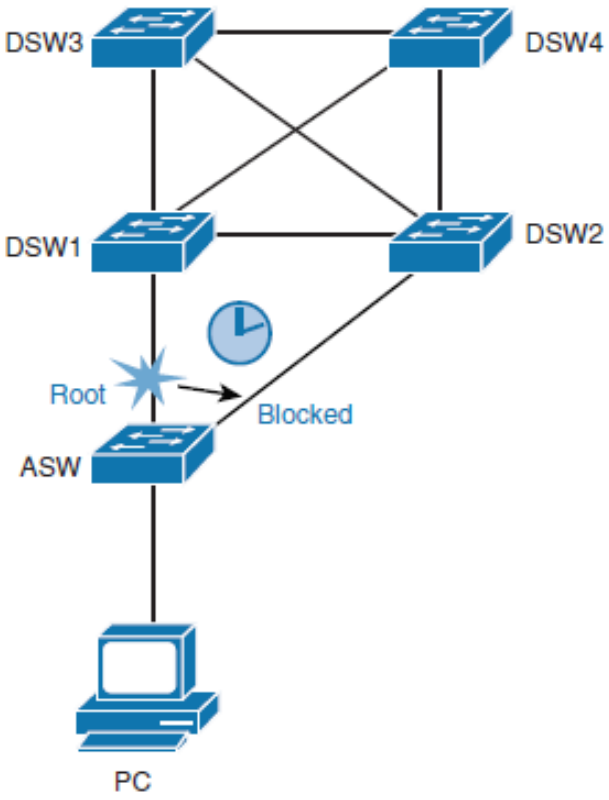
STP Enhancements

Md. Abdul Awal
awal.ece@gmail.com

UplinkFast

- If forwarding uplink fails, it will take 30 to 50 seconds for the other uplink to take over.
- UplinkFast is a Cisco proprietary solution that greatly reduces convergence time.
- The UplinkFast feature is based on the definition of an uplink group. On a given switch, the uplink group consists of the root port and all the ports that provide an alternate connection to the root bridge. If the root port fails, which means if the primary uplink fails, a port with the next lowest cost from the uplink group is selected to immediately replace it.
- The total time to recover the primary link failure will normally be less than 1 second.

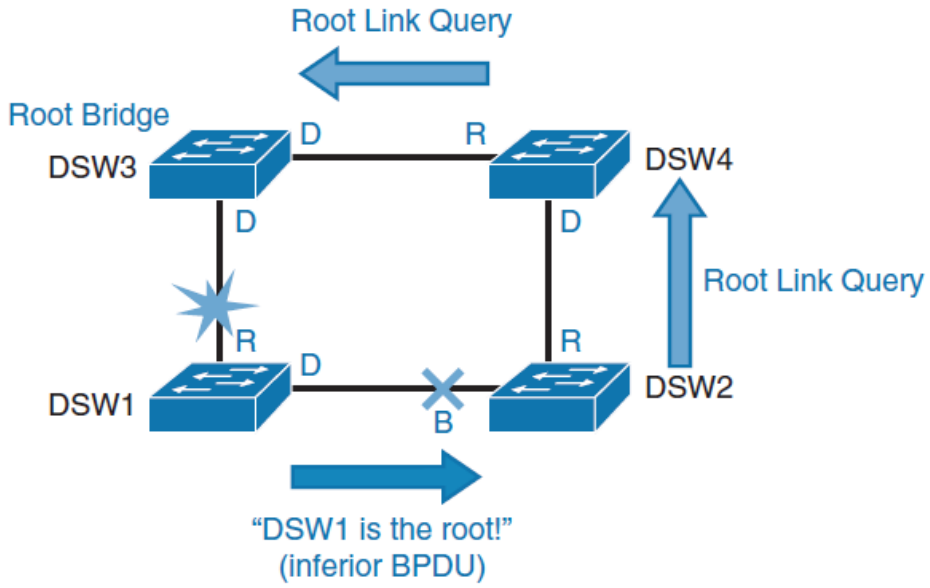
UplinkFast



- UplinkFast is a Cisco proprietary feature
- By default, UplinkFast is disabled.
- To enable UplinkFast, use the following command:
- `ASW(config)# spanning-tree uplinkfast`
- With RSTP, the UplinkFast mechanism is already integrated into the protocol in a standards-based way.

