Capitolul 3:
VLAN-uri

Extinderea rețelei

- Hub
  - **extinde** domeniul de coliziune
  - trimite toate pachetele broadcast
- Switch (default)
  - segmentează domeniul de coliziune
  - **extinde** domeniul de broadcast
  - trimite pachete atât unicast cât și broadcast

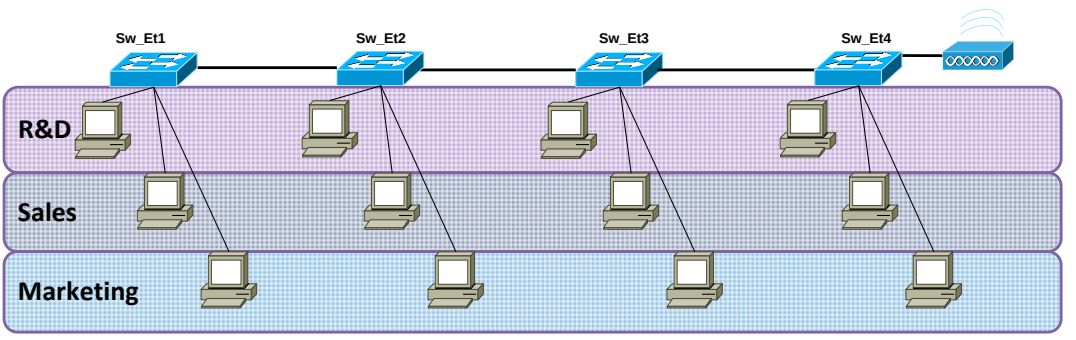
În rețelele actuale se urmărește reducerea dimensiunii domeniilor de broadcast prin separarea acestora în funcție de departamentele specifice fiecarei companii.

Hub-ul este un echipament de rețea ce nu se mai folosește în ziua de astăzi, deoarece extinde domeniile de coliziune, astfel creând riscuri de securitate și un overhead considerabil din cauza trimiterii pachetelor pe toate porturile.

Echipamentul folosit preponderent în rețelele actuale este switch-ul. Acesta segmentează domeniul de coliziune, oferă securitate la nivel de porturi și reduce mult overhead-ul rețelei deoarece folosește predominant transmisie de tip unicast. VLAN-urile sunt o tehnologie ce se mapează perfect pe rețelele locale actuale ce folosesc switch-uri.

Probleme într-o rețea locală

- Broadcast-uri
  - trafic inutil
- Securitate
  - traficul nu poate fi izolat



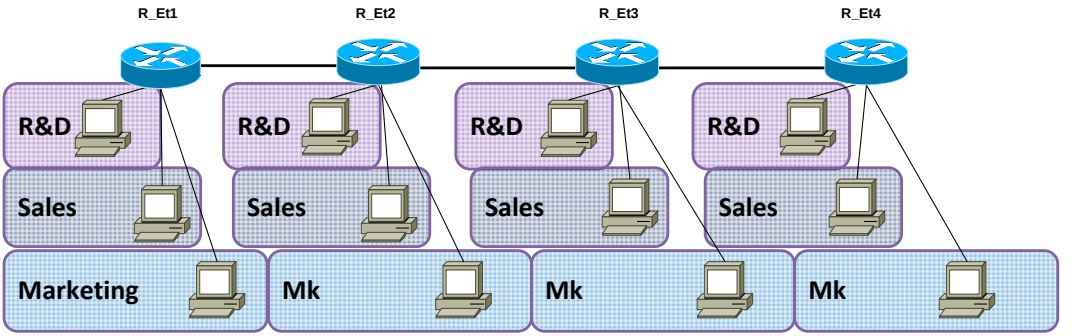
Cu cât avem un număr mai mare de echipamente într-o rețea locală (switch-uri, stații) cu atât numărul pachetelor de broadcast va fi mai mare. Acest lucru creează trafic inutil pe link-urile rețelei, deoarece switch-ul mărește domeniul de broadcast. Un mesaj cu destinația 255.255.255.255 va fi reprodus de fiecare switch pe traseu către toate stațiile din toate departamentele.

O altă problemă majoră în rețelele locale este securitatea. Pachetele trimise broadcast în rețelele locale pot fi interceptate de toate stațiile conectate la rețea.

Vom observa în continuare soluțiile de rezolvare a acestor probleme.

Soluție folosind rutere

- Deficiențele soluției
  - ruterele sunt scumpe
  - porturile pe rutere sunt scumpe
  - prea multe domenii de broadcast



O soluție pentru separarea domeniilor de broadcast în funcție de specificul departamentelor este cea în care echipamentele intermediare sunt înlocuite de rutere.

