
Comutarea în LAN: tabela MAC, ARP, domenii

Un switch primește un dispozitiv nou și, în câteva milisecunde, știe unde se află - fără ca nimeni să îi fi spus nimic. Lucrarea aceasta demontează mecanismul, pas cu pas: goliți tabela MAC, o umpleți privind-o, comparați switch-ul cu un hub pe aceeași topologie și vedeți la propriu ce înseamnă un domeniu de coliziune.

OBIECTIVELE CAPITOLULUI

- Construiți topologia și verificați conectivitatea completă între toate cele șase stații
- Documentați, cu capturi de ecran, cele trei acțiuni ale switch-ului: unicast, flood, drop
- Justificați în scris numărul de domenii de coliziune și de broadcast din topologie
- Comparați timpii de răspuns prin hub și prin switch, în condiții de trafic simultan
- Configurați complet managementul lui SW1 și demonstrați o conexiune SSH reușită
- Configurați port security pe toate cele trei porturi de acces, cu `restrict`, și provocați o violare pe unul dintre ele
- Adăugați un al doilea switch legat de SW1 și explicați ce se întâmplă cu domeniile

2.1 Ce demontăm astăzi

În laboratorul 1 ați dat un ping și a mers. Nimeni nu v-a explicat de ce switch-ul a știut unde să trimită cadrul. Astăzi aflați, iar răspunsul are doar trei reguli.

Tabelul 2.1 Ce demontăm astăzi.

Regula	Ce face switch-ul
învață	La fiecare cadru care intră, notează <i>adresa MAC sursă</i> și portul pe care a intrat. Nimeni nu îi spune nimic: deduce singur.
caută	Se uită la <i>adresa MAC destinație</i> . Dacă o găsește în tabelă, trimite cadrul doar pe portul acela (<i>unicast</i>).
inundă	Dacă nu o găsește - sau dacă destinația este broadcast - trimite cadrul pe toate porturile, în afară de cel pe care a intrat (<i>flood</i>).

Există și a patra situație, mai rară: dacă destinația este pe chiar portul de intrare, switch-ul aruncă cadrul (*drop*) - cele două stații se aud oricum direct.

DEFINIȚIA 2.1 (DOMENIU DE COLIZIUNE). Porțiunea de rețea în care două stații nu pot transmite simultan fără să se încurce. Fiecare port de switch creează unul separat. Un hub le contopește pe toate într-unul singur - de aici vine toată diferența de performanță dintre cele două.

DEFINIȚIA 2.2 (DOMENIU DE BROADCAST). Porțiunea de rețea până la care ajunge un mesaj trimis „către toți”. Se oprește la un ruter (sau la granița unui VLAN, din laboratorul 3). Nici switch-ul, nici hub-ul nu îl opresc.

DEFINIȚIA 2.3 (ARP). Protocolul care traduce o adresă IP într-o adresă MAC. O stație știe cu cine vrea să vorbească (192.168.5.11), dar are nevoie de numărul plăcii de rețea ca să compună cadrul. Întreabă în broadcast, primește răspuns unicast și ține minte răspunsul câteva minute.

2.2 Echipamente necesare

Tabelul 2.2 Echipamente necesare.

Buc.	Echipament	Model	Categoria din Packet Tracer	La ce folosește aici
1	Switch	2960	Network Devices → Switches	partea „inteligentă” a topologiei
1	Hub	Hub-PT	Network Devices → Hubs	termenul de comparație
6	Calculator	PC-PT	End Devices → End Devices	PC-A ... PC-F
7	Cablu de cupru	Copper Straight-Through	Connections → Connections	toate legăturile

Opțional, pentru ultima sarcină: încă un switch 2960 și un cablu Copper Cross-Over.

Ce se poate face în bancul din pagină și ce cere Packet Tracer. Bancul de lucru din această pagină acoperă: tabela MAC și golirea ei, comportamentul hub-ului, ARP, adresa de management pe VLAN 1, port security cu violare provocată prin mutarea unui cablu.

Cer Packet Tracer: modul *Simulation* cu plicuri urmărite pas cu pas, măsurarea timpilor sub trafic simultan, sesiunea SSH propriu-zisă și îmbătrânirea reală a intrărilor în timp.