BackboneFast

- When an indirect link failure occurs, BackboneFast checks whether an alternative path exists to the root bridge.
- Indirect failure is when a link that is not directly connected to a switch fails



BackboneFast

Normally a switch must wait for the maximum age timer to expire before responding to the inferior BPDUs.

However BackboneFast searches for an alternative path:

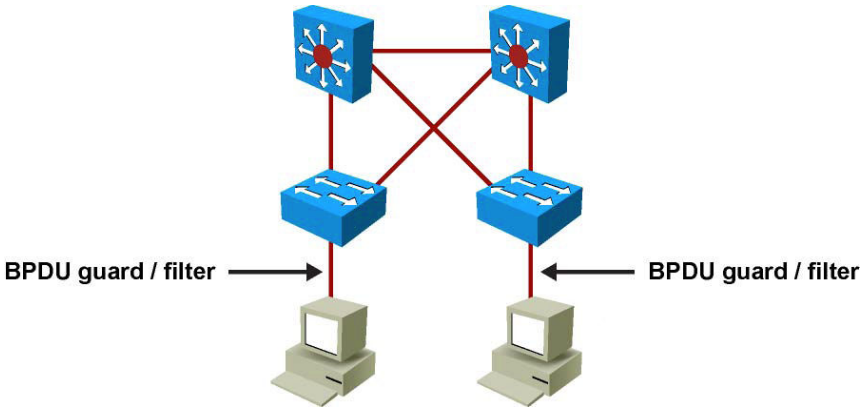
- If the inferior BPDU arrives on a port that is blocked, the switch assumes that the root port and all other blocked ports are an alternative path.
- If the inferior BPDU arrives on a port that is root, the switch assumes all blocked are an alternate path.
- If no ports are blocked, the switch assumes that it lost connectivity with the root bridge and considers itself as the root bridge.

After the switch identifies potential alternative ports, it starts sending RLQs (request link queries). By sending these queries, it finds out whether upstream switches have a path to the root bridge.

BackboneFast

- To configure BackboneFast, use the following command:
  - `DSW1(config)# spanning-tree backbonefast`
- By default, BackboneFast is disabled.
- To verify the current BackboneFast state, issue the following command:
  - `DSW1# show spanning-tree backbonefast`
  - `BackboneFast is enabled`
- BackboneFast was implemented into RSTP. RSTP implementation differs a bit from BackboneFast. Whereas BackboneFast relies on RLQ messages to validate the current root bridge, RSTP relies on cached information.

Spanning Tree Enhancements



- **BPDU guard:** Prevents accidental connection of switching devices to PortFast-enabled ports. Connecting switches to PortFast-enabled ports can cause Layer 2 loops or topology changes.
- **BPDU filtering:** Restricts the switch from sending unnecessary BPDUs out access ports.
- **Root guard:** Prevents switches connected on ports configured as access ports from becoming the root switch.
- **Loop guard:** Prevents root ports and alternate ports from moving to forwarding state when they stop receiving BPDUs.

BPDU Guard

- BPDU Guard puts an interface configured for STP PortFast in the ***err-disable*** state upon receipt of a BPDU. BPDU guard disables interfaces as a preventive step to avoid potential bridging loops.
- BPDU guard shuts down PortFast-configured interfaces that receive BPDUs, rather than putting them into the STP blocking state (the default behavior). In a valid configuration, PortFast-configured interfaces should not receive BPDUs. Reception of a BPDU by a PortFast-configured interface signals an invalid configuration, such as connection of an unauthorized device.
- BPDU guard provides a secure response to invalid configurations, because the administrator must manually re-enable the err-disabled interface after fixing the invalid configuration. It is also possible to set up a time-out interval after which the switch automatically tries to re-enable the interface. However, if the invalid configuration still exists, the switch err-disables the interface again.

