



# VLAN-uri

## Capitolul 5



# Întrebarea zilei



Cum putem separa o rețea în mai multe rețele independente la nivel logic?



# Probleme și soluții în LAN



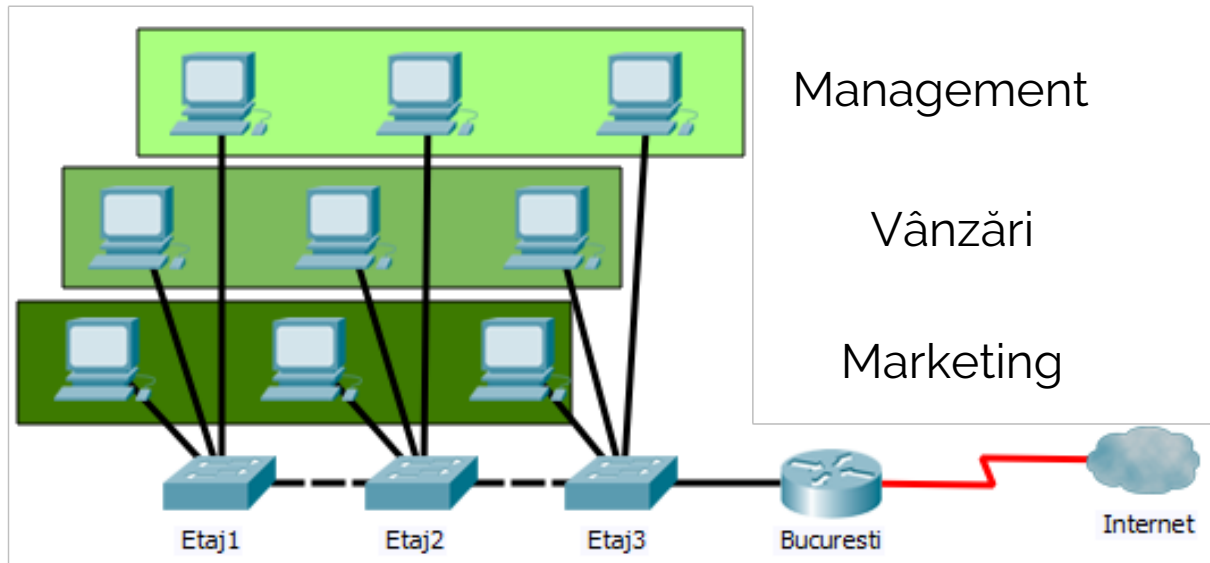
# Problemă



Mesaje broadcast => trafic inutil în rețea