2.3 Topologia de construit

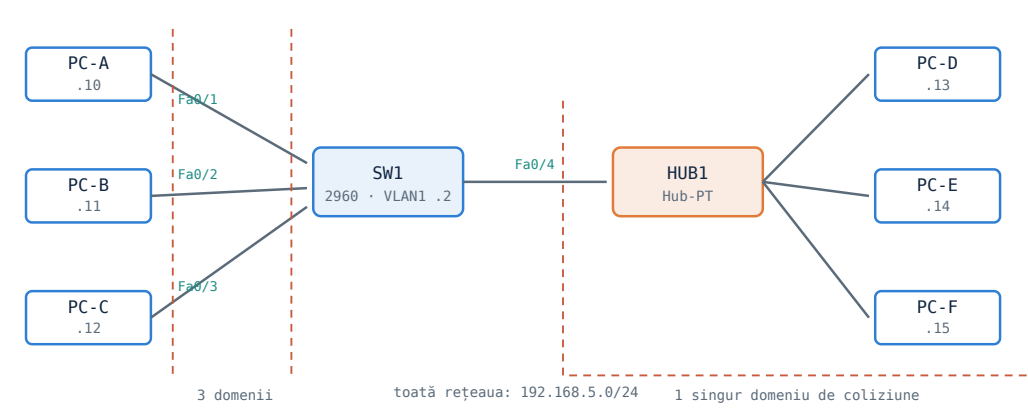


Figura 2.1 Aceeași rețea, două filozofii de interconectare. În stânga, fiecare stație are domeniul ei de coliziune. În dreapta, toate trei îl împart.

Tabelul 2.3 Topologia de construit.

Dispozitiv	Adresă IP	Mască	Port pe SW1 / HUB1
PC-A	192.168.5.10	255.255.255.0	SW1 Fa0/1
PC-B	192.168.5.11	255.255.255.0	SW1 Fa0/2
PC-C	192.168.5.12	255.255.255.0	SW1 Fa0/3
PC-D, PC-E, PC-F	192.168.5.13 – .15	255.255.255.0	HUB1
SW1	192.168.5.2 (VLAN 1)	255.255.255.0	-

Nu există ruter și nu este nevoie de gateway: toate stațiile sunt în aceeași rețea. Legătura SW1 Fa0/4 – HUB1 se face cu cablu straight-through.

2.4 Bancul de lucru

Topologia din figura 1, cablată și adresată. Toate secțiunile următoare se pot face aici; deschideți-l într-o filă alături de text și lucrați pe măsură ce citiți.

2.5 Tabela MAC, observată cum se umple

1. Notați adresele MAC ale stațiilor

Pentru fiecare stație, deschideți terminalul (în Packet Tracer: *Desktop* → *Command Prompt*) și rulați:

pe fiecare stație

```
ipconfig /all
```

Notăți câmpul *Physical Address* - este adresa MAC. Veți avea nevoie de aceste șase valori la fiecare pas care urmează; fără ele, tabela switch-ului este un șir de cifre fără sens.

2. Goliți tabela și verificați că este goală

pe SW1

```
Switch> enable
Switch# clear mac address-table dynamic
Switch# show mac address-table
```

Trebuie să nu apară nicio intrare. Dacă mai apar, înseamnă că a trecut deja trafic între timp - repetați cele două comenzi imediat una după alta.

3. Un singur cadru, și priviți ce s-a întâmplat

De pe PC-A, dați un singur ping către PC-B, apoi reveniți imediat pe SW1:
pe PC-A

```
ping -n 1 192.168.5.11
```

pe SW1

```
SW1# show mac address-table
```

Întrebare

Câte intrări au apărut și de unde a aflat switch-ul fiecare dintre ele?

► Vezi răspunsul

4. Cele trei acțiuni, una câte una

Goliți din nou tabela și executați scenariile în ordinea de mai jos. În Packet Tracer treceți în *Simulation* și filtrați pe ICMP și ARP, ca să vedeți plicurile. În bancul din pagină, urmăriți tabela MAC după fiecare pas.

Scenariu	Ce face switch-ul	Cum verificați
PC-A → PC-B, cu tabela goală	flood: cadrul iese pe toate porturile în afară de Fa0/1	tabela era goală, deci destinația era necunoscută
PC-B → PC-A, imediat după	unicast: doar pe Fa0/1	<code>show mac address-table</code> conține deja PC-A
PC-A → broadcast	flood, întotdeauna	în Packet Tracer: <code>ping 192.168.5.255</code>

5. Îmbătrânirea intrărilor

pe SW1

```
SW1# show mac address-table aging-time
SW1# configure terminal
SW1(config)# mac address-table aging-time 30
SW1(config)# end
```

Valoarea implicită este de 300 de secunde. Reduceți-o la 30, generați trafic de la PC-C, apoi lăsați rețeaua liniștită și urmăriți tabela din 15 în 15 secunde: intrarea dispare. (Trecerea timpului se observă doar în Packet Tracer; în bancul din pagină comanda este acceptată, dar tabela nu îmbătrânește singură.)

