**LAN Security Concepts**

**Distributed Denial of Service (DDoS)** –un atac coordonat de la multe dispozitive, numite zombi, cu intenția de a degrada sau opri accesul public la site-ul și resursele unei organizații.

**Încălcarea datelor** –un atac în care serverele de date sau gazdele unei organizații sunt compromise pentru a fura informații confidențiale.

**Malware** –un atac în care gazdele unei organizații sunt infectate cu software rău intenționat care cauzează o varietate de probleme. De exemplu, ransomware precum WannaCry, prezentat în figură, criptează datele de pe o gazdă și blochează accesul la acestea până când se plătește o răscumpărare.

**Un router compatibil VPN** oferă o conexiune sigură utilizatorilor la distanță printr-o rețea publică și în rețeaua întreprinderii. Serviciile VPN pot fi integrate în firewall.

Un **NGFW** oferă inspecție completă a pachetelor, vizibilitate și control al aplicațiilor, un sistem de prevenire a intruziunilor de ultimă generație (NGIPS), protecție avansată împotriva programelor malware (AMP) și filtrare URL.

Un dispozitiv **NAC** include servicii de autentificare, autorizare și contabilitate (AAA). În întreprinderile mai mari, aceste servicii pot fi încorporate într-un dispozitiv care poate gestiona politicile de acces pentru o mare varietate de utilizatori și tipuri de dispozitive. Cisco Identity Services Engine (ISE) este un exemplu de dispozitiv NAC.

**Autentificare cu o parolă locală**

***R1(config)# line vty 0 4***

***R1(config-line)# password ci5c0***

***R1(config-line)# login***

**SSH** este o formă mai sigură de acces la distanță:

-Necesită un nume de utilizator și o parolă, ambele fiind criptate în timpul transmiterii.

-Numele de utilizator și parola pot fi autentificate prin metoda bazei de date locală.

-Oferă mai multă responsabilitate, deoarece numele de utilizator este înregistrat atunci când un utilizator se conectează.

Exemplu ilustrează metodele SSH și bazele de date locale de acces la distanță.

**R1(config)# ip domain-name example.com**

**R1(config)# crypto key generate rsa general-keys modulus 2048**

**R1(config)# username Admin secret Str0ng3rPa55w0rd**

**R1(config)# ssh version 2**

**R1(config)# line vty 0 4**

**R1(config-line)# transport input ssh**

**R1(config-line)# login local**

Metoda bazei de date locală are câteva limitări:

-Conturile de utilizator trebuie configurate local pe fiecare dispozitiv. Într-un mediu de întreprindere mare, cu mai multe routere și comutatoare de gestionat, implementarea și modificarea bazelor de date locale pe fiecare dispozitiv poate dura timp.

-Configurația bazei de date locală nu oferă nicio metodă de autentificare alternativă. De exemplu, ce se întâmplă dacă administratorul uită numele de utilizator și parola pentru dispozitivul respectiv? Fără o metodă de rezervă disponibilă pentru autentificare, recuperarea parolei devine singura opțiune.

O soluție mai bună este ca toate dispozitivele să se refere la aceeași bază de date de nume de utilizator și parole de la un server central.

**Componente AAA**

AAA înseamnă Autentificare, Autorizare și Contabilitate. Conceptul AAA este similar cu utilizarea unui card de credit, așa cum se arată în figură. Cardul de credit identifică cine îl poate folosi, cât poate cheltui acel utilizator și ține cont de articolele sau serviciile achiziționate de utilizator.

AAA oferă cadrul principal pentru a configura controlul accesului pe un dispozitiv de rețea. AAA este o modalitate de a controla cui îi este permis să acceseze o rețea (autentificare), ce pot face în timp ce sunt acolo (autorizare) și de a audita ce acțiuni au efectuat în timpul accesării rețelei (contabilitate).

**Autentificarea AAA**

Local și bazat pe server sunt două metode comune de implementare a autentificării AAA.

***Autentificare locală AAA***

Local AAA stochează numele de utilizator și parolele local într-un dispozitiv de rețea, cum ar fi routerul Cisco. Utilizatorii se autentifică în baza de date locală, așa cum se arată în figură. Local AAA este ideal pentru rețelele mici.

Clientul stabilește o conexiune cu routerul.

Routerul AAA solicită utilizatorului un nume de utilizator și o parolă.

Routerul autentifică numele de utilizator și parola folosind baza de date locală, iar utilizatorului i se oferă acces la rețea pe baza informațiilor din baza de date locală.

***Autentificare AAA bazată pe server***

Cu metoda bazată pe server, routerul accesează un server central AAA, așa cum se arată în figură. Serverul AAA conține numele de utilizator și parolele pentru toți utilizatorii. Router-ul folosește fie Serviciul de acces la Remote Authentication Dial-In User Service (RADIUS), fie protocoale Terminal Access Controller Access Control System (TACACS+) pentru a comunica cu serverul AAA. Când există mai multe routere și comutatoare, AAA bazat pe server este mai potrivit.

Clientul stabilește o conexiune cu routerul.

Routerul AAA solicită utilizatorului un nume de utilizator și o parolă.

Routerul autentifică numele de utilizator și parola folosind un server AAA.

Utilizatorului i se oferă acces la rețea pe baza informațiilor din serverul AAA la distanță.

**Autorizarea** AAA este automată și nu necesită ca utilizatorii să efectueze pași suplimentari după autentificare. Autorizarea guvernează ce pot și nu pot face utilizatorii în rețea după ce sunt autentificați.

Autorizarea folosește un set de atribute care descriu accesul utilizatorului la rețea. Aceste atribute sunt utilizate de serverul AAA pentru a determina privilegiile și restricțiile pentru acel utilizator, așa cum se arată în figură.

**Contabilitatea** AAA colectează și raportează date de utilizare. Aceste date pot fi utilizate în scopuri precum auditul sau facturarea. Datele colectate pot include orele de pornire și oprire a conexiunii, comenzile executate, numărul de pachete și numărul de octeți.

**802.1X**

Standardul IEEE 802.1X este un protocol de autentificare și control al accesului bazat pe porturi. Acest protocol restricționează stațiile de lucru neautorizate să se conecteze la o rețea LAN prin porturi de comutare accesibile public. Serverul de autentificare autentifică fiecare stație de lucru care este conectată la un port de comutare înainte de a pune la dispoziție orice serviciu oferit de comutator sau de LAN.

Diagrama arată dispozitivele implicate în autentificarea bazată pe porturi 802.1x. În stânga se află solicitantul, în acest caz un desktop, care necesită acces și răspunde la solicitările de la un comutator. Solicitantul este conectat la autentificator, în acest caz un comutator, care controlează accesul fizic la rețea pe baza stării de autentificare a clientului. Autentificatorul este conectat la serverul de autentificare care realizează autentificarea clientului.

***Client (Solicitant)*** - Acesta este un dispozitiv care rulează software client compatibil 802.1X, care este disponibil pentru dispozitive cu fir sau fără fir.

***Switch (Authenticator)*** – Comutatorul acționează ca un intermediar între client și serverul de autentificare. Acesta solicită informații de identificare de la client, verifică aceste informații cu serverul de autentificare și transmite un răspuns către client. Un alt dispozitiv care ar putea acționa ca autentificator este un punct de acces wireless.

***Server de autentificare*** – Serverul validează identitatea clientului și notifică comutatorul sau punctul de acces fără fir că clientul este sau nu autorizat să acceseze LAN și serviciile de comutare.

Securitatea este la fel de puternică ca și cea mai slabă verigă din sistem, iar stratul 2 este considerat a fi acea verigă slabă. Acest lucru se datorează faptului că LAN-urile erau în mod tradițional sub controlul administrativ al unei singure organizații. Am avut încredere în mod inerent în toate persoanele și dispozitivele conectate la LAN-ul nostru. Astăzi, cu BYOD și atacuri mai sofisticate, rețelele LAN au devenit mai vulnerabile la penetrare. Prin urmare, pe lângă protejarea de la Layer 3 la Layer 7, profesioniștii în securitatea rețelei trebuie, de asemenea, să atenueze atacurile asupra infrastructurii LAN de Layer 2.

**Vulnerabilități de nivel 2**

Primul pas în atenuarea atacurilor asupra infrastructurii Layer 2 este înțelegerea funcționării de bază a Layer 2 și a amenințărilor reprezentate de Layer 2.