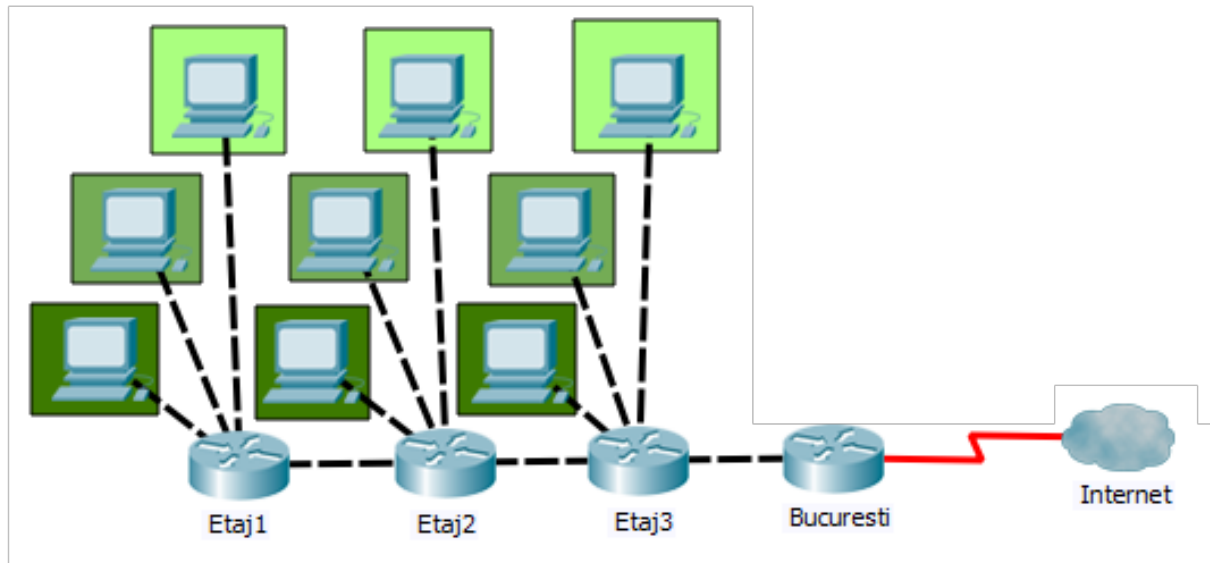
Traficul nu poate fi izolat





# Soluție: rutere

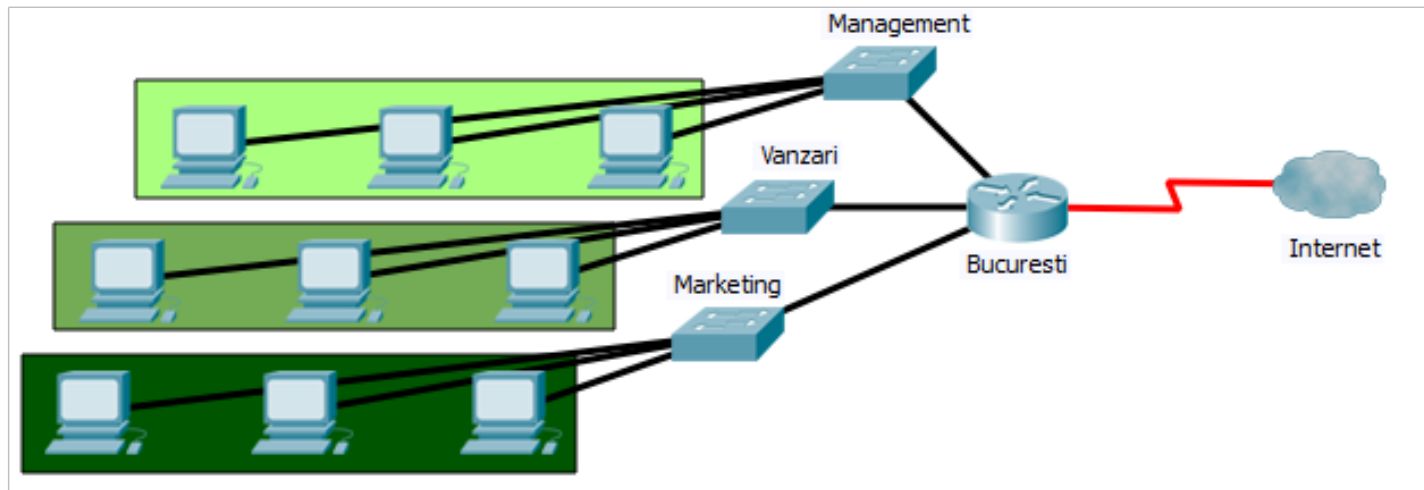
- ⊕ Se limitează domeniile de broadcast
- ⊖ Prețul crește semnificativ