BPDU Guard Configuration

- To enable BPDU guard globally, use the command:
  - **`spanning-tree portfast bpduguard default`**
- To enable BPDU guard on a port, use the command:
  - **`spanning-tree bpduguard enable`**
- BPDU guard logs messages to the console:

```
2009 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received
BPDU on PortFast enable port.

Disabling 2/1

2009 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left
bridge port 2/1
```

BPDU Guard Configuration Example

```
Switch(config)# spanning-tree portfast edge bpduguard default
Switch(config)# end
Switch# show spanning-tree summary totals
Root bridge for: none.
PortFast BPDU Guard is enabled
Etherchannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is short
Name            Blocking Listening Learning Forwarding STP
Active
--------------- -------- --------- -------- ---------- ---------
34 VLANs        0        0         0        36         36
```

BPDU Filtering

- BPDU filtering prevents a Cisco switch from sending BPDUs on PortFast-enabled interfaces, preventing unnecessary BPDUs from being transmitted to host devices.
- BPDU guard has no effect on an interface if BPDU filtering is enabled.
- When enabled globally, BPDU filtering has these attributes:
  - It affects all operational PortFast ports on switches that do not have BPDU filtering configured on the individual ports.
  - If BPDUs are seen, the port loses its PortFast status, BPDU filtering is disabled, and STP sends and receives BPDUs on the port as it would with any other STP port on the switch.
  - Upon startup, the port transmits ten BPDUs. If this port receives any BPDUs during that time, PortFast and PortFast BPDU filtering are disabled.
- When enabled on an interface, BPDU filtering has these attributes:
  - It ignores all BPDUs received.
  - It sends no BPDUs.

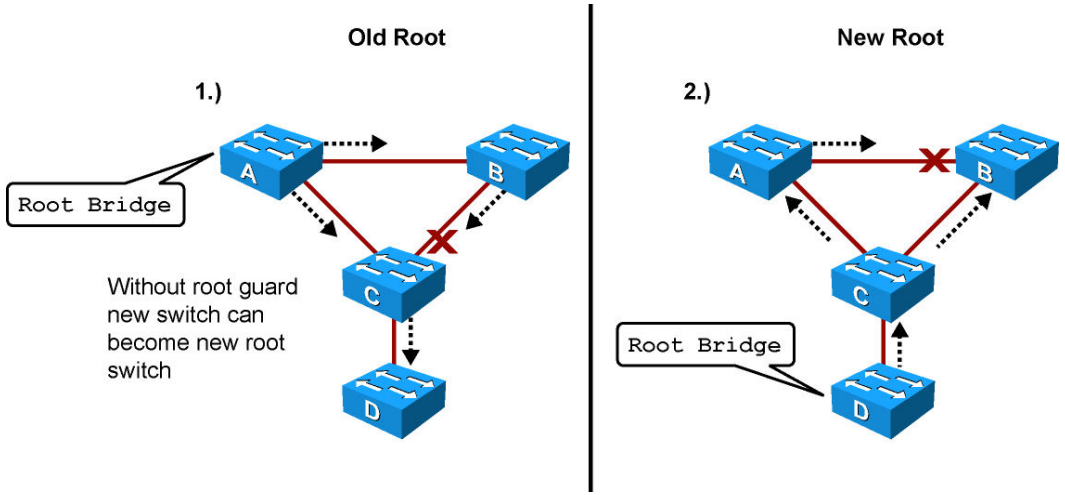
BPDU Filtering Configuration

- To enable BPDU filtering globally, use the command:
  - **`spanning-tree portfast bpdufilter default`**
- To enable BPDU guard on a port, use the command:
  - **`spanning-tree bpdufilter enable`**
- PortFast BPDU filtering status:
  - **`show spanning-tree summary`**
- Verifying PortFast BPDU filtering on a specific port:
  - **`show spanning-tree interface`** *`interface_ID`* **`detail`**

