**Reduceți atacurile DHCP**

**Analiza atacului DHCP**

Scopul unui atac de foame DHCP este de a crea un Denial of Service (DoS) pentru conectarea clienților. Atacurile de foame DHCP necesită un instrument de atac precum Gobbler. Amintiți-vă că atacurile de foame DHCP pot fi atenuate eficient prin utilizarea securității porturilor, deoarece Gobbler utilizează o adresă MAC sursă unică pentru fiecare solicitare DHCP trimisă.

Cu toate acestea, atenuarea atacurilor de falsificare DHCP necesită mai multă protecție. Gobbler ar putea fi configurat să utilizeze adresa MAC reală a interfeței ca adresă Ethernet sursă, dar să specifice o altă adresă Ethernet în încărcarea DHCP. Acest lucru ar face ca securitatea porturilor să fie ineficientă, deoarece adresa MAC sursă ar fi legitimă.

Atacurile de falsificare DHCP pot fi atenuate prin utilizarea DHCP snooping pe porturile de încredere.

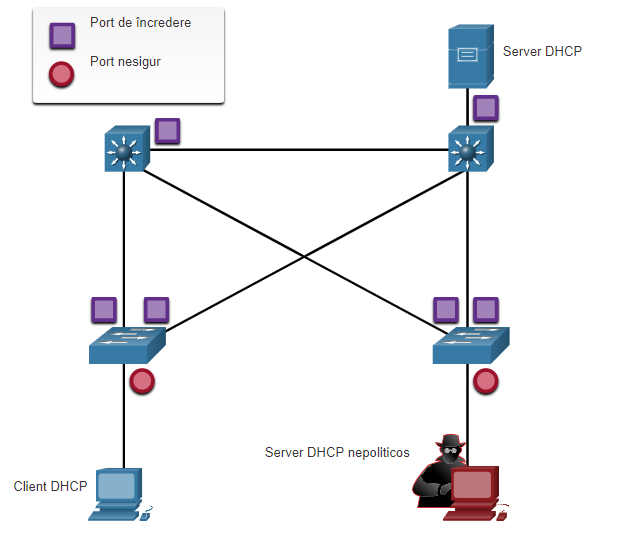
**Snooping DHCP**

Snoopingul DHCP nu se bazează pe adresele MAC sursă. În schimb, DHCP Snooping 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.

Dispozitivele aflate sub controlul dumneavoastră administrativ, cum ar fi comutatoarele, routerele și serverele, sunt surse de încredere. Orice dispozitiv dincolo de firewall sau din afara rețelei dvs. este o sursă de încredere. În plus, toate porturile de acces sunt, în general, tratate ca surse nede încredere. Figura prezintă un exemplu de porturi de încredere și nede încredere.

Diagrama prezintă un server DHCP în partea dreaptă sus a topologiei care este conectat la un comutator de distribuție de sub acesta. Comutatorul de distribuție este conectat la un alt comutator de distribuție din stânga diagramei și comutatorul de acces sub acesta. Celălalt comutator de distribuție are un comutator de acces conectat sub el. Ambele comutatoare de acces au o conexiune la ambele comutatoare de distribuție, dar unul la celălalt. Comutatorul de acces din dreapta are un computer dedesubt, iar celălalt comutator de acces are un computer cu un caracter necinstiți sub el. Diagrama prezintă un pătrat violet pentru porturile de încredere și un cerc roșu pentru porturile de încredere. Există pătrate violet între serverul DHCP și comutatorul de distribuție, precum și între fiecare legătură între toate comutatoarele. Cu toate acestea, există un cerc roșu între cele două P C-uri și comutatoarele de acces.

Client DHCPServer DHCPServer DHCP nepoliticosPort de încrederePort nesigur

Observați că serverul DHCP nepoliticos s-ar afla pe un port neîncrezat după activarea DHCP Snooping. Toate interfețele sunt tratate implicit ca nefiind de încredere. Interfețele de încredere sunt de obicei legături trunchiuri și porturi conectate direct la un server DHCP legitim. Aceste interfețe trebuie să fie configurate în mod explicit ca fiind de încredere. 

Este construit un tabel DHCP care include adresa MAC sursă a unui dispozitiv pe un port care nu are încredere și adresa IP atribuită de serverul DHCP acelui dispozitiv. Adresa MAC și adresa IP sunt legate împreună. Prin urmare, acest tabel se numește tabel de legare DHCP snooping.