# Soluție: rutere și switch-uri

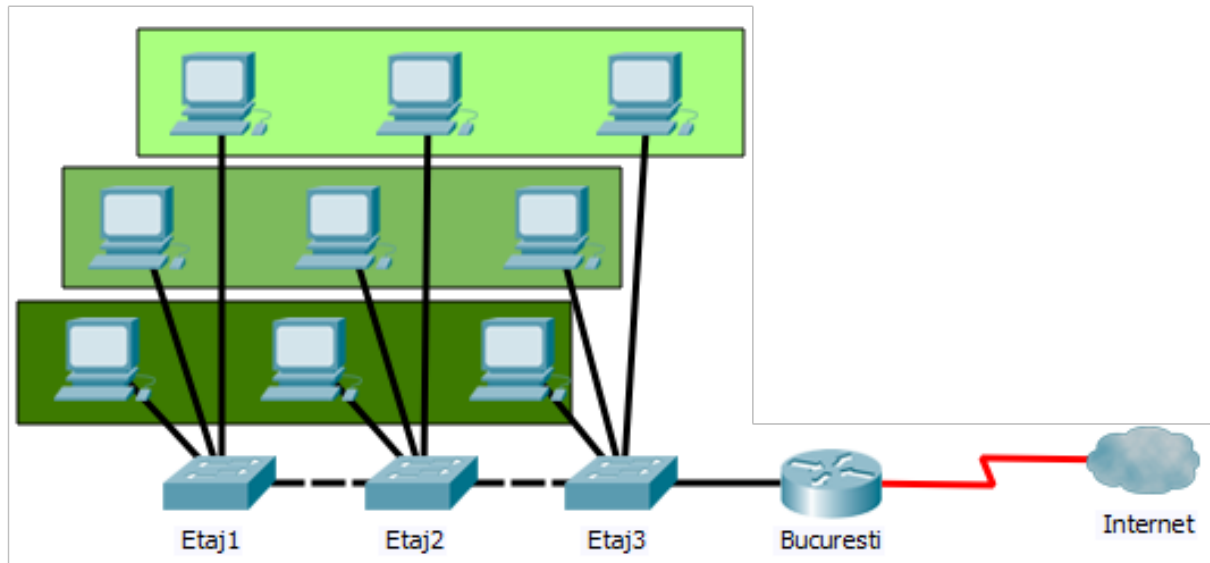
- ⊕ Mai ieftin
- ⊖ Trebuie refăcută topologia





# Soluție: VLAN-uri

- ⊕ Împărțire logică a rețelei
- ⊕ Rețeaua locală este segmentată









# Segmentarea rețelelor





# De ce folosim VLAN-uri?

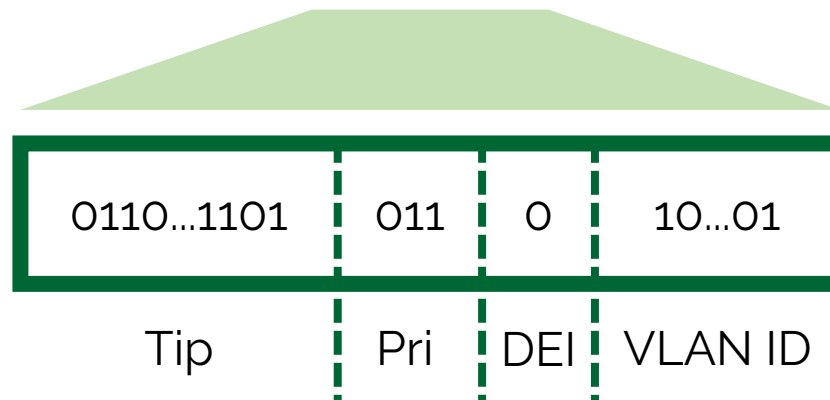
-  Segmentarea domeniilor de broadcast
-  Creșterea performanței
-  Reducerea costurilor
-  Securitate sporită



# Cum funcționează?

- Se adaugă un câmp în antetul de nivel 2

MAC Dest	MAC Sursă	Tag DOT1q	Lungime /Tip	Date	FCS
0110...1101	1110...1100	10...01	110...001	11011100...00111011	0...1





# Tipuri de legături



## Access

- Un singur VLAN poate circula pe legătură
- Legătură folosită între switch și un nod final



## Trunk

- Mai multe VLAN-uri pot circula pe legătură
- Folosită pentru conexiuni între echipamente de rețea