De ce e nevoie de îmbătrânire Dacă mutați PC-C de pe Fa0/3 pe Fa0/5, switch-ul ar continua să trimită traficul pentru el pe portul vechi - la nesfârșit. În practică, primul cadru emis de PC-C de pe noul port corectează imediat intrarea; îmbătrânirea acoperă cazul în care stația a plecat și nu mai vorbește deloc.

Verificați asta chiar acum, în bancul de lucru: alegeți PC-C, în panoul **Cablurile** apăsați *scoate*, apoi *leagă* spre SW1 : Fa0/5. Dați un ping de pe PC-C și priviți din nou `show mac address-table`: intrarea s-a mutat singură pe noul port.

2.6 Switch contra hub

Partea din dreapta a topologiei există dintr-un singur motiv: să vedeți diferența, nu să v-o imaginați.

1. Trafic prin hub

De pe PC-D dați ping către PC-E. În Packet Tracer, în *Simulation*, urmăriți plicul.

Hub-ul îl trimite **pe toate porturile** - inclusiv la PC-F, care nu are nicio treabă cu această conversație, și înapoi spre switch. PC-F primește cadrul, se uită la adresa MAC destinație, constată că nu îi aparține și îl aruncă. Timp și bandă consumate degeaba, la fiecare cadru.

În bancul din pagină, verificați consecința pe switch: după un ping între două stații legate la hub, `show mac address-table` pe SW1 arată ambele adrese **pe același port**, Fa0/4. Switch-ul nu are cum să le separe: din punctul lui de vedere, tot ce e dincolo de hub stă pe un singur fir.

2. Coliziunea, provocată doar în Packet Tracer

Reveniți în *Realtime*. Deschideți simultan terminalele pe PC-D și PC-F și lansați de pe ambele, cât mai apropiat în timp:
pe PC-D și PC-F, aproape simultan

```
ping -n 200 -l 1400 192.168.5.10
```

Comparați timpii de răspuns cu cei obținuți când rulați singur. Repetați experimentul înlocuind hub-ul cu un al doilea switch și observați diferența.

3. Numărați domeniile

Exercițiu

Pentru topologia din figura 1, câte domenii de coliziune și câte domenii de broadcast există?

► Vezi răspunsul

2.7 ARP, cu cache-ul golit

1. Ștergeți cache-ul și priviți cererea

pe PC-A

```
arp -d
arp -a
ping -n 1 192.168.5.12
arp -a
```

Prima afișare trebuie să spună `No ARP Entries Found`. După ping, apare adresa lui PC-C împreună cu MAC-ul ei. Acesta este întreg mecanismul: o întrebare, un răspuns, o notiță ținută minte câteva minute.

În Packet Tracer, urmăriți cererea ARP în *Simulation* și citiți din *Outbound PDU Details*:

- adresa MAC destinație a cadrului: `FFFF.FFFF.FFFF` - broadcast;
- câmpul **Target MAC** din pachetul ARP: zerouri - exact ce se cere;
- câmpul **Target IP**: adresa lui PC-C.

Toate stațiile primesc cererea. Doar PC-C răspunde; celelalte o ignoră tăcut.

2. Efectul cache-ului

Dați `ping 192.168.5.12` imediat după `arp -d` și apoi încă o dată. Prima oară primul pachet se pierde; a doua oară, niciunul. Diferența este exact costul rezoluției ARP.

Rețineți simptomul Într-o rețea cu probleme, ping-uri care „merg, dar prima dată eșuează” indică aproape întotdeauna o chestiune de ARP, nu de rutare. Este primul lucru pe care îl eliminați din listă.

2.8 Administrarea switch-ului

Până acum am configurat switch-ul stând la consola lui. Ca să îl putem administra de la distanță, are nevoie de o adresă IP și de un mod de acces protejat prin parolă.

Comenzile de mai jos se scriu rând cu rând. Cele care încep cu ! sunt comentarii - nu se scriu.