**Atacurile de strat 2**

|  |  |
| --- | --- |
| **Categorie** | **Exemple** |
| **Atacurile MAC Table** | Include atacuri de inundare a adresei MAC. |
| **Atacurile VLAN** | Include atacuri de salt VLAN și atacuri cu etichetare dublă VLAN. De asemenea, include atacuri între dispozitive pe un VLAN comun. |
| **Atacurile DHCP** | Include înfometarea DHCP și atacurile de falsificare DHCP. |
| **Atacurile ARP** | Include spoofing ARP și atacuri de otrăvire ARP. |
| **Abordați atacurile de falsificare** | Include atacuri de falsificare a adresei MAC și a adresei IP. |
| **Atacurile STP** | Include atacuri de manipulare Spanning Tree Protocol. |

**Nivelul 2 de atenuare a atacurilor**

|  |  |
| --- | --- |
| **Soluţie** | **Descriere** |
| **Securitatea Portului** | Previne multe tipuri de atacuri, inclusiv atacurile de inundare a adresei MAC și atacurile de foame DHCP. |
| **Snooping DHCP** | Previne înfometarea DHCP și atacurile de falsificare DHCP. |
| **Inspecție dinamică ARP (DAI)** | Previne falsificarea ARP și atacurile de otrăvire ARP. |
| **IP Source Guard (IPSG)** | Previne atacurile de falsificare a adreselor MAC și IP. |

Aceste soluții de nivel 2 nu vor fi eficiente dacă protocoalele de management nu sunt securizate. De exemplu, protocoalele de management Syslog, Simple Network Management Protocol (SNMP), Trivial File Transfer Protocol (TFTP), telnet, File Transfer Protocol (FTP) și majoritatea altor protocoale comune sunt nesigure; prin urmare, se recomandă următoarele strategii:

Utilizați întotdeauna variante securizate ale acestor protocoale, cum ar fi SSH, Secure Copy Protocol (SCP), Secure FTP (SFTP) și Secure Socket Layer/Transport Layer Security (SSL/TLS).

Luați în considerare utilizarea rețelei de gestionare în afara benzii pentru a gestiona dispozitivele.

Utilizați un VLAN de management dedicat în care nu există decât traficul de management.

Utilizați ACL-uri pentru a filtra accesul nedorit.

**Inundarea tabelului de adrese MAC**

Toate tabelele MAC au o dimensiune fixă ​​și, în consecință, un comutator poate rămâne fără resurse în care să stocheze adrese MAC. Atacurile de inundare a adreselor MAC profită de această limitare bombardând comutatorul cu adrese MAC sursă false până când tabelul de adrese MAC al comutatorului este plin.

Când se întâmplă acest lucru, comutatorul tratează cadrul ca un unicast necunoscut și începe să inunde tot traficul de intrare în toate porturile de pe același VLAN fără a face referire la tabelul MAC. Această condiție permite acum unui actor de amenințare să captureze toate cadrele trimise de la o gazdă la alta pe LAN local sau VLAN local.

Notă : Traficul este inundat numai în rețeaua locală LAN sau VLAN. Actorul amenințării poate capta numai traficul în LAN-ul local sau VLAN-ul la care este conectat actorul amenințării.

**Atenuarea atacurilor din tabelul de adrese MAC**

Ceea ce face ca instrumente precum macof să fie atât de periculoase este că un atacator poate crea un atac de depășire a tabelului MAC foarte rapid. De exemplu, un comutator Catalyst 6500 poate stoca 132.000 de adrese MAC în tabelul său de adrese MAC. Un instrument precum macof poate inunda un comutator cu până la 8.000 de cadre false pe secundă; crearea unui atac de depășire a tabelului de adrese MAC în câteva secunde. Exemplul arată un exemplu de ieșire a comenzii macof pe o gazdă Linux.

**# macof -i eth1**

**Atacurile VLAN Hopping**

Un atac de salt VLAN permite traficul de la un VLAN să fie văzut de un alt VLAN fără ajutorul unui router. Într-un atac de bază de salt VLAN, actorul amenințării configurează o gazdă să acționeze ca un comutator pentru a profita de funcția de port trunking automat activată în mod implicit pe majoritatea porturilor de comutare.

Actorul amenințării configurează gazda pentru a falsifica semnalizarea 802.1Q și semnalizarea DTP (Dynamic Trunking Protocol) proprietar Cisco către trunchiul cu comutatorul de conectare. Dacă reușește, comutatorul stabilește o legătură trunk cu gazda, așa cum se arată în figură. Acum, actorul amenințării poate accesa toate VLAN-urile de pe switch. Actorul amenințării poate trimite și primi trafic pe orice VLAN, saltând efectiv între VLAN-uri.

**Atac cu etichetare dublă VLAN**

Un actor de amenințare în situații specifice ar putea încorpora o etichetă 802.1Q ascunsă în interiorul cadrului care are deja o etichetă 802.1Q. Această etichetă permite cadrului să meargă la un VLAN pe care eticheta originală 802.1Q nu a specificat-o.

**Pasul 1.** Actorul amenințării trimite un cadru 802.1Q cu etichetă dublă către comutator. Antetul exterior are eticheta VLAN a actorului amenințării, care este aceeași cu VLAN-ul nativ al portului trunk. În scopul acestui exemplu, presupuneți că acesta este VLAN 10. Eticheta interioară este VLAN-ul victimă, în acest exemplu, VLAN 20.

**Pasul 2.** Cadrul ajunge pe primul comutator, care se uită la prima etichetă 802.1Q de 4 octeți. Comutatorul vede că cadrul este destinat pentru VLAN 10, care este VLAN-ul nativ. Comutatorul redirecționează pachetul către toate porturile VLAN 10 după ce a demontat eticheta VLAN 10. Cadrul nu este reetichetat deoarece face parte din VLAN-ul nativ. În acest moment, eticheta VLAN 20 este încă intactă și nu a fost inspectată de primul comutator.

**Pasul 3.** Cadrul ajunge la cel de-al doilea comutator care nu știe că ar fi trebuit să fie pentru VLAN 10. Traficul VLAN nativ nu este etichetat de comutatorul de trimitere, așa cum este specificat în specificația 802.1Q. Al doilea comutator se uită numai la eticheta interioară 802.1Q pe care a inserat-o actorul amenințării și vede că cadrul este destinat VLAN 20, VLAN-ul țintă. Al doilea comutator trimite cadrul către țintă sau îl inundă, în funcție de faptul dacă există o intrare în tabelul de adrese MAC pentru țintă.

Un atac cu etichetare dublă VLAN este unidirecțional și funcționează numai atunci când atacatorul este conectat la un port care rezidă în același VLAN ca și VLAN-ul nativ al portului trunk. Ideea este că etichetarea dublă permite atacatorului să trimită date către gazde sau servere de pe un VLAN care altfel ar fi blocat de un anumit tip de configurație de control al accesului. Probabil că va fi permis și traficul de întoarcere, oferind astfel atacatorului capacitatea de a comunica cu dispozitivele de pe VLAN-ul blocat în mod normal.

**Atenuarea atacurilor VLAN**

Atacurile de salt VLAN și de dubla etichetare VLAN pot fi prevenite prin implementarea următoarelor linii directoare de securitate a trunchiului, așa cum sa discutat într-un modul anterior:

•Dezactivați trunchiul pe toate porturile de acces.

•Dezactivați trunchiul automat pe legăturile trunchiului, astfel încât trunchiurile trebuie activate manual.

•Asigurați-vă că VLAN-ul nativ este utilizat numai pentru legăturile trunchiului.

**Mesaje DHCP -**Serverele DHCP oferă în mod dinamic clienților informații de configurare IP, inclusiv adresa IP, masca de subrețea, gateway implicit, servere DNS și multe altele.

**Atacurile DHCP** sunt DHCP starvation și DHCP spoofing. Ambele atacuri sunt atenuate prin implementarea DHCP Snooping.

**Atac de foame DHCP** Starvation este de a crea un DoS pentru conectarea clienților. Atacurile de foame DHCP necesită un instrument de atac precum Gobbler.

Gobbler are capacitatea de a analiza întregul domeniu al adreselor IP care pot fi închiriate și încearcă să le închirieze pe toate. Mai exact, creează mesaje de descoperire DHCP cu adrese MAC false.