Root Guard

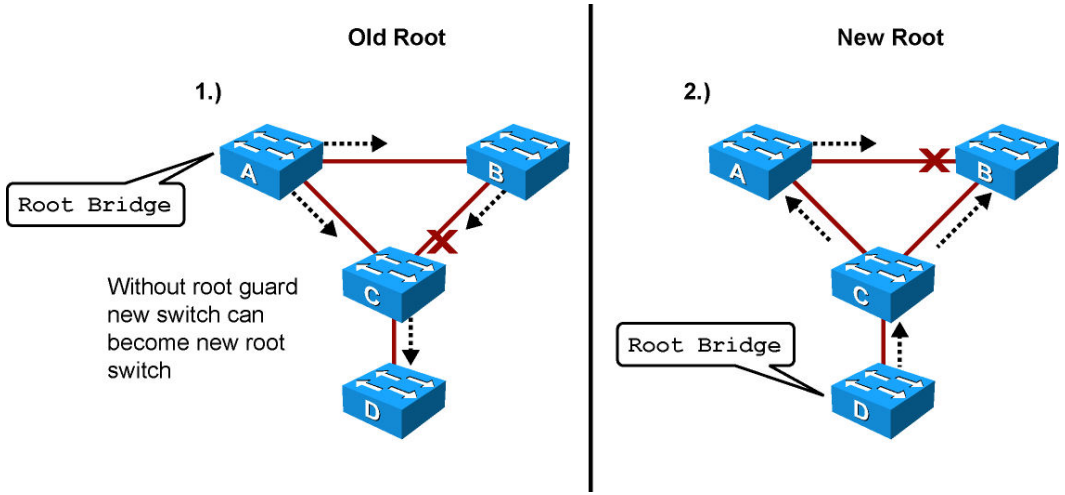
- Root guard is useful in avoiding Layer 2 loops during network anomalies. The Root guard feature forces an interface to become a designated port to prevent surrounding switches from becoming root bridges.
- Root guard-enabled ports are forced to be designated ports. If the bridge receives superior STP BPDUs on a Root guard-enabled port, the port moves to a root-inconsistent STP state, which is effectively equivalent to the STP listening state, and the switch does not forward traffic out of that port. As a result, this feature enforces the position of the root bridge.

Root Guard Motivation



- Switches A and B comprise the core of the network. Switch A is the root bridge.
- Switch C is an access layer switch. When Switch D is connected to Switch C, it begins to participate in STP. If the priority of Switch D is 0 or any value lower than that of the current root bridge, Switch D becomes the root bridge.
- Having Switch D as the root causes the Gigabit Ethernet link connecting the two core switches to block, thus causing all the data to flow via a 100-Mbps link across the access layer. This is obviously a terrible outcome.

