**Reduceți atacurile STP**

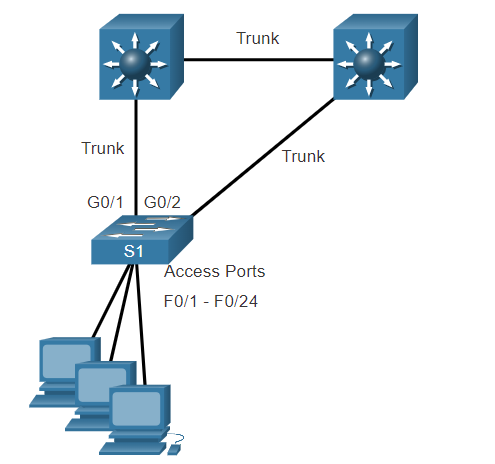
**PortFast și BPDU Guard**

Amintiți-vă că atacatorii de rețea pot manipula protocolul Spanning Tree (STP) pentru a efectua un atac prin falsificarea podului rădăcină și modificarea topologiei unei rețele. Pentru a atenua atacurile de manipulare Spanning Tree Protocol (STP), utilizați PortFast și Bridge Protocol Data Unit (BPDU) Guard:

* **PortFast** - PortFast aduce imediat o interfață configurată ca port de acces la starea de redirecționare dintr-o stare de blocare, ocolind stările de ascultare și de învățare. Aplicați la toate porturile utilizatorului final. PortFast ar trebui configurat numai pe porturile atașate la dispozitivele finale.
* **BPDU Guard** - eroarea BPDU Guard dezactivează imediat un port care primește un BPDU. La fel ca PortFast, protecția BPDU ar trebui configurată numai pe interfețele atașate la dispozitivele finale.

În figură, porturile de acces pentru S1 ar trebui să fie configurate cu PortFast și BPDU Guard.

Există două comutatoare de nivel 3 de distribuție în partea de sus a diagramei care sunt conectate printr-un trunchi.  
Ambele comutatoare de nivel 3 au o legătură trunchială care sunt conectate la același comutator de nivel de acces 2 de mai jos. Acesta se numește S1 și este conectat pe int G0/1 și G0/2. Sub S1 sunt mai multe PC-uri, iar în partea laterală a comutatorului se afișează Porturi de acces F0/1 - F0/24.

**Configurați PortFast**

PortFast ocolește stările de ascultare și învățare STP pentru a minimiza timpul în care porturile de acces trebuie să aștepte ca STP să converge. Dacă PortFast este activat pe un port care se conectează la un alt comutator, există riscul de a crea o buclă spanning-tree.

PortFast poate fi activat pe o interfață utilizând comanda de configurare a interfeței **spanning-tree portfast .**În mod alternativ, Portfast poate fi configurat global pe toate porturile de acces utilizând comanda de configurare globală **implicită spanning-tree portfast .**

Pentru a verifica dacă PortFast este activat la nivel global, puteți utiliza fie **show running-config | începe comanda span** sau comanda **show spanning-tree summary** . Pentru a verifica dacă PortFast are o interfață activată, utilizați comanda **show running-config interface***type/number* , așa cum se arată în exemplul următor. Comanda **show spanning-tree interface***type/number***detail** poate fi folosită și pentru verificare.

Observați că atunci când PortFast este activat, sunt afișate mesaje de avertizare.

**S1(config)# interface fa0/1**

**S1(config-if)# switchport mode access**

**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 FastEthernet0/1 but will only**

**have effect when the interface is in a non-trunking mode.**

**S1(config-if)# exit**

**S1(config)# spanning-tree portfast default**

**%Warning: this command enables portfast by default on all interfaces. You**

**should now disable portfast explicitly on switched ports leading to hubs,**

**switches and bridges as they may create temporary bridging loops.**

**S1(config)# exit**

**S1# show running-config | begin span**

**spanning-tree mode pvst**

**spanning-tree portfast default**

**spanning-tree extend system-id**

**!**

**interface FastEthernet0/1**

**switchport mode access**

**spanning-tree portfast**

**!**

**interface FastEthernet0/2**

**!**

**interface FastEthernet0/3**

**!**

**interface FastEthernet0/4**

**!**

**interface FastEthernet0/5**

**!**

**(output omitted)**

**S1#**

**Configurați BPDU Guard**

Chiar dacă PortFast este activat, interfața va asculta în continuare BPDU. BPDU-urile neașteptate pot fi accidentale sau pot face parte dintr-o încercare neautorizată de a adăuga un comutator la rețea.