**Atac de falsificare DHCP** are loc atunci când un server DHCP nepoliticos este conectat la rețea și oferă parametri de configurare IP falși clienților legitimi. Un server necinstiți poate furniza o varietate de informații înșelătoare:

•*Gateway implicit greșit -* Serverul necinstiți oferă un gateway nevalid sau adresa IP a gazdei sale pentru a crea un atac de tip man-in-the-middle. Acest lucru poate rămâne complet nedetectat, deoarece intrusul interceptează fluxul de date prin rețea.

*•Server DNS greșit* - Serverul necinstit furnizează o adresă incorectă a serverului DNS, indicând utilizatorul către un site web nefast.

*•Adresă IP greșită* - Serverul necinstit oferă o adresă IP invalidă, creând efectiv un atac DoS asupra clientului DHCP.

**Pasul 1** Actorul de amenințare conectează serverul DHCP necinstiți

Un actor de amenințare conectează cu succes un server DHCP nepoliticos la un port de comutare de pe aceeași subrețea și VLAN-uri ca și clienții țintă. Scopul serverului rogue este de a oferi clienților informații false de configurare IP.

**Pasul 2** Clientul transmite mesaje de descoperire DHCP

Un client legitim se conectează la rețea și necesită parametrii de configurare IP. Prin urmare, clientul difuzează o cerere de descoperire DHCP în căutarea unui răspuns de la un server DHCP. Ambele servere vor primi mesajul și vor răspunde

**Pasul 3** Răspuns DHCP legitim și nepoliticos

Serverul DHCP legitim răspunde cu parametrii de configurare IP validi. Cu toate acestea, serverul necinstiți răspunde și cu o ofertă DHCP care conține parametrii de configurare IP definiți de actorul amenințării. Clientul va raspunde la prima oferta primita.

**Pasul 4** Clientul acceptă oferta Rogue DHCP

Oferta necinstită a fost primită mai întâi și, prin urmare, clientul difuzează o solicitare DHCP acceptând parametrii IP definiți de actorul amenințării. Serverul legitim și necinstiți va primi cererea.

**Pasul 5** Rogue Server recunoaște

Serverul necinstit transmite un răspuns clientului pentru a confirma cererea acestuia. Serverul legitim va înceta comunicarea cu clientul.

**Atacurile ARP**

Gazdele difuzează solicitări ARP pentru a determina adresa MAC a unei gazde cu o anumită adresă IPv4. Acest lucru se face de obicei pentru a descoperi adresa MAC a gateway-ului implicit. Toate gazdele de pe subrețea primesc și procesează Solicitarea ARP. Gazda cu adresa IPv4 corespunzătoare în Solicitarea ARP trimite un Răspuns ARP.

Potrivit ARP RFC, unui client i se permite să trimită o solicitare ARP nesolicitată numită „ARP gratuit”. Când o gazdă trimite un ARP gratuit, alte gazde de pe subrețea stochează adresa MAC și adresa IPv4 conținute în ARP gratuit în tabelele lor ARP.

Problema este că un atacator poate trimite un mesaj ARP gratuit care conține o adresă MAC falsificată către un comutator, iar comutatorul își va actualiza tabelul MAC în consecință. Prin urmare, orice gazdă poate pretinde că este proprietarul oricărei combinații de adrese IP și MAC pe care o alege. Într-un atac tipic, un actor de amenințare poate trimite răspunsuri ARP nesolicitate către alte gazde de pe subrețea cu adresa MAC a actorului amenințării și adresa IPv4 a gateway-ului implicit.

Există multe instrumente disponibile pe internet pentru a crea atacuri ARP man-in-the-middle, inclusiv dsniff, Cain & Abel, ettercap, Yersinia și altele. IPv6 utilizează protocolul ICMPv6 Neighbor Discovery pentru rezoluția adreselor de nivel 2. IPv6 include strategii pentru a atenua falsificarea publicității învecinate, similar modului în care IPv6 previne un răspuns ARP falsificat.

Falsificarea ARP și otrăvirea ARP sunt atenuate prin implementarea DAI.

**Pasul 1.** Stare normală cu tabele MAC convergente

Fiecare dispozitiv are un tabel MAC precis cu adresele IPv4 și MAC corecte pentru celelalte dispozitive din LAN.

**Pasul 2.** Atac de falsificare ARP

Actorul amenințării trimite două răspunsuri ARP gratuite falsificate în încercarea de a înlocui R1 ca gateway implicit:

1.Primul informează toate dispozitivele din LAN că adresa MAC a actorului amenințării (CC:CC:CC) se mapează la adresa IPv4 a lui R1, 10.0.0.1.

2.Al doilea informează toate dispozitivele din LAN că adresa MAC a actorului amenințării (CC:CC:CC) se mapează la adresa IPv4 a PC1, 10.0.0.11.

**Pasul 3.** Atacul de otrăvire ARP cu atacul Man-in-the-Middle

R1 și PC1 elimină intrarea corectă pentru adresa MAC a celuilalt și o înlocuiesc cu adresa MAC a PC2. Actorul amenințării a otrăvit acum cache-urile ARP ale tuturor dispozitivelor de pe subrețea. Otrăvirea ARP duce la diferite atacuri de tip man-in-the-middle, reprezentând o amenințare serioasă de securitate pentru rețea.

**Adresează atacul de falsificare**

Adresele IP și adresele MAC pot fi falsificate din mai multe motive. Falsificarea adresei IP este atunci când un actor de amenințări deturnează o adresă IP validă a unui alt dispozitiv din subrețea sau folosește o adresă IP aleatorie. Falsificarea adresei IP este dificil de atenuat, mai ales atunci când este utilizată într-o subrețea din care aparține IP-ul.

Atacurile de falsificare a adresei MAC apar atunci când actorii amenințărilor modifică adresa MAC a gazdei lor pentru a se potrivi cu o altă adresă MAC cunoscută a unei gazde țintă. Gazda atacatoare trimite apoi un cadru în întreaga rețea cu adresa MAC nou configurată. Când comutatorul primește cadrul, examinează adresa MAC sursă. Comutatorul suprascrie intrarea curentă în tabelul MAC și atribuie adresa MAC noului port, așa cum se arată în figură. Apoi transmite din neatenție cadrele destinate gazdei țintă către gazda atacatoare.

Când gazda țintă trimite trafic, comutatorul va corecta eroarea, realinând adresa MAC la portul original. Pentru a opri comutatorul să readucă alocarea portului la starea sa corectă, actorul amenințării poate crea un program sau un script care va trimite în mod constant cadre către comutator, astfel încât comutatorul să mențină informațiile incorecte sau falsificate. Nu există niciun mecanism de securitate la nivelul 2 care să permită unui comutator să verifice sursa adreselor MAC, ceea ce îl face atât de vulnerabil la falsificare.

Falsificarea adreselor IP și MAC poate fi atenuată prin implementarea IPSG.

**Atacul STP**

Atacatorii de rețea pot manipula protocolul Spanning Tree (STP) pentru a efectua un atac prin falsificarea podului rădăcină și modificarea topologiei unei rețele. Atacatorii își pot face gazdele să apară ca punți rădăcină; și, prin urmare, capturați tot traficul pentru domeniul comutat imediat.

Pentru a efectua un atac de manipulare STP, gazda atacatoare transmite unități de date STP bridge protocol (BPDU) care conțin modificări de configurare și topologie care vor forța recalculările spanning-tree, așa cum se arată în figură. BPDU-urile trimise de gazda atacatoare anunță o prioritate mai mică a podului în încercarea de a fi aleasă ca punte rădăcină.

Notă : Aceste probleme pot apărea atunci când cineva adaugă un comutator Ethernet în rețea fără nicio intenție rău intenționată.

Dacă are succes, gazda atacatoare devine puntea rădăcină, așa cum se arată în figură, și acum poate captura o varietate de cadre care altfel nu ar fi accesibile.

Acest atac STP este atenuat prin implementarea BPDU Guard pe toate porturile de acces. BPDU Guard este discutat mai detaliat mai târziu în curs.

**Recunoaștere CDP**

Cisco Discovery Protocol (CDP) este un protocol proprietar de descoperire a legăturilor de nivel 2. Este activat în mod implicit pe toate dispozitivele Cisco. CDP poate descoperi automat alte dispozitive compatibile cu CDP și poate ajuta la configurarea automată a conexiunii acestora. Administratorii de rețea folosesc, de asemenea, CDP pentru a ajuta la configurarea și depanarea dispozitivelor de rețea.