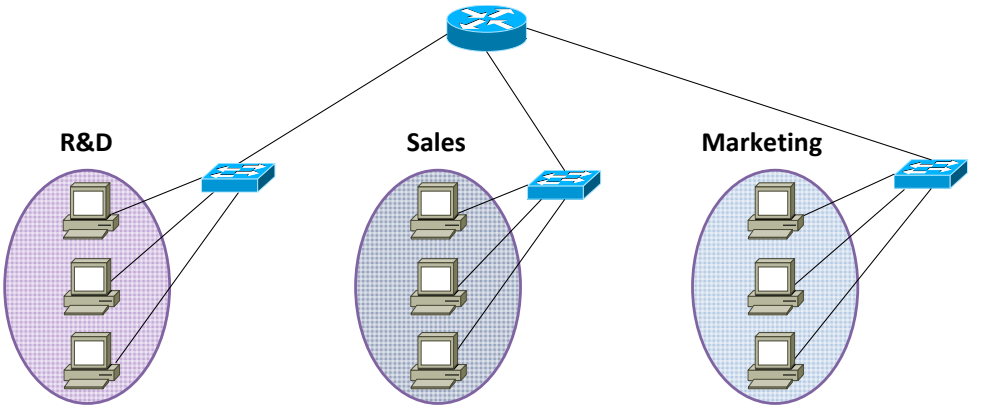
Ruterele fiind echipamente ce iau decizii în funcție de nivelul 3, separă departamentele în rețele diferite. Fiecare interfață a unui ruter delimitează un domeniu de broadcast, deci dimensiunea unui domeniu de broadcast va fi minimizată cu ajutorul acestei soluții.

De asemenea, pe rutere se pot implementa politici de filtrare a traficului astfel încât să se poată controla traficul de la o subretea la cealaltă.

Neajunsul acestei soluții, în afara de costul ridicat al echipamentelor, este faptul că ruterele introduc un overhead foarte mare în rețeaua locală (fiecare calculator să fie într-o rețea unică și să existe rutare end-to-end).

Soluție folosind ruter și switchuri

- Mai ieftină
- Mai eficientă



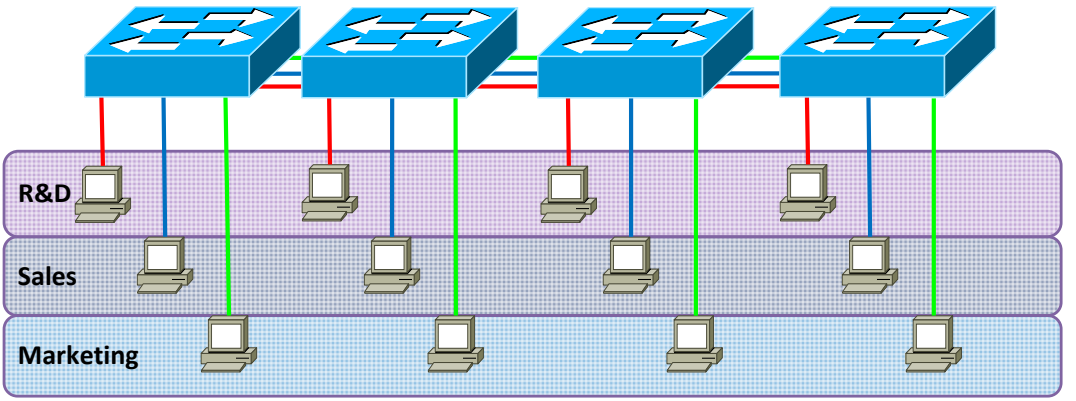
O combinație între primele două soluții ar însemna legarea stațiilor de pe fiecare departament la câte un switch, urmând ca apoi switch-urile să fie conectate la un ruter care stabilește politicile de trimitere ale pachetelor.

Această soluție deși rezolvă problema domeniilor de broadcast este nerecomandată datorită faptului că este nescalabilă. Pentru a implementa această soluție, este necesar ca toate echipamentele terminale ale aceluiași departament să fie legate la același switch. Spre deosebire de exemplul anterior, soluția prezentată este mult mai eficientă dar oferă foarte puțină flexibilitate la nivelul fizic .

Această soluție este mai ieftină decât precedenta, dar în funcție de numărul de departamente al companiei poate presupune topologii foarte complicate.

