**Ce am învățat în acest modul?**

Toate porturile (interfețele) switch-ului trebuie securizate înainte ca comutatorul să fie implementat pentru utilizare în producție. Cea mai simplă și eficientă metodă de a preveni atacurile de depășire a tabelului de adrese MAC este activarea securității porturilor. În mod implicit, porturile de comutare Layer 2 sunt setate la automat dinamic (trunking activat). Comutatorul poate fi configurat pentru a afla despre adresele MAC pe un port securizat într-unul din trei moduri: configurat manual, învățat dinamic și învățat dinamic - sticky. Îmbătrânirea securității porturilor poate fi utilizată pentru a seta timpul de îmbătrânire pentru adresele securizate statice și dinamice pe un port. Două tipuri de îmbătrânire sunt acceptate pe port: absolută și inactivitate. Dacă adresa MAC a unui dispozitiv atașat la port diferă de lista de adrese securizate, atunci are loc o încălcare a portului. În mod implicit, portul intră în starea dezactivată de eroare. Când un port este oprit și plasat în starea dezactivată de eroare, nu este trimis sau primit niciun trafic pe acel port. Pentru a afișa setările de securitate a porturilor pentru comutator, utilizațiarată comanda **port-security .**

Pentru a atenua atacurile de salt VLAN:

**Pasul 1.** Dezactivează negocierile DTP pe porturile non-trunking.  
**Pasul 2.** Dezactivează porturile neutilizate.  
**Pasul 3.** Activați manual legătura trunchiului pe un port trunk.  
**Pasul 4.** Dezactivați negocierile DTP pe porturile de trunking.  
**Pasul 5.** Setați VLAN-ul nativ la un alt VLAN decât VLAN 1.

Scopul unui atac de foame DHCP este de a crea un Denial of Service (DoS) pentru conectarea clienților. Atacurile de falsificare DHCP pot fi atenuate prin utilizarea DHCP snooping pe porturile de încredere. Snooping DHCP determină dacă mesajele DHCP provin dintr-o sursă de încredere configurată administrativ sau nede încredere. Apoi filtrează mesajele DHCP și limitează rata traficului DHCP din surse nesigure. Utilizați următorii pași pentru a activa DHCP Snooping:

**Pasul 1.** Activați DHCP Snooping.  
**Pasul 2.** Pe porturile de încredere, utilizați comanda de configurare a interfeței **ip dhcp snooping trust .**  
**Pasul 3.** Limitați numărul de mesaje de descoperire DHCP care pot fi primite pe secundă pe porturi care nu sunt de încredere.  
**Pasul 4.** Activați DHCP snooping prin VLAN sau printr-o serie de VLAN-uri.

Inspecția dinamică ARP (DAI) necesită DHCP snooping și ajută la prevenirea atacurilor ARP prin:

* Nu transmiterea răspunsurilor ARP invalide sau gratuite către alte porturi din același VLAN.
* Interceptarea tuturor solicitărilor și răspunsurilor ARP pe porturi nede încredere.
* Verificarea fiecărui pachet interceptat pentru o legare IP-la-MAC validă.
* Aruncarea și înregistrarea răspunsurilor ARP care provin de la invalid pentru a preveni otrăvirea ARP.
* Eroare la dezactivarea interfeței dacă numărul DAI configurat de pachete ARP este depășit.

Pentru a reduce șansele de falsificare ARP și otrăvire cu ARP, urmați aceste linii directoare de implementare a DAI:

* Activați DHCP Snooping la nivel global.
* Activați DHCP Snooping pe VLAN-urile selectate.
* Activați DAI pe VLAN-urile selectate.
* Configurați interfețe de încredere pentru inspecția DHCP și inspecția ARP.

Ca un ghid general, configurați toate porturile comutatorului de acces ca neîncrezători și toate porturile de legătură în sus care sunt conectate la alte comutatoare ca fiind de încredere.

DAI poate fi, de asemenea, configurat pentru a verifica ambele adrese MAC și IP de destinație sau sursă:

* **Destination MAC** - Verifică adresa MAC destinație din antetul Ethernet cu adresa MAC țintă din corpul ARP.
* **Sursă MAC** - Verifică adresa MAC sursă din antetul Ethernet cu adresa MAC a expeditorului din corpul ARP.
* **Adresă IP** - Verifică corpul ARP pentru adrese IP nevalide și neașteptate, inclusiv adresele 0.0.0.0, 255.255.255.255 și toate adresele IP multicast.

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 sau trunk în 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. 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.
* **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. 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.**