Informațiile CDP sunt trimise în porturile compatibile CDP într-un multicast periodic, necriptat. Informațiile CDP includ adresa IP a dispozitivului, versiunea software-ului IOS, platforma, capabilitățile și VLAN-ul nativ. Dispozitivul care primește mesajul CDP își actualizează baza de date CDP.

Informațiile CDP sunt extrem de utile în depanarea rețelei. De exemplu, CDP poate fi utilizat pentru a verifica conectivitatea Layer 1 și 2. Dacă un administrator nu poate face ping la o interfață conectată direct, dar primește în continuare informații CDP, atunci problema este cel mai probabil legată de configurația Layer 3.

Cu toate acestea, informațiile furnizate de CDP pot fi folosite și de un actor de amenințare pentru a descoperi vulnerabilitățile infrastructurii de rețea.

În figură, un exemplu de captură Wireshark afișează conținutul unui pachet CDP. Atacatorul este capabil să identifice versiunea software Cisco IOS folosită de dispozitiv. Acest lucru permite atacatorului să determine dacă au existat vulnerabilități de securitate specifice acelei versiuni de IOS.

Emisiunile CDP sunt trimise necriptate și neautentificate. Prin urmare, un atacator ar putea interfera cu infrastructura rețelei trimițând cadre CDP concepute care conțin informații false despre dispozitiv către dispozitivele Cisco conectate direct.

Pentru a atenua exploatarea CDP, limitați utilizarea CDP pe dispozitive sau porturi. De exemplu, dezactivați CDP pe porturile de margine care se conectează la dispozitive care nu sunt de încredere.

Pentru a dezactiva global CDP pe un dispozitiv, utilizați comanda no cdp run global configuration mode. Pentru a activa CDP la nivel global, utilizați comanda cdp run global configuration.

Pentru a dezactiva CDP pe un port, utilizați comanda de configurare a interfeței no cdp enable . Pentru a activa CDP pe un port, utilizați comanda de configurare a interfeței cdp enable .

**Notă :** Protocolul Link Layer Discovery (LLDP) este, de asemenea, vulnerabil la atacurile de recunoaștere. Configurați nicio rulare lldp pentru a dezactiva LLDP la nivel global. Pentru a dezactiva LLDP pe interfață, configurați nicio transmisie lldp și nicio recepție lldp.

**Rezumat**

Punctele finale sunt deosebit de susceptibile la atacuri legate de malware care provin prin e-mail sau navigare pe web, cum ar fi DDOS, încălcări ale datei și programe malware. Aceste puncte finale au folosit de obicei caracteristici tradiționale de securitate bazate pe gazdă, cum ar fi antivirus/antimalware, firewall-uri bazate pe gazdă și sisteme de prevenire a intruziunilor (HIPS) bazate pe gazdă. Punctele finale sunt cel mai bine protejate printr-o combinație de NAC, software AMP bazat pe gazdă, un dispozitiv de securitate pentru e-mail (ESA) și un dispozitiv de securitate web (WSA). Cisco WSA poate efectua lista neagră de adrese URL, filtrare URL, scanare malware, categorizare URL, filtrare a aplicațiilor web și criptare și decriptare a traficului web.

**AAA** controlează cui are permisiunea de a accesa o rețea (autentificare), ce pot face în timp ce sunt acolo (autorizare) și să auditeze ce acțiuni au efectuat în timp ce accesează rețeaua (contabilitate). Autorizarea folosește un set de atribute care descriu accesul utilizatorului la rețea. Contabilitatea este combinată cu autentificarea AAA. Serverul AAA păstrează un jurnal detaliat cu exact ceea ce face utilizatorul autentificat pe dispozitiv. Standardul IEEE 802.1X este un protocol de autentificare și control al accesului bazat pe porturi care restricționează stațiile de lucru neautorizate să se conecteze la o rețea LAN prin porturi de comutare accesibile public.

Dacă Stratul 2 este compromis, atunci toate straturile de deasupra acestuia sunt și ele afectate. Primul pas în atenuarea atacurilor asupra infrastructurii Layer 2 este înțelegerea funcționării de bază a Layer 2 și a soluțiilor Layer 2: Port Security, DHCP Snooping, DAI și IPSG. Acestea nu vor funcționa decât dacă protocoalele de management sunt securizate.

Atacurile de inundare a adreselor MAC bombardează comutatorul cu adrese MAC sursă false până când tabelul de adrese MAC al comutatorului este plin. În acest moment, comutatorul tratează cadrul ca un unicast necunoscut și începe să inunde tot traficul de intrare în toate porturile de pe același VLAN fără a face referire la tabelul MAC. Actorul amenințării poate captura acum toate cadrele trimise de la o gazdă la alta pe LAN local sau VLAN local. Actorul amenințării folosește **macof** pentru a genera rapid multe surse aleatorii și destinații MAC și IP. Pentru a atenua atacurile de depășire a tabelelor MAC, administratorii de rețea trebuie să implementeze securitatea porturilor.

Un atac de salt VLAN permite traficul de la un VLAN să fie văzut de un alt VLAN fără ajutorul unui router. Actorul amenințării configurează o gazdă să acționeze ca un comutator pentru a profita de funcția de port trunking automat activată în mod implicit pe majoritatea porturilor de comutare.

Un atac cu etichetare dublă VLAN este unidirecțional și funcționează numai atunci când actorul amenințării este conectat la un port care locuiește în același VLAN ca și VLAN-ul nativ al portului trunk. Etichetarea dublă permite actorului amenințării să trimită date către gazde sau servere pe un VLAN care altfel ar fi blocat de un anumit tip de configurație de control al accesului. Traficul de întoarcere va fi, de asemenea, permis, permițând actorului amenințării să comunice cu dispozitivele de pe VLAN-ul blocat în mod normal.

Atacurile de salt VLAN și de dubla etichetare VLAN pot fi prevenite prin implementarea următoarelor reguli de securitate a trunchiului:

-Dezactivați trunchiul pe toate porturile de acces.

-Dezactivați trunchiul automat pe legăturile trunchiului, astfel încât trunchiurile trebuie activate manual.

-Asigurați-vă că VLAN-ul nativ este utilizat numai pentru legăturile trunchiului.

Atacul DHCP: serverele DHCP oferă în mod dinamic clienților informații despre configurația IP, inclusiv adresa IP, masca de subrețea, gateway implicit, servere DNS și multe altele. Două tipuri de atacuri DHCP sunt DHCP starvation și DHCP spoofing. Ambele atacuri sunt atenuate prin implementarea DHCP Snooping.

**Atacul ARP:** un actor de amenințare trimite un mesaj ARP gratuit care conține o adresă MAC falsificată către un comutator, iar comutatorul își actualizează tabelul MAC în consecință. Acum, actorul amenințării trimite solicitări ARP nesolicitate către alte gazde de pe subrețea cu adresa MAC a actorului amenințării și adresa IP a gateway-ului implicit. Falsificarea ARP și otrăvirea ARP sunt atenuate prin implementarea DAI.

Atacul de falsificare a adresei: falsificarea adresei IP este atunci când un actor de amenințare deturnează o adresă IP validă a altui dispozitiv din subrețea sau folosește o adresă IP aleatorie. Atacurile de falsificare a adresei MAC apar atunci când actorii amenințărilor modifică adresa MAC a gazdei lor pentru a se potrivi cu o altă adresă MAC cunoscută a unei gazde țintă. Falsificarea adreselor IP și MAC poate fi atenuată prin implementarea IPSG.

**Atacul STP:** actorii amenințări manipulează STP pentru a efectua un atac prin falsificarea podului rădăcină și schimbând topologia unei rețele. Actorii amenințărilor își fac gazdele să apară ca punți rădăcină; prin urmare, captarea întregului trafic pentru domeniul comutat imediat. Acest atac STP este atenuat prin implementarea BPDU Guard pe toate porturile de acces

**Recunoaștere CDP:** informațiile CDP sunt trimise în porturile compatibile CDP într-un multicast periodic, necriptat. Informațiile CDP includ adresa IP a dispozitivului, versiunea software-ului IOS, platforma, capabilitățile și VLAN-ul nativ. Dispozitivul care primește mesajul CDP își actualizează baza de date CDP. informațiile furnizate de CDP pot fi folosite și de un actor de amenințare pentru a descoperi vulnerabilitățile infrastructurii de rețea. Pentru a atenua exploatarea CDP, limitați utilizarea CDP pe dispozitive sau porturi.