**Pași pentru implementarea DHCP Snooping**

Utilizați următorii pași pentru a activa DHCP Snooping:

**Pasul 1** . Activați DHCP snooping utilizând comanda de configurare globală **ip dhcp snooping .**

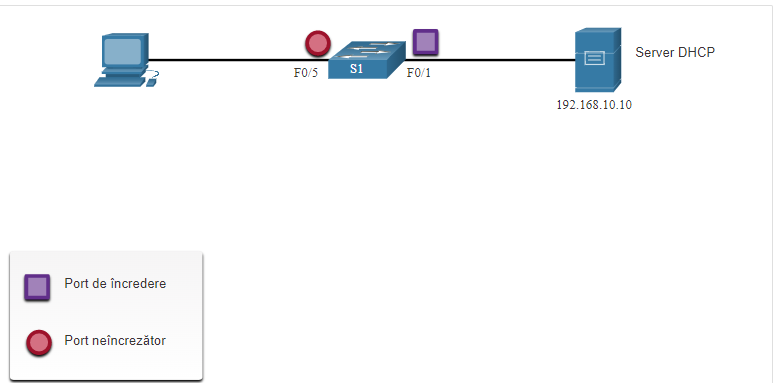
**Pasul 2** . Pe porturile de încredere, utilizați comanda de configurare a interfeței **ip dhcp snooping trust .**

**Pasul 3** . Limitați numărul de mesaje de descoperire DHCP care pot fi recepționate pe secundă pe porturi nesigure utilizând comanda de configurare a interfeței **ip dhcp snooping limit rate .**

**Pasul 4** . Activați DHCP snooping prin VLAN sau printr-o serie de VLAN-uri, utilizând comanda de configurare globală **ip dhcp snooping***vlan .*

**Exemplu de configurare DHCP Snooping**

Topologia de referință pentru acest exemplu de snooping DHCP este prezentată în figură. Observați că F0/5 este un port care nu este de încredere, deoarece se conectează la un computer. F0/1 este un port de încredere deoarece se conectează la serverul DHCP.

Graficul are o legendă cu un pătrat violet Trusted Port și un cerc roșu Untrusted Port sub diagrama topologiei. Apoi, graficul arată o rețea LAN cu un comutator cu porturi de încredere și nede încredere. Comutatorul are un PC conectat în stânga și un DHCP conectat la acesta în dreapta. Pe interfața care se conectează la PC este un cerc roșu pentru o interfață de încredere, iar pe interfața conectată la serverul DHCP este pătratul violet pentru un port de încredere.

192.168.10.10F0/5S1F0/1

Server DHCPPort de încrederePort neîncrezător

Următorul este un exemplu despre cum să configurați DHCP Snooping pe S1. Observați cum DHCP snooping este mai întâi activat. Apoi, interfața din amonte către serverul DHCP este de încredere în mod explicit. Apoi, intervalul de porturi FastEthernet de la F0/5 la F0/24 nu este de încredere în mod implicit, astfel încât o limită de rată este setată la șase pachete pe secundă. În cele din urmă, DHCP Snooping este activat pe VLANS 5, 10, 50, 51 și 52.

**S1(config)# ip dhcp snooping**

**S1(config)# interface f0/1**

**S1(config-if)# ip dhcp snooping trust**

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

**S1(config)# interface range f0/5 - 24**

**S1(config-if-range)# ip dhcp snooping limit rate 6**

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

**S1(config)# ip dhcp snooping vlan 5,10,50-52**

**S1(config)# end**

**S1#**

Utilizați comanda **show ip dhcp snooping** EXEC privilegiat pentru a verifica DHCP snooping și **afișați ip dhcp snooping binding** pentru a vedea clienții care au primit informații DHCP, așa cum se arată în exemplu.