Root Guard Operation

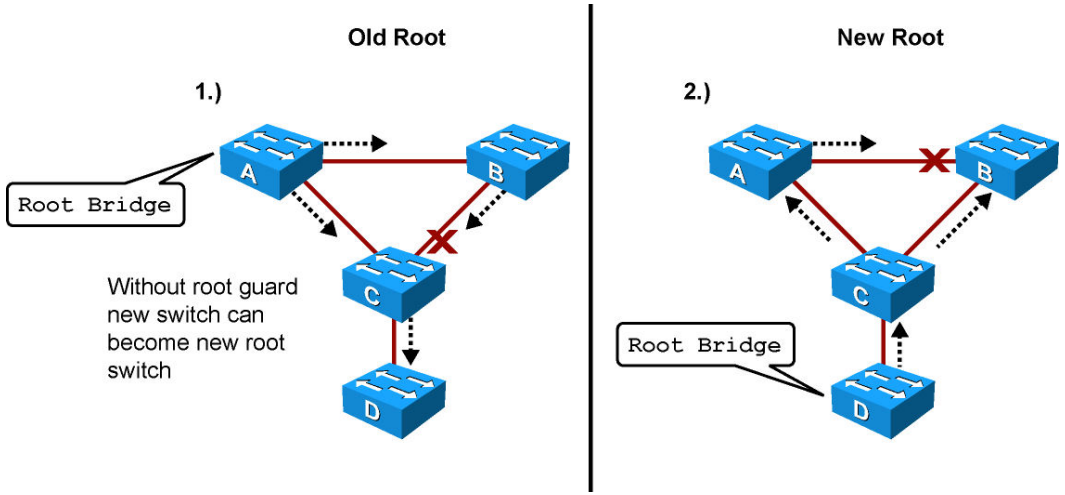


- After the root guard feature is enabled on a port, the switch does not enable that port to become an STP root port.
- Cisco switches log the following message when a root guard–enabled port receives a superior BPDU:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-
designated in VLAN 77.