**Switch Security Configuration**

**Securizare porturi neutilizate**

Dispozitivele de nivel 2 sunt considerate a fi cea mai slabă verigă din infrastructura de securitate a unei companii. Atacurile de nivel 2 sunt unele dintre cele mai ușor de implementat de către hackeri, dar aceste amenințări pot fi, de asemenea, atenuate cu unele soluții comune de nivel 2.

Toate porturile (interfețele) switch-ului trebuie securizate înainte ca comutatorul să fie implementat pentru utilizare în producție. Modul în care este securizat un port depinde de funcția acestuia.

O metodă simplă pe care o folosesc mulți administratori pentru a ajuta la securizarea rețelei împotriva accesului neautorizat este de a dezactiva toate porturile neutilizate de pe un comutator. De exemplu, dacă un switch Catalyst 2960 are 24 de porturi și există trei conexiuni Fast Ethernet în uz, este o practică bună să dezactivați cele 21 de porturi neutilizate. Navigați la fiecare port neutilizat și lansați comanda de închidere Cisco IOS . Dacă un port trebuie reactivat mai târziu, acesta poate fi activat cu comanda no shutdown .

Pentru a configura o serie de porturi, utilizați comanda interfață interval .

**Switch(config)# interface range type module/first-number – last-number**

De exemplu, pentru a închide porturile pentru Fa0/8 prin Fa0/24 pe S1, ar trebui să introduceți următoarea comandă.

S1(config)# interface range fa0/8 - 24

S1(config-if-range)# shutdown

**Activați Port Security**

Observați în exemplu, comanda switchport port-security a fost respinsă. Acest lucru se datorează faptului că securitatea porturilor poate fi configurată numai pe porturi de acces configurate manual sau porturi trunchi configurate manual. În mod implicit, porturile de comutare Layer 2 sunt setate la automat dinamic (trunking activat). Prin urmare, în exemplu, portul este configurat cu comanda de configurare a interfeței de acces în modul switchport .

**Notă :** Securitatea porturilor trunchi depășește scopul acestui curs.

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

**S1(config-if)# switchport port-security**

**Command rejected: FastEthernet0/1 is a dynamic port.**

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

**S1(config-if)# switchport port-security**

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

**S1#**

Utilizați comanda show port-security interface pentru a afișa setările curente de securitate a portului pentru FastEthernet 0/1, așa cum se arată în exemplu. Observați cum este activată securitatea portului, starea portului este Securizat, ceea ce înseamnă că nu există dispozitive atașate și nu a avut loc nicio încălcare, modul de încălcare este Închidere și cum numărul maxim de adrese MAC este 1. Dacă un dispozitiv este conectat la port, starea portului comutatorului va afișa Secure-up și comutatorul va adăuga automat adresa MAC a dispozitivului ca MAC securizat. În acest exemplu, niciun dispozitiv nu este conectat la port.

**S1# show port-security interface f0/1**

**Port Security : Enabled**

**Port Status : Secure-down**

**Violation Mode : Shutdown**

**Aging Time : 0 mins**

**Aging Type : Absolute**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 1**

**Total MAC Addresses : 0**

**Configured MAC Addresses : 0**

**Sticky MAC Addresses : 0**

**Last Source Address:Vlan : 0000.0000.0000:0**

**Security Violation Count : 0**

**S1#**

**Notă : Da**că un port activ este configurat cu comanda switchport port-security și mai mult de un dispozitiv este conectat la acel port, portul va trece la starea dezactivată de eroare. Această condiție este discutată mai târziu în acest subiect.

După ce securitatea portului este activată, pot fi configurate alte specificații de securitate a portului, așa cum se arată în exemplu.

**S1(config-if)# switchport port-security ?**

**aging Port-security aging commands**

**mac-address Secure mac address**

**maximum Max secure addresses**

**violation Security violation mode**

**S1(config-if)# switchport port-security**

**Limitați și aflați adresele MAC**

Pentru a seta numărul maxim de adrese MAC permise pe un port, utilizați următoarea comandă:

**Switch(config-if)# switchport port-security valoarea maximă**

Valoarea implicită de securitate a portului este 1. Numărul maxim de adrese MAC sigure care pot fi configurate depinde de comutator și de IOS. În acest exemplu, maximul este 8192.

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

**S1(config-if)# switchport port-security maximum ?**

**<1-8192> Maximum addresses**

**S1(config-if)# switchport port-security maximum**

Comutatorul poate fi configurat pentru a afla despre adresele MAC pe un port securizat într-unul din trei moduri:

**1 . Configurat manual**

Administratorul configurează manual o adresă(e) MAC statică(e) utilizând următoarea comandă pentru fiecare adresă MAC sigură de pe port:

**Switch(config-if)# switchport port-security mac-address sticky**

**2 . Învățat dinamic**

Când este introdusă comanda **switchport port-security** , sursa MAC curentă pentru dispozitivul conectat la port este securizată automat, dar nu este adăugată la configurația de pornire. Dacă comutatorul este repornit, portul va trebui să învețe din nou adresa MAC a dispozitivului.

**3 . Învățat dinamic – Lipicios**

Administratorul poate activa comutatorul să învețe în mod dinamic adresa MAC și să le „lipească” de configurația care rulează utilizând următoarea comandă:

**Switch(config-if)# switchport port-security adresa mac sticky**

Salvarea configurației de rulare va trimite adresa MAC învățată dinamic la NVRAM.

Următorul exemplu demonstrează o configurație completă de securitate a porturilor pentru FastEthernet 0/1 cu o gazdă conectată la portul Fa0/1. Administratorul specifică maximum 2 adrese MAC, configurează manual o adresă MAC securizată și apoi configurează portul pentru a afla în mod dinamic adrese MAC sigure suplimentare până la maximum 2 adrese MAC securizate. Utilizați **interfața show port-security** și comanda **show port-security address** pentru a verifica configurația.

**\*Mar 1 00:12:38.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up**

**\*Mar 1 00:12:39.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up**

**S1#conf t**

**Enter configuration commands, one per line. End with CNTL/Z.**

**S1(config)#**

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

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

**S1(config-if)# switchport port-security**

**S1(config-if)# switchport port-security maximum 2**

**S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234**

**S1(config-if)# switchport port-security mac-address sticky**

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

**S1# show port-security interface fa0/1**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Shutdown**

**Aging Time : 0 mins**

**Aging Type : Absolute**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7272.676a:1**

**Security Violation Count : 0**

**S1# show port-security address**

**Secure Mac Address Table**

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

**Vlan Mac Address Type Ports Remaining Age**

**(mins)**

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

**1 a41f.7272.676a SecureSticky Fa0/1 -**

**1 aaaa.bbbb.1234 SecureConfigured Fa0/1 -**

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

**Total Addresses in System (excluding one mac per port) : 1**

**Max Addresses limit in System (excluding one mac per port) : 8192**

**S1#**

Ieșirea comenzii **show port-security interface** verifică dacă securitatea portului este activată, există o gazdă conectată la port (adică Secure-up), vor fi permise un total de 2 adrese MAC și S1 a învățat o adresă MAC static și o adresă MAC dinamic (adică, sticky).

Ieșirea comenzii **show port-security address** listează cele două adrese MAC învățate.

**Îmbătrânirea securității portuare**

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 pentru fiecare port:

* **Absolut** - Adresele securizate de pe port sunt șterse după perioada de vechime specificată.
* **Inactivitate** - Adresele securizate de pe port sunt șterse numai dacă sunt inactive pentru perioada de vechime specificată.

Utilizați vechimea pentru a elimina adresele MAC securizate de pe un port securizat fără a șterge manual adresele MAC securizate existente. Limitele de timp învechite pot fi, de asemenea, mărite pentru a se asigura că adresele MAC securizate din trecut rămân, chiar dacă sunt adăugate noi adrese MAC. Îmbătrânirea adreselor securizate configurate static poate fi activată sau dezactivată în funcție de port.

Utilizați comanda **switchport port-security aging** pentru a activa sau dezactiva îmbătrânirea statică pentru portul securizat sau pentru a seta timpul sau tipul de îmbătrânire.

**Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}**

Parametrii pentru comandă sunt descriși în tabel.

|  |  |
| --- | --- |
| **Parametru** | **Descriere** |
| **static** | Activați vechimea pentru adresele securizate configurate static pe acest port. |
| **time time** | Specificați timpul de îmbătrânire pentru acest port. Intervalul este de la 0 la 1440 de minute. Dacă timpul este 0, vechimea este dezactivată pentru acest port. |
| **type absolute** | Setați timpul absolut de îmbătrânire. Toate adresele securizate de pe acest port expiră exact după timpul (în minute) specificat și sunt eliminate din lista de adrese securizate. |
| **type inactivity** | Setați tipul de îmbătrânire inactivitate. Adresele securizate de pe acest port expiră numai dacă nu există trafic de date de la adresa sursă securizată pentru perioada de timp specificată. |

**Notă** : adresele MAC sunt afișate ca 24 de biți pentru simplitate.

Exemplul arată un administrator care configurează tipul de vechime la 10 minute de inactivitate și utilizând comanda **show port-security interface** pentru a verifica configurația.

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

**S1(config-if)# switchport port-security aging time 10**

**S1(config-if)# switchport port-security aging type inactivity**

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

**S1# show port-security interface fa0/1**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Shutdown**

**Aging Time : 10 mins**

**Aging Type : Inactivity**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7272.676a:1**

**Security Violation Count : 0**

**S1#**

**Moduri de încălcare a securității porturilor**

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.

Pentru a seta modul de încălcare a securității porturilor, utilizați următoarea comandă:

**Switch(config-if)# switchport port-security violation { protect | restrânge | oprire }**

Următoarele tabele arată cum reacţionează un comutator pe baza modului de încălcare configurat.

Descrieri ale modului de încălcare a securității

|  |  |
| --- | --- |
| **Modul** | **Descriere** |
| **shutdown**  **(default)** | Portul trece imediat la starea dezactivată de eroare, stinge LED-ul portului și trimite un mesaj syslog. Crește contorul de încălcări. Când un port securizat se află în starea dezactivată de eroare, un administrator trebuie să-l reactiveze introducând comenzile de **închidere** și **fără închidere .** |
| **restrict** | Portul elimină pachetele cu adrese sursă necunoscute până când eliminați un număr suficient de adrese MAC securizate pentru a scădea sub valoarea maximă sau pentru a crește valoarea maximă. Acest mod face ca contorul de încălcări de securitate să crească și generează un mesaj syslog. |
| **protect** | Acesta este cel mai puțin sigur dintre modurile de încălcare a securității. Portul elimină pachete cu adrese MAC necunoscute până când eliminați un număr suficient de adrese MAC securizate pentru a scădea sub valoarea maximă sau pentru a crește valoarea maximă. Nu este trimis niciun mesaj syslog. |

**Comparația modului de încălcare a securității**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Modul de încălcare** | **Renunță la traficul ofensator** | **Trimite un mesaj Syslog** | **Măriți contorul de încălcări** | **Închide portul** |
| Protect | da | Nu | Nu | Nu |
| R**estrict** | da | da | da | Nu |
| **SHutdown** | da | da | da | da |

Următorul exemplu arată un administrator care modifică încălcarea securității în „restricționare”. Ieșirea comenzii **show port-security interface** confirmă că modificarea a fost făcută.

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

**S1(config-if)# switchport port-security violation restrict**

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

**S1#**

**S1# show port-security interface f0/1**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Restrict**

**Aging Time : 10 mins**

**Aging Type : Inactivity**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7272.676a:1**

**Security Violation Count : 0**

**S1#**

**Porturi în stare dezactivată de eroare**

Ce se întâmplă când încălcarea securității portului este oprită și are loc o încălcare a portului? Portul este oprit fizic și plasat în starea dezactivată de eroare și nu este trimis sau primit niciun trafic pe acel port.

În figură, încălcarea securității portului este schimbată înapoi la setarea implicită de oprire. Apoi gazda cu adresa MAC a41f.7272.676a este deconectată și o nouă gazdă este conectată la Fa0/1.

Observați cum sunt generate pe consolă o serie de mesaje legate de securitatea porturilor.

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

**S1(config-if)# switchport port-security violation shutdown**

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

**S1#**

**\*Mar 1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down**

**\*Mar 1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down**

**\*Mar 1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up**

**\*Mar 1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up**

**S1#**

**\*Mar 1 00:24:32.829: %PM-4-ERR\_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state**

**\*Mar 1 00:24:32.838: %PORT\_SECURITY-2-PSECURE\_VIOLATION: Security violation occurred, caused by MAC address a41f.7273.018c on port FastEthernet0/1.**

**\*Mar 1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down**

**\*Mar 1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down**

**S1#**

**Notă** : Protocolul portului și starea conexiunii sunt schimbate în jos și LED-ul portului este stins.

În exemplu, comanda **show interface** identifică starea portului ca fiind **err-disabled** . Ieșirea comenzii **show port-security** interface arată acum starea portului ca Secure-shutdown în loc de Secure-up. Contorul de încălcări de securitate crește cu 1.

**S1# show interface fa0/1 | include down**

**FastEthernet0/18 is down, line protocol is down (err-disabled)**

**(output omitted)**

**S1# show port-security interface fa0/1**

**Port Security : Enabled**

**Port Status : Secure-shutdown**

**Violation Mode : Shutdown**

**Aging Time : 10 mins**

**Aging Type : Inactivity**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7273.018c:1**

**Security Violation Count : 1**

**S1#**

Administratorul ar trebui să determine ce a cauzat încălcarea securității Dacă un dispozitiv neautorizat este conectat la un port securizat, amenințarea de securitate este eliminată înainte de a reactiva portul.

În exemplul următor, prima gazdă este reconectată la Fa0/1. Pentru a reactiva portul, utilizați mai întâi comanda **shutdown** , apoi folosiți comanda **no shutdown** pentru a face portul operațional, așa cum se arată în exemplu.

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

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

**S1(config-if)#**

**\*Mar 1 00:39:54.981: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down**

**S1(config-if)# no shutdown**

**S1(config-if)#**

**\*Mar 1 00:40:04.275: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up**

**\*Mar 1 00:40:05.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up**

**S1(config-if)#**

**Verificați securitatea portului**

După configurarea securității portului pe un comutator, verificați fiecare interfață pentru a verifica dacă securitatea portului este setată corect și verificați pentru a vă asigura că adresele MAC statice au fost configurate corect.

**Securitatea porturilor pentru toate interfețele**

Pentru a afișa setările de securitate a porturilor pentru comutator, utilizați comanda **show port-security** . Exemplul indică faptul că un singur port este configurat cu comanda switchport port-security.

**S1# show port-security**

**Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action**

**(Count) (Count) (Count)**

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

**Fa0/1 2 2 0 Shutdown**

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

**Total Addresses in System (excluding one mac per port) : 1**

**Max Addresses limit in System (excluding one mac per port) : 8192**

**S1#**

**Securitate port pentru o interfață specifică**

Utilizați comanda **show port-security interface** pentru a vizualiza detaliile pentru o anumită interfață, așa cum se arată anterior și în acest exemplu.

**S1# show port-security interface fastethernet 0/1**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Shutdown**

**Aging Time : 10 mins**

**Aging Type : Inactivity**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 2**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : a41f.7273.018c:1**

**Security Violation Count : 0**

**S1#**

**Verificați adresele MAC învățate**

Pentru a verifica dacă adresele MAC „se lipesc” de configurație, utilizați comanda **show run** așa cum se arată în exemplul pentru FastEthernet 0/19.

**S1# show run interface fa0/1**

**Building configuration...**

**Current configuration : 365 bytes**

**!**

**interface FastEthernet0/1**

**switchport mode access**

**switchport port-security maximum 2**

**switchport port-security mac-address sticky**

**switchport port-security mac-address sticky a41f.7272.676a**

**switchport port-security mac-address aaaa.bbbb.1234**

**switchport port-security aging time 10**

**switchport port-security aging type inactivity**

**switchport port-security**

**end**

**S1#**

**Verificați adresele MAC securizate**

Pentru a afișa toate adresele MAC securizate care sunt configurate manual sau învățate dinamic pe toate interfețele switch-ului, utilizați comanda **show port-security address** , așa cum se arată în exemplu.

