**Atacuru LAN**

**Atacuri VLAN și DHCP**

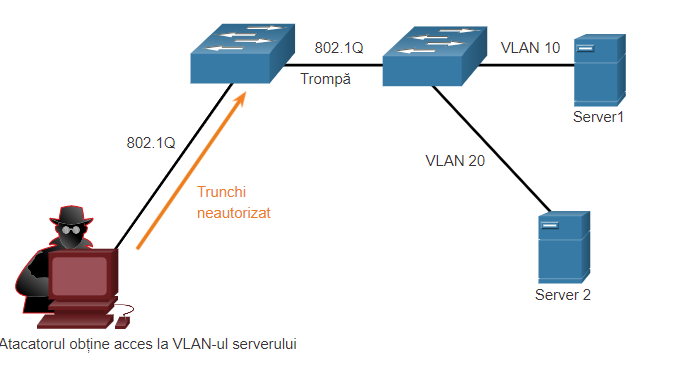
Acest subiect investighează numeroasele tipuri diferite de atacuri LAN și tehnicile lor de atenuare. La fel ca subiectele anterioare, aceste atacuri tind să fie specifice comutatoarelor și stratului 2.

## Atacurile de salt VLAN

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) proprietate 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.

Un atacator este conectat la un comutator care este conectat la un alt comutator printr-un trunchi 802.1Q. Cel de-al doilea comutator are o conexiune la Server 1 pe V LAN 10 și o conexiune la Server 2 la V LAN 20. Atacatorul a stabilit o legătură trunchială 802.1Q neautorizată la switch pentru a obține acces la serverul V LAN. o săgeată indică de la atacator la comutator și este etichetată trunchi neautorizat.

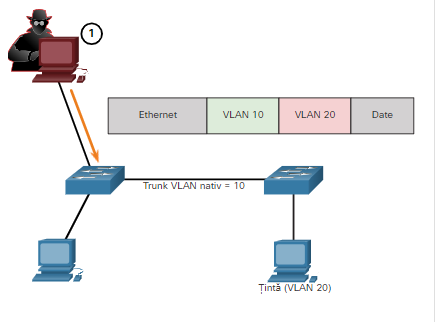


## Atac cu etichetare dublă VLAN

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.

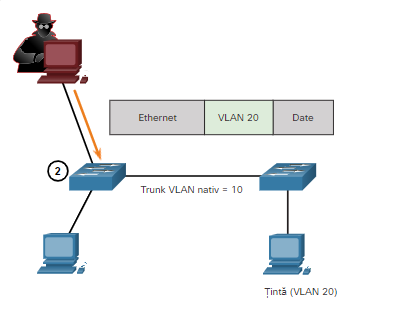
**Pasul 1.**

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.



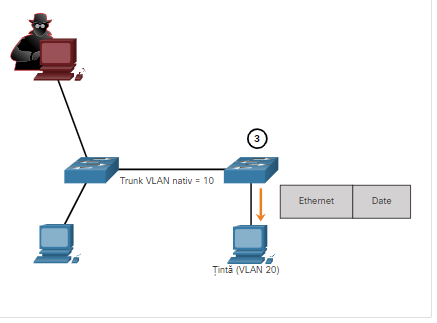
**Pasul 2**

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.

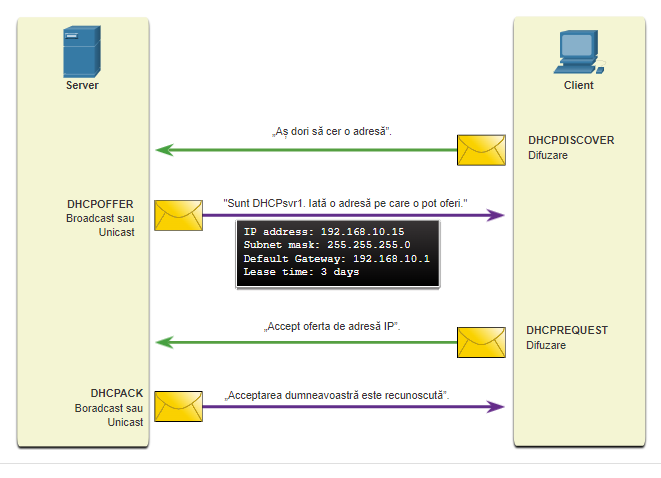
**Atenuarea atacurilor VLAN**

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. O revizuire a secvenței schimbului de mesaje DHCP între client și server este prezentată în figură.



**Atacurile DHCP**

Două tipuri de atacuri DHCP sunt DHCP starvation și DHCP spoofing. Ambele atacuri sunt atenuate prin implementarea DHCP Snooping.

**Atac de foame DHCP**

Scopul atacului 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.