Soluție folosind VLAN-uri

- Împărțire a rețelei în funcție de departament nu în funcție de așezarea geografică



Soluția optimă pentru rezolvarea problemei domeniilor de broadcast a diferitelor departamente într-o rețea locală este folosirea tehnologiei Virtual LAN (VLAN). Aceasta permite unui administrator de rețea să creeze grupuri de echipamente ce se află în rețele independente la nivel logic chiar dacă folosesc aceeași infrastructură la nivel fizic. Această tehnologie permite crearea mai multor rețele de nivel 3 în aceeași rețea locală folosindu-se aceeași infrastructură de switching.

De asemenea putem folosi un VLAN pentru a ne structura geografic rețeaua astfel încât aceasta să poată scala fără modificarea drastică a topologiei inițiale.

Reguli

- Un VLAN corespunde unui subnet
  - un VLAN este un domeniu de broadcast
- Un VLAN este configurat per port
  - stațiile nu știu că aparțin unui VLAN
- Pentru a comunica între VLAN-uri este nevoie de un dispozitiv Layer 3
  - ruter
  - switch L3
- Un switch are câte o tabelă MAC pentru fiecare VLAN

Pentru ca stațiile să comunice în același VLAN ele trebuie să aibă un IP și o mască de rețea consistentă pentru întreg VLAN-ul . Port-ul switch-ului la care este conectată stația trebuie să fie asignat VLAN-ului din care face parte echipamentul terminal. Un port al unui switch ce este atribuit exclusiv unui singur VLAN se numește un port de tip Access.

Stațiile aflate în VLAN-uri diferite, chiar dacă sunt conectate la același switch, nu pot comunica între ele. Pentru a rezolva această problemă avem nevoie de un echipament de nivel 3 (Switch Layer 3, Ruter). Switch-ul menține o tabelă CAM pentru fiecare VLAN în care reține MAC-urile stațiilor ce se conectează la switch pe porturile asignate VLAN-ului respectiv.

Beneficii VLAN-uri

- Securitate sporită
- Reducerea costurilor
- Performanță crescută
- Delimitare domenii Broadcast
- Management simplificat al rețelei

VLAN-urile presupun securitate sporită deoarece grupurile ce au de transmis date confidențiale sunt separate de restul rețelei. Reducerea costului provine din lipsa necesității unor echipamente ce operează la nivelul 3 sau mai sus în stiva OSI și din folosirea mai eficientă a lățimii de bandă existente.

Performanța sporită se datorează împărțirii în domenii de broadcast astfel reducând traficul ce nu este necesar tuturor echipamentelor din rețea.

VLAN-urile simplifică mult administrarea rețelei deoarece utilizatorii ce au nevoi similare împart același VLAN.

LAN-uri Virtuale

- VLAN implicit: **VLAN1**
  - creat automat pe switch-uri
  - nu poate fi șters
  - inițial toate porturile sunt în VLAN 1
- VLAN 2 – 1001
  - Ethernet VLAN
- VLAN 1002 – 1005
  - Token Ring și FDDI VLAN
  - create automat pe switch și nu pot fi șterse
- VLAN 1006 - 4096
  - extended VLANs

VLAN-urile standard se află între ID-urile 1 - 1005 . Aceste VLAN-uri se împart în VLAN-uri Ethernet (cu valori între 2 - 1001) și VLAN-uri Token Ring și FDDI VLAN (cu valori 1002 - 1005), cele din urmă creându-se automat pe switch și neputând fi șterse. VLAN-urile cuprinse între ID-urile 1006 și 4096 se numesc Extended VLAN. VLAN-urile extinse suportă mai puține facilități decât VLAN-urile standard și permit unei companii enterprise să își extindă infrastructura la un număr mai mare de clienți.

VLAN-urile standard, salvate în fișierul vlan.dat în Flash, se păstrează la restartarea switch-ului.

VLAN-urile extinse nu se păstrează în vlan.dat ci în running-config. Astfel, pentru a se păstra configurația, este necesar să copiem modificarile in startup-config.