**S1# show port-security address**

**Secure Mac Address Table**

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

**Vlan Mac Address Type Ports Remaining Age**

**(mins)**

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

**1 a41f.7272.676a SecureSticky Fa0/1 -**

**1 aaaa.bbbb.1234 SecureConfigured Fa0/1 -**

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

**Total Addresses in System (excluding one mac per port) : 1**

**Max Addresses limit in System (excluding one mac per port) : 8192**

S1#

**Syntax Checker - Implement Port Security**

Implement port security for a switch interface based on the specified requirements

You are currently logged into S1. Configure FastEthernet 0/5 for port security by using the following requirements:

**Use the interface name fa0/5 to enter interface configuration mode.**

**Enable the port for access mode.**

**Enable port security.**

**Set the maximum number of MAC address to 3.**

**Statically configure the MAC address aaaa.bbbb.1234.**

**Configure the port to dynamically learn additional MAC addresses and dynamically add them to the running configuration.**

**Return to privileged EXEC mode.**

**S1(config)#interface fa0/5**

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

**S1(config-if)#switchport port-security**

**S1(config-if)#switchport port-security maximum 3**

**S1(config-if)#switchport port-security mac-address aaaa.bbbb.1234**

**S1(config-if)#switchport port-security mac-address sticky**

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

**Enter the command to verify port security for all interfaces.**

**S1#show port-security**

**Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action**

**(Count) (Count) (Count)**

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

**Fa0/5 3 2 0 Shutdown**

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

**Total Addresses in System (excluding one mac per port) : 0**

**Max Addresses limit in System (excluding one mac per port) : 8192**

**Enter the command to verify port security on FastEthernet 0/5. Use fa0/5 for the interface name.**

**S1#show port-security interface fa0/5**

**Port Security : Enabled**

**Port Status : Secure-up**

**Violation Mode : Shutdown**

**Aging Time : 0 mins**

**Aging Type : Absolute**

**SecureStatic Address Aging : Disabled**

**Maximum MAC Addresses : 3**

**Total MAC Addresses : 2**

**Configured MAC Addresses : 1**

**Sticky MAC Addresses : 1**

**Last Source Address:Vlan : 0090.2135.6B8C:1**

**Security Violation Count : 0**

**Enter the command that will display all of the addresses to verify that the manually configured and dynamically learned MAC addresses are in the running configuration.**

**S1#show port-security address**

**Secure Mac Address Table**

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

**Vlan Mac Address Type Ports Remaining Age**

**(mins)**

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

**1 0090.2135.6b8c SecureSticky Fa0/5 -**

**1 aaaa.bbbb.1234 SecureConfigured Fa0/5 -**

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

**Total Addresses in System (excluding one mac per port) : 0**

**Max Addresses limit in System (excluding one mac per port) : 8192**

**You have successfully configured and verified po**

**Reduceți atacurile VLAN**

**Analiza atacurilor VLAN**

Ca o scurtă trecere în revistă **,** un atac de salt VLAN poate fi lansat în unul din trei moduri:

* Falsificarea mesajelor DTP de la gazda atacatoare pentru ca comutatorul să intre în modul trunking. De aici, atacatorul poate trimite trafic etichetat cu VLAN-ul țintă, iar comutatorul livrează apoi pachetele la destinație.
* Introducerea unui comutator necinstiți și activarea trunchiului. Atacatorul poate accesa apoi toate VLAN-urile de pe comutatorul victimă de la comutatorul necinstiți.
* Un alt tip de atac de salt VLAN este un atac cu etichetare dublă (sau dublu încapsulat). Acest atac profită de modul în care funcționează hardware-ul pe majoritatea switch-urilor.

**Pași pentru a atenua atacurile VLAN Hopping**

Utilizați următorii pași pentru a atenua atacurile de salt VLAN:

**Pasul 1** : Dezactivați negocierile DTP (trunking automat) pe porturile non-trunking utilizând comanda de configurare a interfeței de **switchport mode access.**

**Pasul 2** : Dezactivați porturile neutilizate și puneți-le într-un VLAN neutilizat.

**Pasul 3** : Activați manual legătura trunk pe un port trunk utilizând comanda **switchport trunk mode** .

**Pasul 4** : Dezactivați negocierile DTP (trunking automat) pe porturile de trunking utilizând comanda **switchport nonegotiate** .

**Pasul 5** : Setați VLAN-ul nativ la un alt VLAN decât VLAN 1 utilizând comanda **switchport trunk native vlan***vlan \_ number* .

De exemplu, presupuneți următoarele:

* Porturile FastEthernet de la 0/1 la fa0/16 sunt porturi de acces active
* Porturile FastEthernet de la 0/17 la 0/20 nu sunt utilizate în prezent
* Porturile FastEthernet de la 0/21 la 0/24 sunt porturi trunk.

Hoppingul VLAN poate fi atenuat prin implementarea următoarei configurații.

**S1(config)# interface range fa0/1 - 16**

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

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

**S1(config)#**

**S1(config)# interface range fa0/17 - 20**

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

**S1(config-if-range)# switchport access vlan 1000**

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

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

**S1(config)#**

**S1(config)# interface range fa0/21 - 24**

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

**S1(config-if-range)# switchport nonegotiate**

**S1(config-if-range)# switchport trunk native vlan 999**

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

**S1#**

* Porturile FastEthernet de la 0/1 la 0/16 sunt porturi de acces și, prin urmare, trunchiul este dezactivat făcându-le în mod explicit porturi de acces.
* Porturile FastEthernet de la 0/17 la 0/20 sunt porturi neutilizate și sunt dezactivate și atribuite unui VLAN neutilizat.
* Porturile FastEthernet de la 0/21 la 0/24 sunt legături trunchiuri și sunt activate manual ca trunchiuri cu DTP dezactivat. VLAN-ul nativ este, de asemenea, schimbat de la VLAN-ul implicit 1 la un VLAN 999 neutilizat.

**Syntax Checker - Atenuarea atacurilor VLAN Hopping**

**You are currently logged into S1. The ports status of the ports are as follows:**

**FastEthernet ports 0/1 through 0/4 are used for trunking with other switches.**

**FastEthernet ports 0/5 through 0/10 are unused.**

**FastEthernet ports 0/11 through 0/24 are active ports currently in use.**

**Use range fa0/1 - 4 to enter interface configuration mode for the trunks.**

**S1(config)#interface range fa0/1 - 4**

**Configure the interfaces as nonnegotiating trunks assigned to default VLAN 99.**

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

**S1(config-if-range)#switchport nonegotiate**

**S1(config-if-range)#switchport trunk native vlan 99**

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

**Use range fa0/5 - 10 to enter interface configuration mode for the unused ports.**

**S1(config)#interface range fa0/5 - 10**

**Configure the unused ports as access ports, assign them to VLAN 86, and shutdown the ports.**

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

**S1(config-if-range)#switchport access vlan 86**

**% Access VLAN does not exist. Creating vlan 86**

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

**\*Mar 1 00:28:48.883: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down**

**\*Mar 1 00:28:48.900: %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down**

**\*Mar 1 00:28:48.908: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down**

**\*Mar 1 00:28:48.917: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down**

**\*Mar 1 00:28:48.942: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down**

**\*Mar 1 00:28:48.950: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down**

**\*Mar 1 00:28:49.890: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down**

**\*Mar 1 00:28:49.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down**

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

**Use range fa0/11 - 24 to enter interface configuration mode for the active ports and then configure them to prevent trunking.**

**S1(config)#interface range fa0/11 - 24**

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

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

**S1#**

**You have successfully mitigated VLAN hopping attacks on this switch.**

**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.

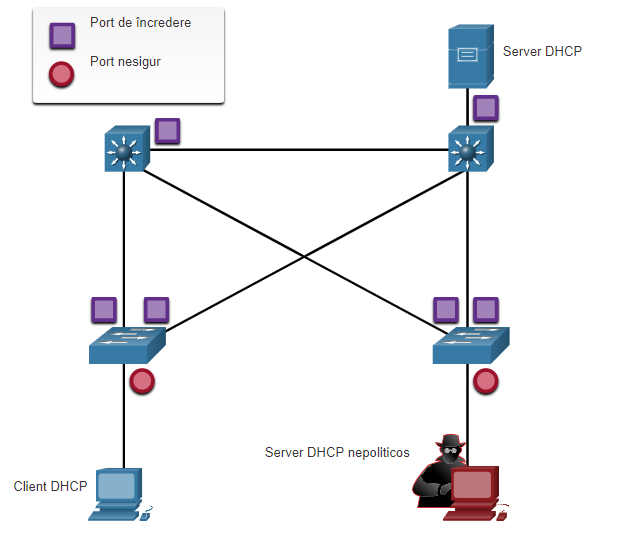
**Snooping DHCP**

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 .**

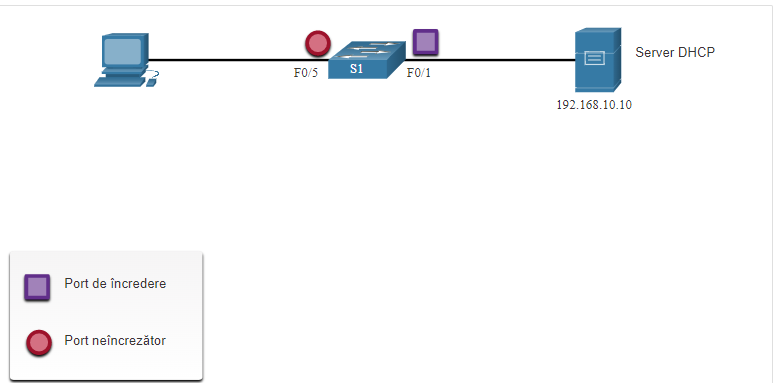
**Pasul 2** . Pe porturile de încredere, utilizați comanda de configurare a interfeței **ip dhcp snooping trust .**