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW1
SW1(config)# no ip domain-lookup

! adresa de management stă pe interfața virtuală VLAN 1
SW1(config)# interface vlan 1
SW1(config-if)# ip address 192.168.5.2 255.255.255.0
SW1(config-if)# no shutdown
SW1(config-if)# exit

! parola pentru modul privilegiat
SW1(config)# enable secret Cisco123
SW1(config)# service password-encryption

SW1(config)# end
SW1# copy running-config startup-config
```

Listingul 2.1 configurația de management a lui SW1 copiază

Verificați din două locuri:

```
SW1# show ip interface brief
```

Listingul 2.2 pe SW1 copiază

Vlan1 trebuie să apară cu 192.168.5.2 și up / up. Dacă apare administratively down, ați uitat no shutdown pe interfața VLAN.

```
ping 192.168.5.2
```

Listingul 2.3 pe PC-A copiază

Accesul de la distanță

Pentru o sesiune SSH adevărată, mai sunt necesare un nume de domeniu, o cheie și un utilizator. Aceste comenzi se demonstrează în Packet Tracer:

```
SW1(config)# ip domain-name retele.local
SW1(config)# crypto key generate rsa
! la intrebarea despre lungimea cheii, raspundeti 1024
SW1(config)# username admin privilege 15 secret Admin123
SW1(config)# line vty 0 4
SW1(config-line)# transport input ssh
SW1(config-line)# login local
SW1(config-line)# exit
SW1(config)# banner motd #Acces autorizat numai#
```

Listingul 2.4 pe SW1, în Packet Tracer copiază

```
ssh -l admin 192.168.5.2
```

Listingul 2.5 pe PC-A copiază

Adresa de pe VLAN 1 nu face switch-ul un ruter. Este doar un punct de contact pentru administrare. Switch-ul continuă să comute pe baza adreselor MAC și nu va ruta nimic între rețele. Dacă trebuie administrat dintr-o altă rețea, are nevoie în plus de ip default-gateway.

2.9 Port security

Un port de switch acceptă, implicit, orice adresă MAC i se prezintă. Port security limitează numărul de adrese care pot fi învățate pe un port și decide ce se întâmplă când limita e depășită - prima apărare împotriva atacului de tip CAM overflow din cursul 12.

```
SW1# configure terminal
SW1(config)# interface fastEthernet 0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security maximum 1
SW1(config-if)# switchport port-security mac-address sticky
SW1(config-if)# switchport port-security violation shutdown
SW1(config-if)# end

SW1# show port-security
SW1# show port-security interface fastEthernet 0/1
SW1# show running-config
```

Listingul 2.6 pe portul lui PC-A copiază

Dați un ping de pe PC-A, apoi priviți din nou `show running-config`: adresa MAC a lui PC-A a fost „lipită” automat în configurație. Asta face *sticky*.

Provocați violarea

În bancul din pagină, mutarea cablului se face din panoul **Cablurile**:

- 1. Alegeți PC-A și apăsați *scoate* pe portul Fa0.
- 2. Alegeți PC-C, apăsați *scoate*, apoi *leagă* și alegeți SW1 : Fa0/1.
- 3. Dați un ping de pe PC-C către PC-B.
- 4. Pe SW1: `show interfaces status` - portul apare `err-disabled`.