Moved to root-inconsistent state.
```

Root Guard Operation

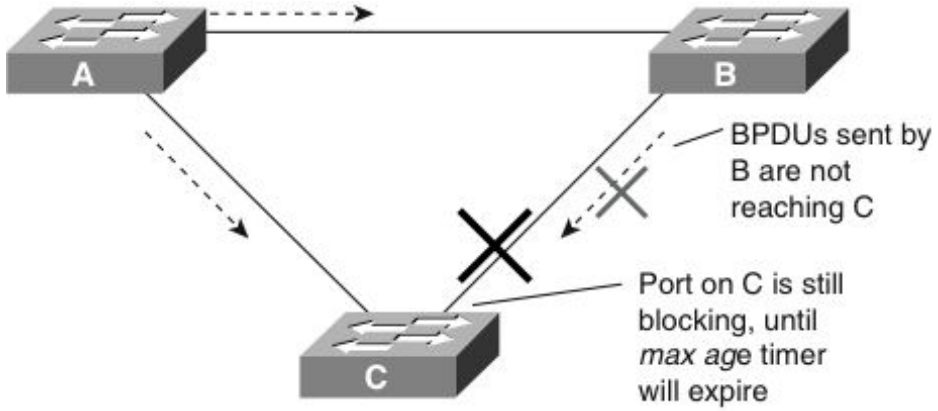


- The current design recommendation is to enable root guard on all access ports so that a root bridge is not established through these ports.
- In this configuration, Switch C blocks the port connecting to Switch D when it receives a superior BPDU. The port transitions to the ***root-inconsistent*** STP state. No traffic passes through the port while it is in root-inconsistent state.
- When Switch D stops sending superior BPDUs, the port unblocks again and goes through regular STP transition states. Recovery is automatic; no intervention is required.

Root Guard Configuration

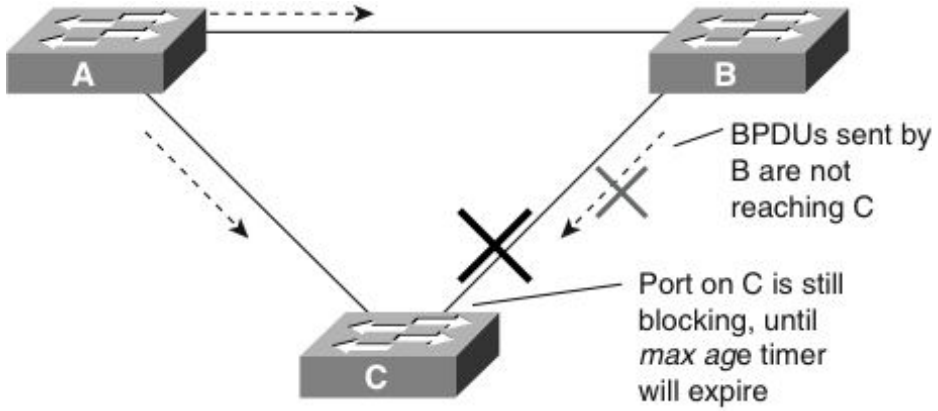
- To enable BPDU guard on a port, use the command:
  - **`spanning-tree guard root`**
- Verify Root Guard configuration:
  - **`show spanning-tree inconsistentports`**

Loop Guard



- The Loop Guard STP feature improves the stability of Layer 2 networks by preventing bridging loops.