**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**

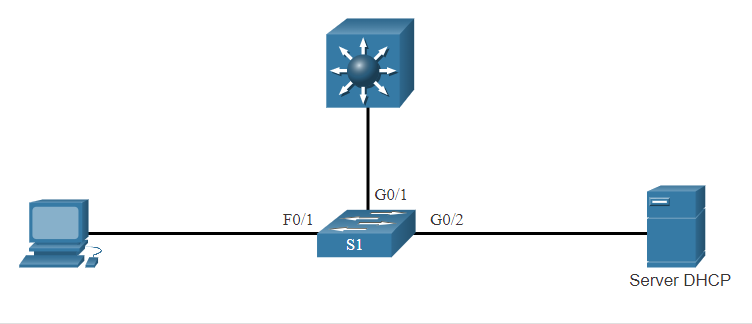
**MacAddress IpAddress Lease(sec) Type VLAN Interface**

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

**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.**

**Reduceți atacurile ARP**

**Inspecție ARP dinamică**

Într-un atac ARP tipic, un actor de amenințare poate trimite cereri ARP nesolicitate către alte gazde de pe subrețea cu adresa MAC a actorului amenințării și adresa IP a gateway-ului implicit. Pentru a preveni falsificarea ARP și otrăvirea ARP rezultată, un comutator trebuie să se asigure că sunt transmise numai solicitările și răspunsurile ARP valide.

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

* Nu transmiterea solicitărilor 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.
* Eliminarea și înregistrarea solicitărilor ARP care provin din surse nevalide pentru a preveni otrăvirea ARP.
* Eroare la dezactivarea interfeței dacă numărul DAI configurat de pachete ARP este depășit.

**Ghid de implementare DAI**

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.

În general, este recomandabil să configurați toate porturile comutatoarelor de acces ca nede încredere și să configurați toate porturile de legătură în sus care sunt conectate la alte comutatoare ca fiind de încredere.

Exemplul de topologie din figură identifică porturile de încredere și cele nede încredere.

Graficul arată o legendă cu un pătrat violet Trusted Port și un cerc roșu Untrusted Port, deasupra ei este o diagramă LAN care arată Dynamic ARP Inspection Trust. Diagrama ilustrează o rețea LAN cu porturi de încredere și nede încredere. Pe o interfață din stânga jos este un atacator pe un PC, iar în stânga sus este un P C obișnuit. Ambele dispozitive sunt conectate la comutator și ambele au un cerc roșu pe portul comutatorului pentru un port neîncrezat. În dreapta comutatorului se află un router care este, de asemenea, conectat la comutator. Conexiunea la router are un pătrat violet pe comutator care simbolizează o conexiune de încredere pentru ARP.

PC-AS1R1F0/1F0/2F0/24

Port neîncrezătorPort de încredereVLAN 10

**Exemplu de configurare DAI**

În topologia anterioară, S1 conectează doi utilizatori pe VLAN 10. DAI va fi configurat pentru a atenua atacurile ARP spoofing și ARP otravire.

După cum se arată în exemplu, DHCP snooping este activat deoarece DAI necesită ca tabelul de legare DHCP snooping să funcționeze. Apoi, DHCP Snooping și inspecția ARP sunt activate pentru computerele de pe VLAN10. Portul uplink către router este de încredere și, prin urmare, este configurat ca de încredere pentru DHCP snooping și inspecția ARP.

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

**S1(config)# ip dhcp snooping vlan 10**

**S1(config)# ip arp inspection vlan 10**

**S1(config)# interface fa0/24**

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

**S1(config-if)# ip arp inspection trust**

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.

Comanda de configurare globală **ip arp validate { [ src-mac ] [ dst-mac ] [ ip ] }** este utilizată pentru a configura DAI să arunce pachetele ARP atunci când adresele IP sunt invalide. Poate fi folosit atunci când adresele MAC din corpul pachetelor ARP nu se potrivesc cu adresele specificate în antetul Ethernet. Observați în exemplul următor cum poate fi configurată o singură comandă. Prin urmare, introducerea mai multor comenzi **ip arp inspection validate** suprascrie comanda anterioară. Pentru a include mai multe metode de validare, introduceți-le pe aceeași linie de comandă așa cum este prezentată și verificată în rezultatul următor.

**S1(config)# ip arp inspection validate ?**

**dst-mac Validate destination MAC address**

**ip Validate IP addresses**

**src-mac Validate source MAC address**

**S1(config)# ip arp inspection validate src-mac**

**S1(config)# ip arp inspection validate dst-mac**

**S1(config)# ip arp inspection validate ip**

**S1(config)# do show run | include validate**

**ip arp inspection validate ip**

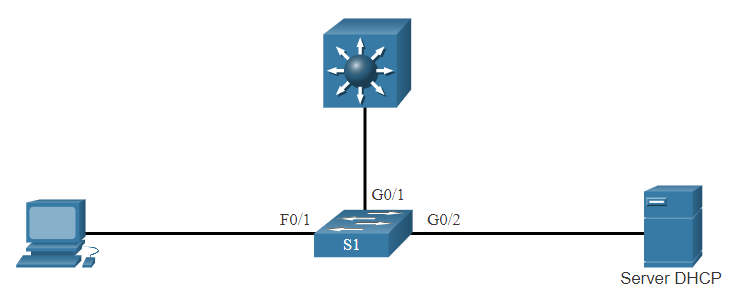
**S1(config)# ip arp inspection validate src-mac dst-mac ip**

**S1(config)# do show run | include validate**

**ip arp inspection validate src-mac dst-mac ip**

**S1(config)#**

**Syntax Checker - Atenuează atacurile ARP**

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

**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 for both DHCP snooping and DAI, and then return to global configuration mode.**

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

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

**S1(config-if-range)#ip arp inspection trust**

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

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

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

**S1(config)#ip arp inspection vlan 10,20,30-49**

**S1(config)#**

**You have successfully configured DAI for the switch.**

**Reduceți atacurile STP**

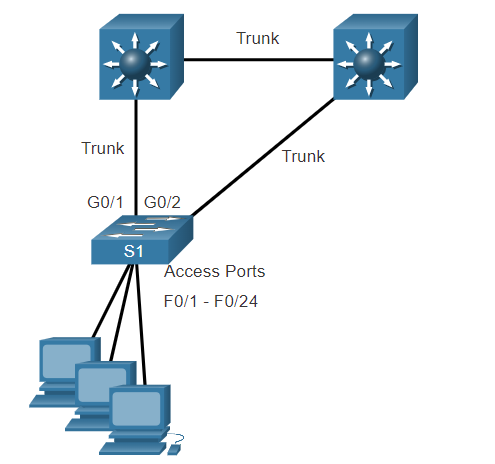
**PortFast și BPDU Guard**

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**

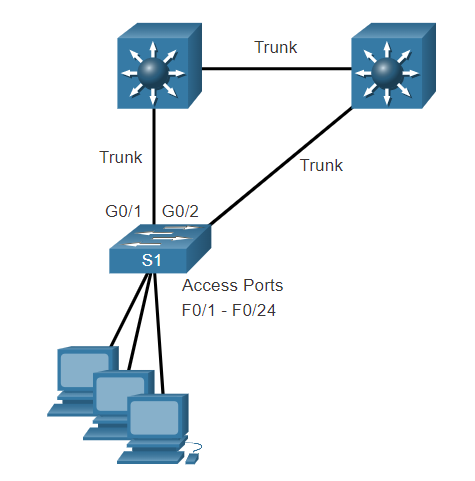
**(output omitted)**

**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.**

**Rezumat**

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.**