```
SW1# configure terminal
SW1(config)# interface fastEthernet 0/1
SW1(config-if)# shutdown
SW1(config-if)# no shutdown
SW1(config-if)# end
```

Listingul 2.7 reactivarea portului copiază

Portul se închide din nou imediat. Cât timp PC-C stă pe acel port, violarea se repetă la primul cadru: adresa lipită în configurație este tot a lui PC-A. Portul rămâne utilizabil doar dacă puneți PC-A la loc sau dacă ștergeți adresa lipită. Este exact comportamentul din rețelele reale - și motivul pentru care un administrator obosit alege `restrict`.

Tabelul 2.4 Provocați violarea.

Acțiune	Cadrela în exces	Contor	Notificare	Portul
protect	aruncate	nu	nu	rămâne activ
restrict	aruncate	da	SNMP + syslog	rămâne activ
shutdown	-	da	SNMP + syslog	err-disabled

Alegeți cu cap acțiunea. `shutdown` pare cea mai sigură, dar înseamnă că orice utilizator care își schimbă laptopul rămâne fără rețea până când vine cineva să reactiveze portul. În majoritatea rețelelor de birou, `restrict` este compromisul corect: blochează traficul suspect, dar anunță în loc să pedepsească.

2.10 Provocare

Exemplul 2.1. Considerați topologia din figura 1, cu tabela MAC a lui SW1 **complet goală**. Se execută, în ordine, următoarele trei operații:

1. PC-C trimite un cadru unicast către PC-A
2. PC-D trimite un cadru unicast către PC-A
3. PC-B trimite un cadru unicast către PC-D

Pentru fiecare operație, precizați: ce intrări se adaugă în tabela MAC a lui SW1, ce acțiune ia switch-ul, și care dintre cele șase stații primesc efectiv cadrul.

Rezolvare. 1. PC-C → PC-A. SW1 învață MAC-ul lui PC-C pe Fa0/3. Destinația e necunoscută, deci **flood** pe Fa0/1, Fa0/2, Fa0/4. Primesc cadrul: PC-A, PC-B și, prin hub, PC-D, PC-E, PC-F. Doar PC-A îl procesează; restul îl aruncă.

2. PC-D → PC-A. Cadrul intră pe Fa0/4, deci SW1 învață MAC-ul lui PC-D pe **Fa0/4** - portul dinspre hub. Destinația PC-A este încă necunoscută (PC-A nu a transmis nimic până acum), deci din nou **flood**, pe Fa0/1, Fa0/2, Fa0/3. Primesc: PC-A, PC-B, PC-C. În plus, PC-E și PC-F primesc cadrul direct de la hub, care îl repetă pe toate porturile.

3. PC-B → PC-D. SW1 învață MAC-ul lui PC-B pe Fa0/2. Destinația PC-D **este** cunoscută, pe Fa0/4, deci de această dată **unicast**: cadrul pleacă doar pe Fa0/4. Îl primesc însă PC-D, PC-E și PC-F - pentru că hub-ul nu știe să facă altceva decât să repete.

Concluzia care contează: switch-ul a devenit selectiv după primul cadru al fiecărei stații. Hub-ul nu devine niciodată. Iar un atacator conectat la hub vede tot traficul, fără să facă absolut nimic.

2.11 Ce se predă

Tabelul 2.5 Ce se predă.

Livrabil	Format	Punctaj
Fișierul Packet Tracer, cu management și port security configurate	.pkt	35 %
Documentarea celor trei acțiuni ale switch-ului, cu capturi	document	25 %
Analiza domeniilor de coliziune și broadcast, justificată	document	20 %
Rezolvarea provocării, cu raționamentul pas cu pas	document	20 %

Exerciții

1. Dintr-un singur ping între două stații, câte intrări apar în tabela MAC a switch-ului?
 - a. Una, a sursei
 - b. Două: sursa și destinația, învățate din cererea și răspunsul ARP
 - c. Trei
 - d. Niciuna, până la expirarea aging-time
2. Câte domenii de coliziune are un switch cu 24 de porturi, toate ocupate?
 - a. 1
 - b. 12
 - c. 24
 - d. Depinde de VLAN-uri
3. Un switch primește un cadru a cărui adresă MAC destinație este în tabela, pe chiar portul de intrare. Ce face?
 - a. Il inunda
 - b. Il comută unicast pe acel port
 - c. Il aruncă - sursa și destinația sunt de aceeași parte
 - d. Il trimite la router
4. Două stații sunt legate la un hub, iar hub-ul la un switch. Cum apar ele în tabela MAC a switch-ului?
 - a. Fiecare pe portul ei
 - b. Amândouă pe același port, cel dinspre hub
 - c. Nu apar deloc
 - d. Doar prima care transmite
5. Ce face opțiunea mac-address sticky din port security?
 - a. Fixează portul în starea up
 - b. Învăță automat adresa MAC conectată și o scrie în configurație
 - c. Blochează toate adresele MAC
 - d. Criptează adresa MAC

6. De ce un hub face imposibila comunicatia full-duplex?

- a. Pentru ca nu are suficiente porturi
- b. Pentru ca toate statiile impart acelasi mediu si trebuie sa asculte inainte de a transmite
- c. Pentru ca nu suporta cabluri Cat 5e
- d. Pentru ca nu are tabela MAC

Extras din volumul „Rețele Locale - Note de curs și lucrări de laborator”. Varianta online a acestui capitol conține figurile în formă interactivă.