Stocarea configurărilor de VLAN

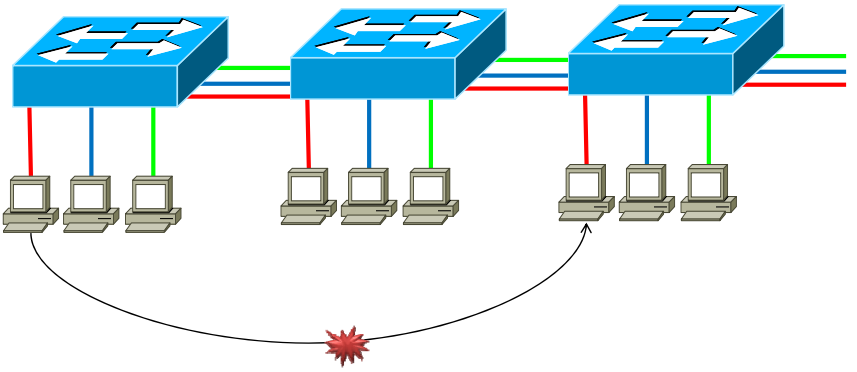
- Lista de VLAN-uri standard (1-1005)
  - salvată în **vlan.dat** în Flash
  - nu se șterg la reset
  - nu se șterg dacă ștergem **startup-config**
- Lista de VLAN-uri extinse (1006 – 4094)
  - salvată în **running-config**
  - se șterg la resetarea configurațiilor

VLAN-urile standard se păstrează la restartarea switch-ului datorită faptului că sunt salvate în fisierul vlan.dat în Flash.

VLAN-urile extinse nu se păstrează în **vlan.dat** ci în **running-config**.

Consistența VLAN-urilor

- Este necesar un drum neîntrerupt între dispozitivele din același VLAN



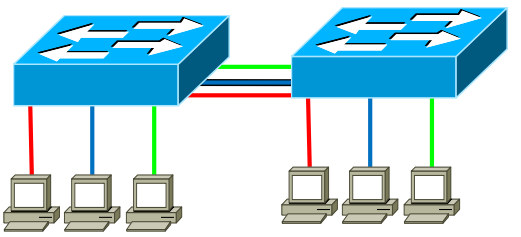
Pentru a obține conectivitate între mai multe stații aflate în același VLAN trebuie să ne asigurăm că toate switch-urile intermediare celor 2 echipamente au configurat VLAN-ul respectiv și pot trimite pachete pe acel segment.

Un switch reține în tabela CAM atât adresa MAC sursă asociată cu portul de intrare, cât și numărul VLAN-ului configurat pe acel port. Când un switch primește un pachet destinat VLAN-ului 100, acesta nu îl va putea trimite decât pe porturile ce sunt configurate să accepte trafic pentru VLAN-ul 100.

Să presupunem că 2 stații aparțin VLAN-ului 100. Dacă pe una dintre legăturile dintre switch-urile intermediare nu este permis acest VLAN, cele două stații nu vor putea comunica.

Scalabilitatea VLAN-urilor

- Pentru fiecare VLAN între două switch-uri se consumă câte două porturi
  - scump
  - nescalabil
- Soluția:
  - **trunking**



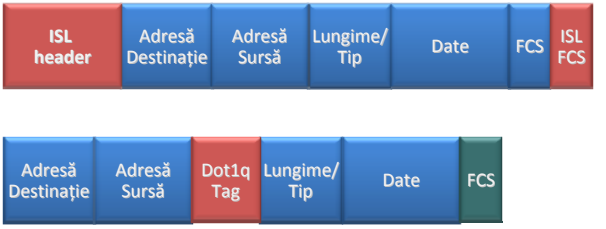
O linie trunk este o legătură point-to-point între 2 dispozitive de rețea ce poate transmite mai mult de un singur VLAN. O linie trunk VLAN îți permite să extinzi VLAN-urile peste o întreagă rețea . Un trunk nu aparține unui VLAN specific, ci este o modalitate de a transmite mai multe VLAN-uri folosind aceleași politici, între switch-uri și rutere.

Astfel, dacă un switch va primi un pachet din VLAN-ul 10, acesta îl va putea comuta atât pe legăturile configurate explicit cu VLAN 10 cât și pe legăturile trunk, care poate transmite informații din toate VLAN-urile.

Folosirea liniilor de trunk aduce avantaje precum costuri reduse ale echipamentelor (switch-urile nu mai necesită un port separat per VLAN), oferă o scalabilitate sporită (adăugarea unui VLAN presupune doar adăugarea acestuia pe liniile de trunk).

Trunking

- Marcarea cadrelor pentru a le ghida prin rețea
  - nivel 2
  - protocoale specializate
- ISL
  - proprietar Cisco
  - încapsulare
- 802.1Q (dot1q)
  - open standard
  - tagging



Când un switch primește un frame pe un port configurat în mod access pentru un anumit VLAN, switch-ul decapsulează frame-ul, inserează un VLAN Tag, recalculează FCS-ul și trimite frame-ul marcat.