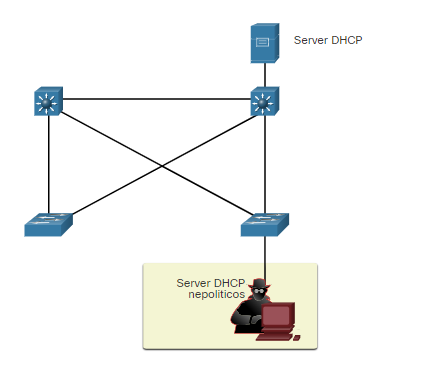
**Atac de falsificare DHCP**

Un 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.

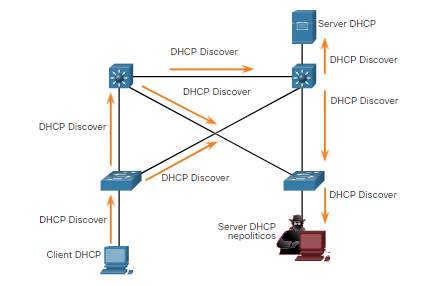
**Pasul 1** **Actorul de amenințare conectează serverul DHCP necinstiți**

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.



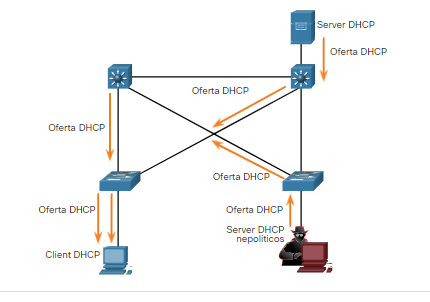
**Pasul 2 Clientul transmite mesaje de descoperire DHCP**

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



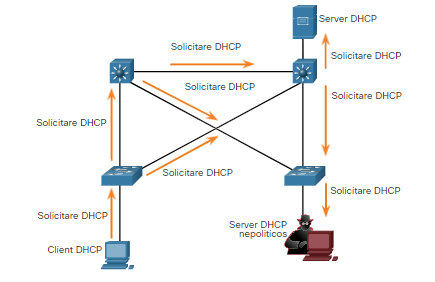
**Pasul 3** **Răspuns DHCP legitim și nepoliticos**

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.



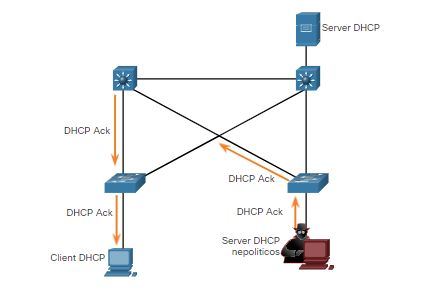
**Pasul 4** **Clientul acceptă oferta Rogue DHCP**

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

Amintiți-vă că 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.

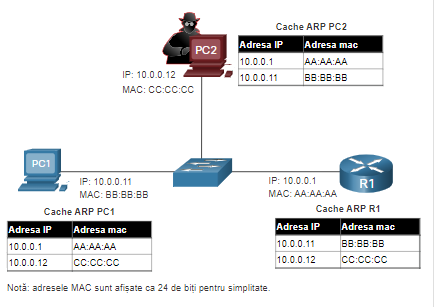
Problema este că un atacator poate trimite un mesaj ARP gratuit care conține o adresă MAC falsificată către un comutator, iar comutatorul își va actualiza tabelul MAC în consecință. Prin urmare, orice gazdă poate pretinde că este proprietarul oricărei combinații de adrese IP și MAC pe care o alege. Într-un 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**

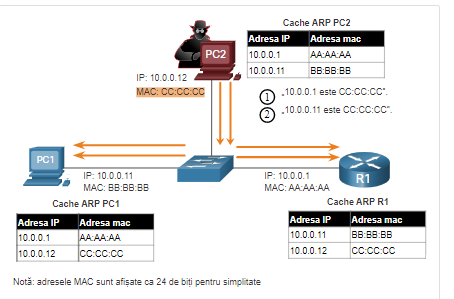
Fiecare dispozitiv are un tabel MAC precis cu adresele IPv4 și MAC corecte pentru celelalte dispozitive din LAN.



**Pasul 2.** **Atac de falsificare ARP**

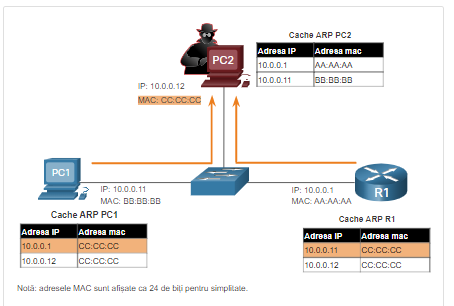
Actorul amenințării trimite două răspunsuri ARP gratuite falsificate în încercarea de a înlocui R1 ca gateway implicit:

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**

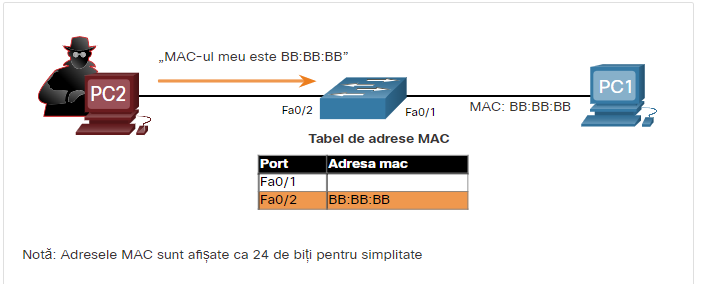
R1 și PC1 elimină intrarea corectă pentru adresa MAC a celuilalt și o înlocuiesc cu adresa MAC a PC2. Actorul amenințării a otrăvit acum cache-urile ARP ale tuturor dispozitivelor de pe subrețea. Otrăvirea ARP duce la diferite atacuri de tip man-in-the-middle, reprezentând o amenințare serioasă de securitate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

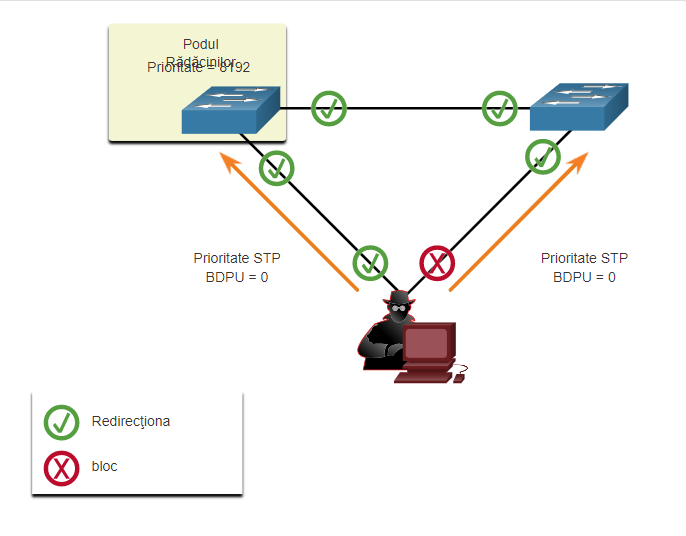
Falsificarea adreselor IP și MAC poate fi atenuată prin implementarea IPSG.

**Atacul STP**

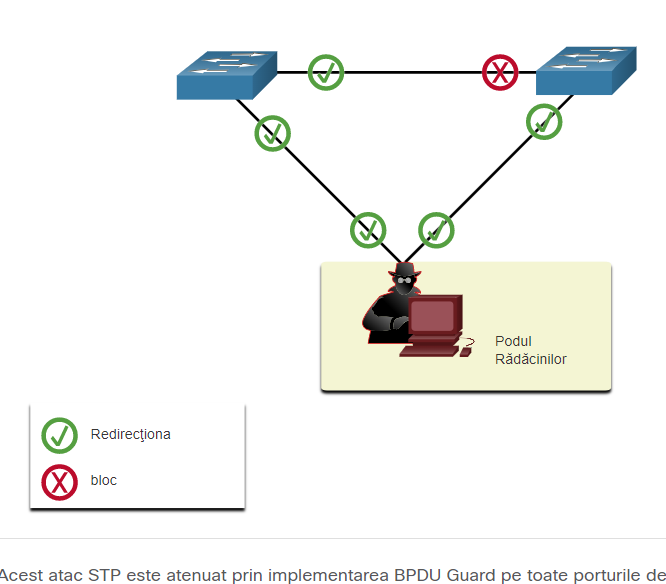
Atacatorii de rețea pot manipula protocolul Spanning Tree (STP) pentru a efectua un atac prin falsificarea podului rădăcină și modificarea topologiei unei rețele. Atacatorii își pot face gazdele să apară ca punți rădăcină; și, prin urmare, capturați tot traficul pentru domeniul comutat imediat.

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**

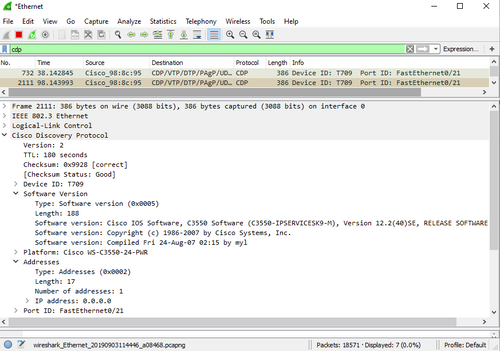
Cisco Discovery Protocol (CDP) este un protocol proprietar de descoperire a legăturilor de nivel 2. Este activat în mod implicit pe toate dispozitivele Cisco. CDP poate descoperi automat alte dispozitive compatibile cu CDP și poate ajuta la configurarea automată a conexiunii acestora. Administratorii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