- In STP, switches rely on continuous reception or transmission of BPDUs, depending on the port role. A designated port transmits BPDUs whereas a nondesignated port receives BPDUs.
- Bridging loops occur when a port erroneously transitions to forwarding state because it has stopped receiving BPDUs.
- Ports with loop guard enabled do an additional check before transitioning to forwarding state. If a nondesignated port stops receiving BPDUs, the switch places the port into the STP loop-inconsistent blocking state.
- If a switch receives a BPDU on a port in the loop-inconsistent STP state, the port transitions through STP states according to the received BPDU. As a result, recovery is automatic, and no manual intervention is necessary.

Loop Guard Messages



- When the Loop Guard feature places a port into the loop-inconsistent blocking state, the switch logs the following message:

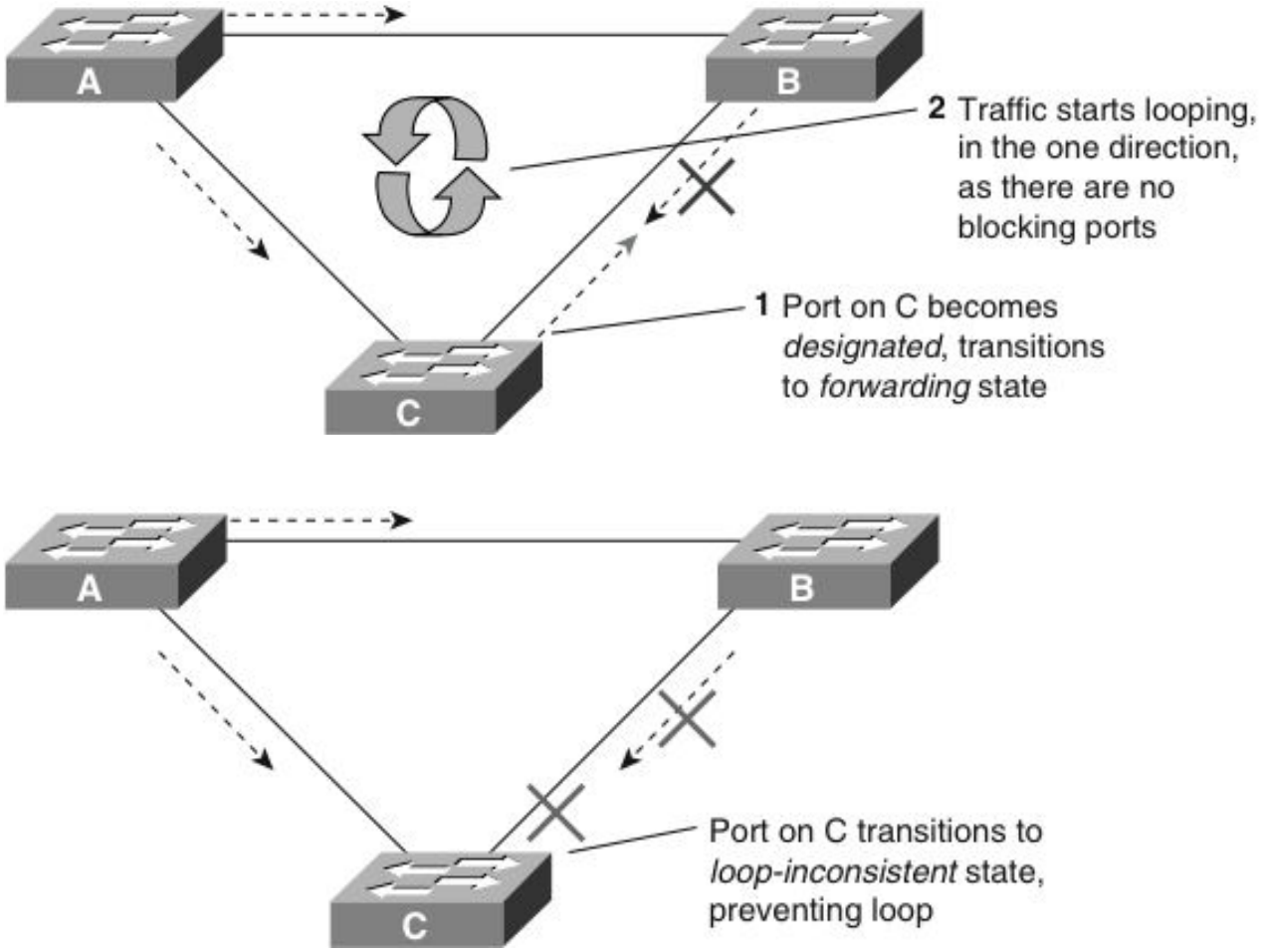
```
SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2
in vlan 3.

