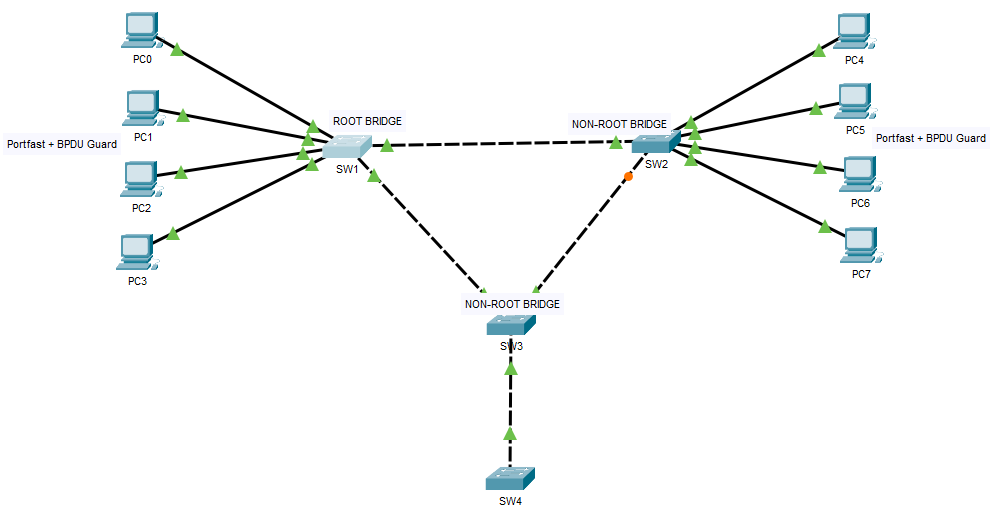
STP Portfast, BPDU Guard, Root Guard Configuration

STP Attacks Prevention

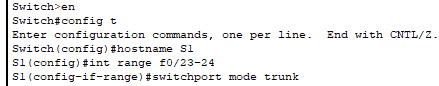
Inacio Andre

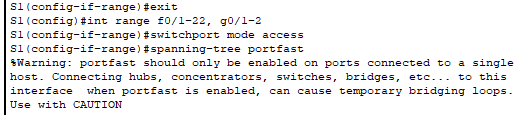
2024



* Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) are switching mechanisms that prevent a LAN with redundant links to forward Ethernet frames to loop in an indefinite time in a network. STP and RSTP have features that help the network work better and more securely, such as Portfast, BPDU Guard, and Root Guard.
* PortFast enables the switch to instantaneously transition from blocking state to forwarding state immediately through bypassing the listening and learning state. However, PortFast is highly recommended only on non-trunking access ports, such as edge ports, because these ports typically do not send nor receive BPDU.
* Because PortFast can be enabled on non-trunking ports connecting two switches, spanning-tree loops can occur because Bridge Protocol Data Units (BPDUs) are still being transmitted and received on those ports.
* Layer 2 loops in our network topology can be prevented by enabling another feature called PortFast BPDU Guard wherein it prevents the loop from happening by moving non-trunking switch ports into an errdisable state when the Bridge Protocol Data Unit (BPDU) is accepted on that port. Whenever STP BPDU guard is enabled on the switch, STP shuts down PortFast-configured interfaces on the switch that received Bridge Protocol Data Unit (BPDU) instead of putting them into STP blocking state.
* In a correct configuration, PortFast-configured ports do not receive BPDU. If a PortFast-configured interface receives a Bridge Protocol Data Unit (BPDU), a misconfiguration exists. BPDU guard provides a secure response to invalid configurations because the network engineer needs to manually put the interface in a forwarding state.

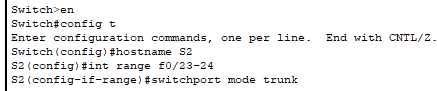
S1

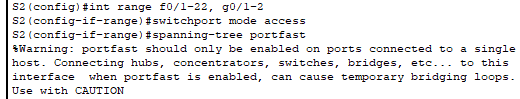






S2







S3