**Notă** : Snooping DHCP este, de asemenea, cerut de Dynamic ARP Inspection (DAI), care este următorul subiect

**S1# show ip dhcp snooping**

**Switch DHCP snooping is enabled**

**DHCP snooping is configured on following VLANs:**

**5,10,50-52**

**DHCP snooping is operational on following VLANs:**

**none**

**DHCP snooping is configured on the following L3 Interfaces:**

**Insertion of option 82 is enabled**

**circuit-id default format: vlan-mod-port**

**remote-id: 0cd9.96d2.3f80 (MAC)**

**Option 82 on untrusted port is not allowed**

**Verification of hwaddr field is enabled**

**Verification of giaddr field is enabled**

**DHCP snooping trust/rate is configured on the following Interfaces:**

**Interface Trusted Allow option Rate limit (pps)**

**----------------------- ------- ------------ ----------------**

**FastEthernet0/1 yes yes unlimited**

**Custom circuit-ids:**

**FastEthernet0/5 no no 6**

**Custom circuit-ids:**

**FastEthernet0/6 no no 6**

**Custom circuit-ids:**

**S1# show ip dhcp snooping binding**

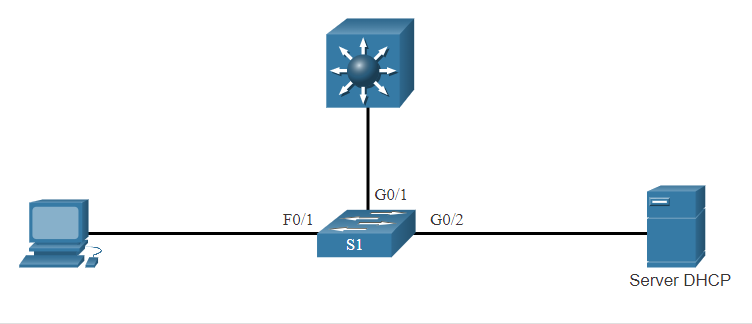
**MacAddress IpAddress Lease(sec) Type VLAN Interface**

**------------------ --------------- ---------- ------------- ---- --------------------**

**00:03:47:B5:9F:AD 192.168.10.11 193185 dhcp-snooping 5 FastEthernet0/5**

**Syntax Checker - Reduceți atacurile DHCP**

Implementați DHCP snooping pentru un comutator bazat pe următoarea topologie și cerințele specificate.



Verificatorul de sintaxă are o topologie care are un comutator de distribuție conectat la o interfață G0/1 a comutatorului de acces. Interfața comutatorului de acces F0/1 se conectează la PC în stânga, iar în partea dreaptă interfața comutatorului G0/2 este conectată la un server.

S1F0/1G0/1G0/2

Server DHCP

**You are currently logged into S1. Enable DHCP snooping globally for the switch.**

**S1(config)#ip dhcp snooping**

**Enter interface configuration mode for g0/1 - 2, trust the interfaces, and return to global configuration mode.**

**S1(config)#interface range g0/1 - 2**

**S1(config-if-range)#ip dhcp snooping trust**

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

**Enter interface configuration mode for f0/1 - 24, limit the DHCP messages to no more than 10 per second, and return to global configuration mode.**

**S1(config)#interface range f0/1 - 24**

**S1(config-if-range)#ip dhcp snooping limit rate 10**

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

**Enable DHCP snooping for VLANs 10,20,30-49.**

**S1(config)#ip dhcp snooping vlan 10,20,30-49**

**S1(config)# exit**

**Enter the command to verify DHCP snooping.**

**S1#show ip dhcp snooping**

**Switch DHCP snooping is enabled**

**DHCP snooping is configured on following VLANs:**

**10,20,30-49**

**DHCP snooping is operational on following VLANs:**

**none**

**DHCP snooping is configured on the following L3 Interfaces:**

**Insertion of option 82 is enabled**

**circuit-id default format: vlan-mod-port**

**remote-id: 0cd9.96d2.3f80 (MAC)**

**Option 82 on untrusted port is not allowed**

**Verification of hwaddr field is enabled**

**Verification of giaddr field is enabled**

**DHCP snooping trust/rate is configured on the following Interfaces:**

**Interface Trusted Allow option Rate limit (pps)**

**----------------------- ------- ------------ ----------------**

**GigabitEthernet0/1 yes yes unlimited**

**Custom circuit-ids:**

**GigabitEthernet0/2 yes yes unlimited**

**Custom circuit-ids:**

**FastEthernet0/1 no no 10**

**Custom circuit-ids:**

**Enter the command to verify the current DHCP bindings logged by DHCP snooping**

**S1#show ip dhcp snooping binding**

**MacAddress IpAddress Lease(sec) Type VLAN Interface**

**------------------ --------------- ---------- ------------- ---- --------------------**

**00:03:47:B5:9F:AD 10.0.0.10 193185 dhcp-snooping 5 FastEthernet0/1**

**S1#**

**You have successfully configured and verified DHCP snooping for the switch.**