interface that receives the **BPDU on in err-disable mode (brings down)** while **BPDU filter just "filters" it.**
- BPDU filter can be configured globally or on the interface level.

- Global: if you enable BPDU filter globally then any interface with **portfast enabled** will not send or receive any BPDUs. When you receive a BPDU on a portfast-enabled interface it will lose its portfast status, disables BPDU filtering, and acts as a normal interface.
- Interface: if you enable BPDU filter on the interface it will ignore incoming BPDUs, and it will not send any BPDUs. This is the equivalent of disabling spanning tree.
- We have to be careful when we enable BPDU filter on interfaces.
- We can use it on interfaces in access mode that connect to computers but make sure we never configure it on interfaces connected to other switches.



If we want to enable under interface we will use the below command:
SW2(config)#interface fa0/1 SW2(config-if)#spanning-tree portfast trunk SW2(config-if)#spanning-tree bpdufilter enable
If we want to enable Globally then we will use the below command:
SW2(config)#spanning-tree portfast bpdufilter default

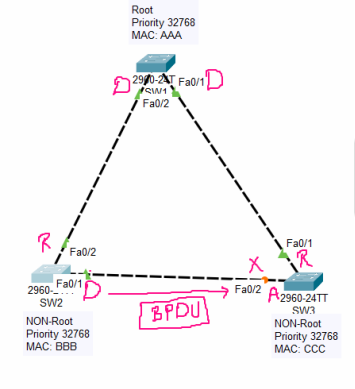
Spanning-Tree LoopGuard:

- If you ever used fiber cables you might have noticed that there is a different connector to transmit and receive traffic

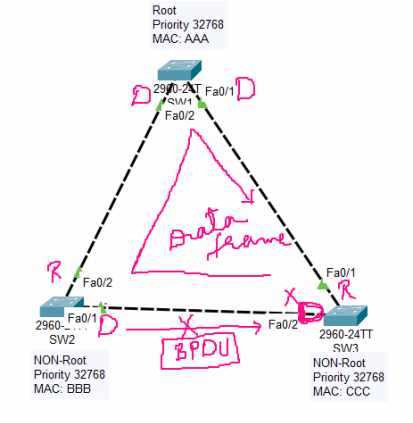
If one of the cables (transmit or receive) fails we'll have a unidirectional link failure and this can cause spanning tree loops.

There are two protocols that can take care of this problem:

- LoopGuard
- UDLD (Unidirectional Link Detection)



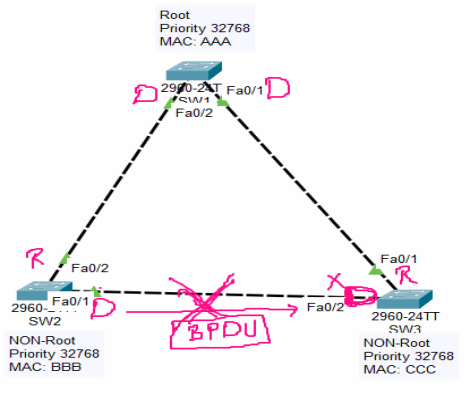
Imagine the links between the switches are fiber links. In reality there's a different connector for transmit and receive. SW3 is receiving BPDUs from SW2 and as a result the interface has become an alternate port and is in blocking mode.



Now something goes wrong…the transmit connector on SW2 towards SW3 failed due to unknown reasons. As a result, SW3 is not receiving any BPDUs from SW2 but it can still send traffic to SW2

Because SW3 is not receiving anymore BPDUs on its alternate port it will go into forwarding mode. We now have a one way loop as indicated by the arrow.

One of the methods we can use to solve our unidirectional link failure is to configure LoopGuard. When a switch is sending but not receiving BPDUs on the interface, LoopGuard will place the interface in the loop-inconsistent state and block all traffic:



Let’s enable loopguard:

SW1(config)#spanning-tree loopguard default

SW2(config)#spanning-tree loopguard default
SW3(config)#spanning-tree loopguard default

UDLD (Unidirectional Link Detection):

There are two options for UDLD:

- Normal (default)
- Aggressive

When you set UDLD to normal it will mark the port as undetermined but it won't shut the interface when something is wrong. This is only used to "inform" you but it won't stop loops.

Aggressive is a better solution. When it loses connectivity to a neighbor it will send a UDLD frame out once a second for 8 seconds. If the neighbor does not respond the interface will be put in err-disable mode.