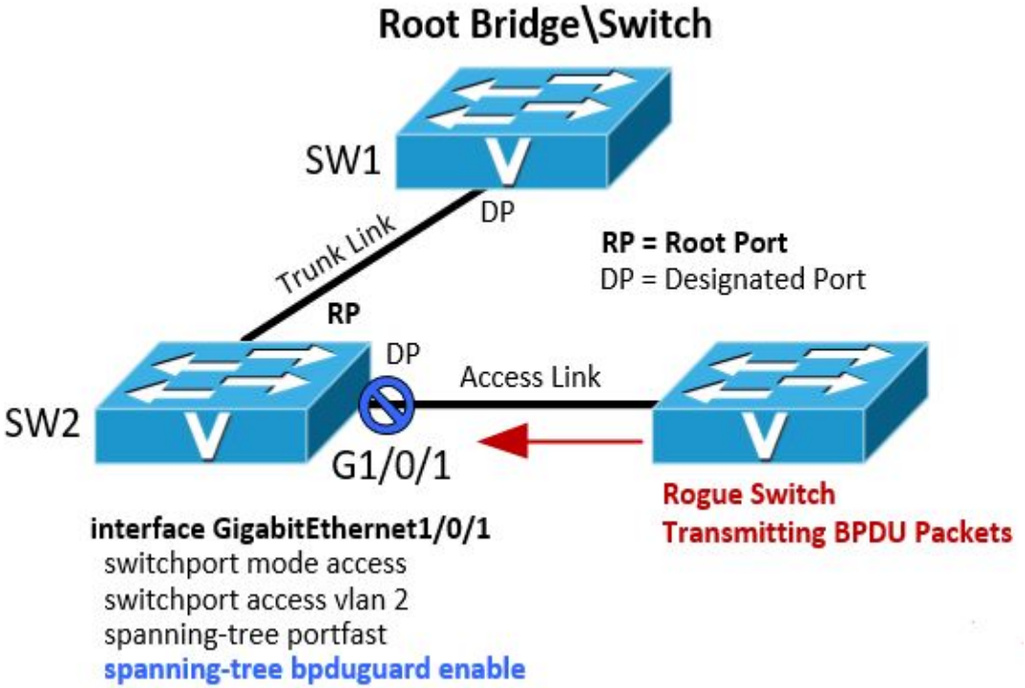
STP Security

There are two measures you can take to mitigate the STP BridgeRoot takeover attack: **BPDU Guard** and **Root Guard**.



BPDU Guard:

- Feature that comes with PortFast and is applicable

to access layer switches. It enforce the STP domain borders.

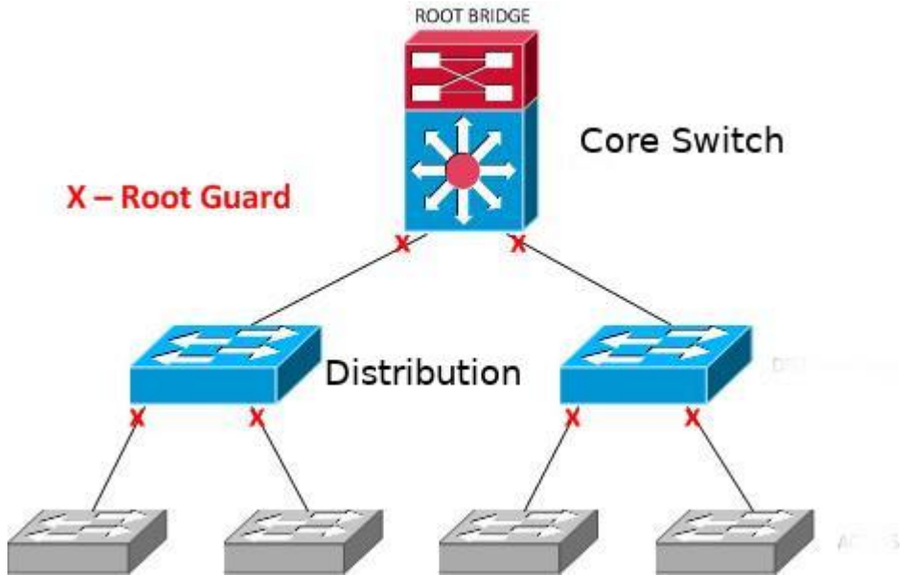
- Devices behind ports with BPDU-guard enabled are

  unable to influence the STP topology

- At the reception of a BPDU frame BPDU Guard disables the port which will move into the errdisable state and a message is generated.

Root Guard

- Root Guard can be applied on core and distribution layer switches (BPDU Guard is applied on access layer switches).
- Root Guard reacts to BPDUs which would lead to the election of a new root bridge behind protected ports. **Root Guard enforces the position of the RootBridge.**
- A violation results in the port being temporarily set to “root-inconsistent” state and not forwarding any frame.
- The port connectivity (forwarding state) will be automatically re-enabled as soon as no more illegal or superior BPDUs are received on the port.



Root Guard

- Root Guard can be applied on core and distribution layer switches (BPDU Guard is applied on access layer switches).
- Root Guard reacts to BPDUs which would lead to the election of a new root bridge behind protected ports. **Root Guard enforces the position of the RootBridge.**
- A violation results in the port being temporarily set to “root-inconsistent” state and not forwarding any frame.
- The port connectivity (forwarding state) will be

  automatically re-enabled as soon as no more

  illegal or superior BPDUs are received on the port.