# Tipuri de VLAN-uri

- Data
  - Trafic generat de utilizatori
- Default
- Nativ
- Management



# Tipuri de VLAN-uri

- Data
- Default
  - Conține toate porturile
  - Inițial = VLAN 1
- Nativ
- Management



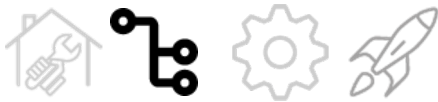
# Tipuri de VLAN-uri

- Data
- Default
- Nativ
  - Atribuit unui port trunk
  - Traficul din acest VLAN circulă neetichetat
- Management



# Tipuri de VLAN-uri

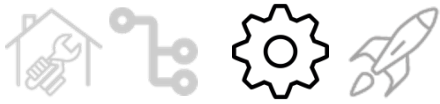
- Data
- Default
- Nativ
- Management
  - Pentru administrarea echipamentului de la distanță



# VLAN ID

- ID-ul poate fi între 1 și 4094
- VLAN-urile cu ID mai mare de 1005 nu sunt salvate în vlan.dat
- VLAN-urile 1 și 1002-1005 sunt create automat și nu pot fi șterse (cele din urmă sunt folosite pentru alte protocoale de nivel 2, FDDI și Token Ring)





# Configurare

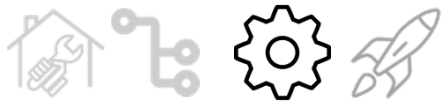


# Crearea unui VLAN

- Din modul global de configurare:

```
Etaj1 (config) #vlan 10  
Etaj1 (config-vlan) #name Vanzari  
Etaj1 (config-vlan) #exit
```

- Nu este nevoie de comanda **write**
- Configurație stocată în Flash (vlan.dat)
- La reload, vlan-urile create nu se pierd



# Configurarea interfețelor

- Access
  - Permite pachete dintr-un singur VLAN
  - Default, toate interfețele sunt în VLAN-ul 1
  - Dacă VLAN-ul asignat este șters, interfața nu mai primește trafic

```
Etaj1 (config) #interface fa0/2  
Etaj1 (config-if) #switchport mode access  
Etaj1 (config-if) #switchport access vlan 10
```

- Trunk
- Dynamic



# Configurarea interfețelor

- Access
- Trunk
  - Permite trecerea pachetelor din mai multe VLAN-uri
  - O legătură trunk are întotdeauna un VLAN nativ

```
Etaj1 (config) #interface fa0/1  
Etaj1 (config-if) #switchport mode trunk  
Etaj1 (config-if) #switchport trunk allowed vlan 10,20,30
```

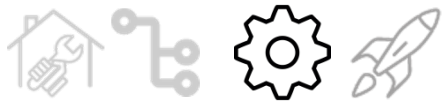
- Dynamic



# Configurarea interfețelor

- Access
- Trunk
- Dynamic
  - Folosește DTP (Dynamic Trunking Protocol) pentru determinarea tipului de interfață

```
Etaj1(config) #interface fa0/1  
Etaj1(config-if) #switchport mode dynamic {desirable | auto}
```



# Negocierea modului interfeței

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access



# Rocket Science



# Switch Spoofing



Atacatorul anunță echipamentul său ca fiind switch, căpătând acces în rețea



Prevenire:

- dezactivare DTP
- dezactivare trunking porturi nefolosite





# Double-tagging attack



Atacatorul adaugă un tag de VLAN în plus



Prevenire:

- VLAN nativ diferit de toate VLAN-urile utilizatorilor



# Bune practici

- Separarea VLAN-ului de management de VLAN-urile de date
- Schimbarea VLAN nativ pe legăturile trunk
- Dezactivarea negocierii auto în DTP
- Folosirea unui VLAN Voce separat
- Dezactivarea porturilor nefolosite



# Răspunsul zilei



## Răspunsul zilei

❗ Cum putem separa o rețea în mai multe rețele independente la nivel logic?