Dacă sunt primite BPDU-uri pe un port activat pentru BPDU Guard, acel port este pus în starea dezactivată de eroare. Aceasta înseamnă că portul este închis și trebuie reactivat manual sau recuperat automat prin comanda globală **bpduguard de recuperare cauzată de errdisable** .

BPDU Guard poate fi activat pe un port utilizând comanda **spanning-tree bpduguard enable** interface configuration. Ca alternativă, utilizați comanda de configurare globală **implicită spanning-tree portfast bpduguard pentru a activa la nivel global protecția BPDU pe toate porturile activate cu PortFast.**

Pentru a afișa informații despre starea spanning-tree, utilizați comanda **show spanning-tree summary** . În exemplu, PortFast implicit și BPDU Guard sunt ambele activate ca stare implicită pentru porturile configurate ca mod de acces.

**Notă** : activați întotdeauna BPDU Guard pe toate porturile activate pentru PortFast.

**S1(config)# interface fa0/1**

**S1(config-if)# spanning-tree bpduguard enable**

**S1(config-if)# exit**

**S1(config)# spanning-tree portfast bpduguard default**

**S1(config)# end**

**S1# show spanning-tree summary**

**Switch is in pvst mode**

**Root bridge for: none**

**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**

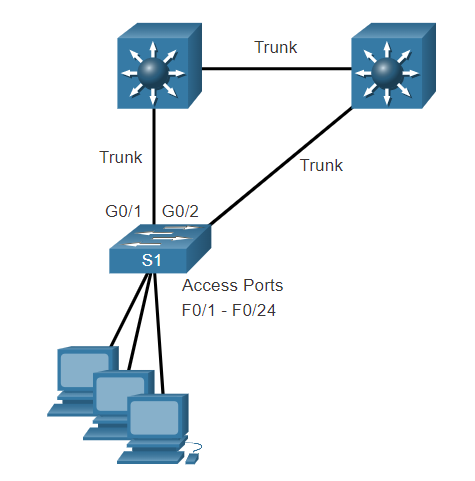
**(output omitted)**

**S1#**

**Syntax Checker - Reduceți atacurile STP**

Implementați PortFast și BPDU Guard pentru un comutator bazat pe următoarea topologie și pe cerințele specificate

Verificatorul de sintaxă are o topologie în care există două comutatoare de nivel 3 de distribuție în partea de sus a diagramei care sunt conectate printr-un trunchi. Ambele comutatoare de nivel 3 au o legătură trunchială care sunt conectate la același comutator de nivel de acces 2 de mai jos. Acesta se numește S 1 și este conectat pe G0/1 și G0/2. Sub S 1 sunt mai multe P C-uri și în partea laterală a comutatorului se afișează Porturi de acces F0/1 - F0/24.12.1.5.



**You are currently logged into S1. Complete the following steps to implement PortFast and BPDU Guard on all access ports:**

**Enter interface configuration mode for fa0/1 - 24.**

**Configure the ports for access mode.**

**Return to global configuration mode.**

**Enable PortFast by default for all access ports.**

**Enable BPDU Guard by default for all access ports.**

**S1(config)#interface range fa0/1 - 24**

**S1(config-if-range)#switchport mode access**

**S1(config-if-range)#exit**

**S1(config)#spanning-tree portfast default**

**S1(config)#spanning-tree portfast bpduguard default**

**S1(config)# exit**

**Verify that PortFast and BPDU Guard is enabled by default by viewing STP summary information.**

**S1#show spanning-tree summary**

**Switch is in pvst mode**

**Root bridge for: none**

**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**

**(output omitted)**

**S1#**

**You have successfully configured and verified PortFast and BPDU Guard for the switch.**