Moved to loop-inconsistent state.
```

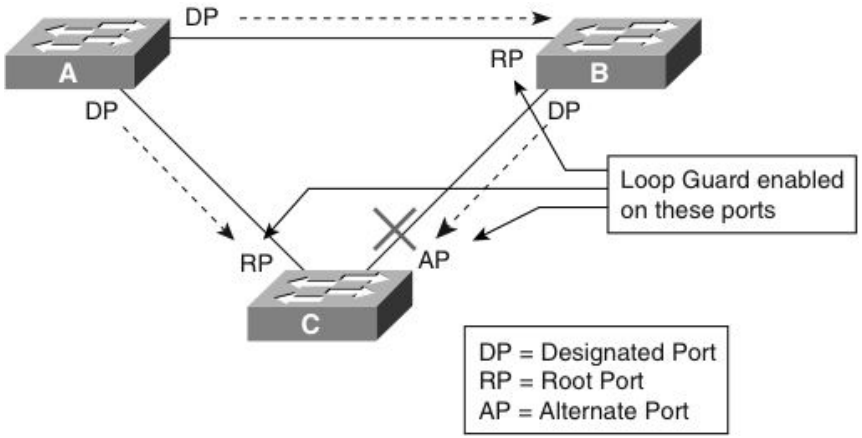
- After recovery, the switch logs the following message:

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

Loop Guard Operation



Loop Guard Configuration Considerations

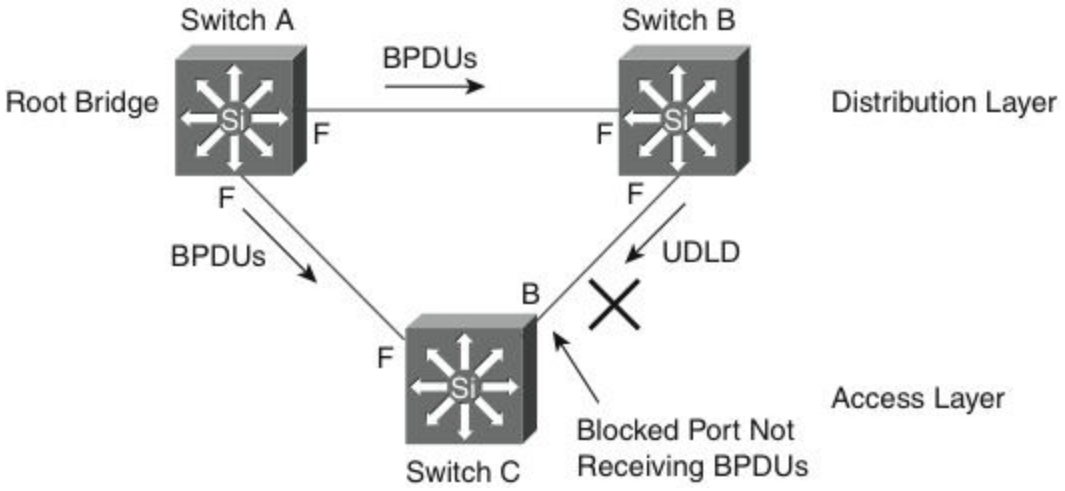


- Configure Loop Guard on a per-port basis, although the feature blocks inconsistent ports on a per-VLAN basis; for example, on a trunk port, if BPDUs are not received for only one particular VLAN, the switch blocks only that VLAN (that is, moves the port for that VLAN to the loop-inconsistent STP state). In EtherChannel interface, the channel status goes into the inconsistent state for all the ports belonging to the channel group for the particular VLAN not receiving BPDUs.
- Enable Loop Guard on all nondesignated ports. Loop guard should be enabled on root and alternate ports for all possible combinations of active topologies.
- Loop Guard is disabled by default on Cisco switches.

Loop Guard Configuration

- To enable Loop Guard globally, use the command:
  - **`spanning-tree loopguard default`**
- If Loop Guard is enabled globally, the switch enables Loop Guard only on ports considered to be point-to-point links (full-duplex links).
- To enable Loop Guard on a port, use the command:
  - **`spanning-tree guard loop`**
- Verifying Loop Guard on a specific port:
  - **`show spanning-tree interface`** *`interface_ID`* **`detail`**

Unidirectional Link Detection (UDLD)



- The link between Switches B and C becomes unidirectional. Switch B can receive traffic from Switch C, but Switch C cannot receive traffic from Switch B.
- On the segment between Switches B and C, Switch B is the designated bridge sending the root BPDUs and Switch C expects to receive the BPDUs.
- Switch C waits until the max-age timer (20 seconds) expires before it takes action. When this timer expires, Switch C moves through the listening and learning states and then to the forwarding state. At this moment, both Switch B and Switch C are forwarding to each other and there is no blocking port in the network.

UDLD Modes

- **Normal Mode**: UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. UDLD changes the UDLD-enabled port to an undetermined state if it stops receiving UDLD messages from its directly connected neighbor.
- **Aggressive Mode** (Preferred): When a port stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port state changes to the err-disable state. Aggressive mode UDLD detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links.

UDLD Configuration

- UDLD is disabled on all interfaces by default.
- The udld global configuration command affects fiber-optic interfaces only.
  - **`udld enable`** enables UDLD normal mode on all fiber interfaces.
  - **`udld aggressive`** enables UDLD aggressive mode on all fiber interfaces.
- The **`udld port`** interface configuration command can be used for twisted-pair and fiber interfaces.
  - To enable UDLD in normal mode, use the **`udld port`** command. To enable UDLD in aggressive mode, use the **`udld port aggressive`**.

STP Best Practices

- Use Layer 3 connectivity at the distribution and core layers.
- Use PVRST+ or MST. Do not disable STP at the access layer. Isolate different STP domains in a multivendor environment.
- Use Loop Guard on Layer 2 ports between distribution switches and on uplink ports from access to distribution switches.
- Use Root Guard on distribution switches facing access switches.
- Use Port security, PortFast, BPDU Guard, and Root Guard on access switch ports facing end stations.
- Use aggressive mode UDLD on ports linking switches.