Pe liniile de tip trunk există două protocoale specializate ce permit transmitera VLAN-urilor: ISL și 802.1Q.

ISL este actualmente un protocol legacy însă se mai folosește în rețele implementate cu mai mult timp în urmă. Într-un port trunk ce rulează ISL toate pachetele primite trebuie să conțină antet ISL și toate pachetele transmise sunt trimise cu un antet ISL. Frame-urile ce nu sunt marcate și sunt primite pe un trunk ISL sunt aruncate.

Câmpul dot1.q tag conține 3 biți de prioritate, un bit CFI (Canonical Format Identifier - permite transmiterea frame-urilor Token Ring pe acel VLAN) și 12 biți ce reprezintă VLAN ID-ul.

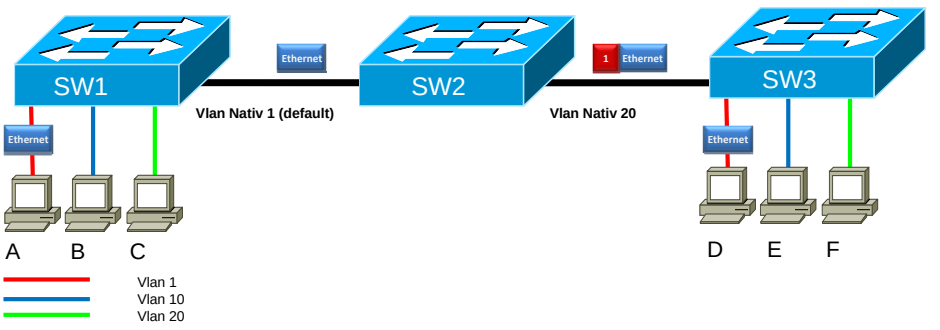
802.1q

- Setat implicit pe unele switch-uri (dacă ISL nu este disponibil)
- Oferă suport pentru maxim 4096 VLAN-uri
- Fiecare legătură trunk are un **VLAN nativ**
  - implicit este VLAN 1
  - cadrele ce aparțin VLAN-ului nativ circulă nemarcate
  - switch-urile de la capătul legăturii trunk trebuie să aibă același VLAN nativ configurat

Protocolul 802.1Q este protocolul folosit actualmente pe toate switch-urile Cisco. Când un pachet urmează a fi trimis pe o linie de tip trunk, acestuia îi este întâi verificat marcajul. Dacă VLAN-ul ce este inclus în acel marcaj este permis pe trunk, pachetul va fi transmis mai departe cu marcajul aferent. În situația în care VLAN-ul nu este permis pe trunk, pachetul va fi aruncat.

Când pe un port trunk este primit un frame nemarcat acel frame este trimis implicit pe VLAN-ul nativ . VLAN-ul nativ standard este VLAN-ul 1.

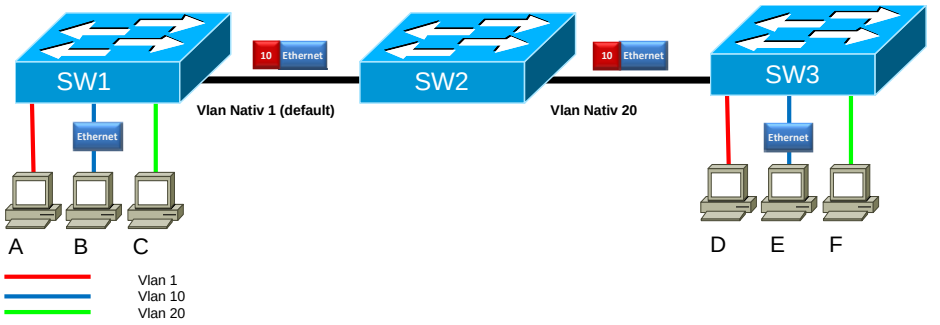
Marcarea folosind dot1q



În această imagine observăm că PC A vrea să trimită un pachet către PC D. A se află în VLAN-ul 1, astfel că pachet-ul Ethernet trimis de PC nu va fi marcat pe legătura dintre SW1 și SW2 deoarece această legătură are ca VLAN nativ VLAN-ul 1. Pe legătura dintre SW2 și SW3 pachetul va fi marcat cu VLAN-ul 1 deoarece VLAN-ul nativ este 20. Odată ajuns pachetul la SW3 acesta va ști să îl trimită PC-ului aflat în VLAN-ul 1 și anume PC-ul D.

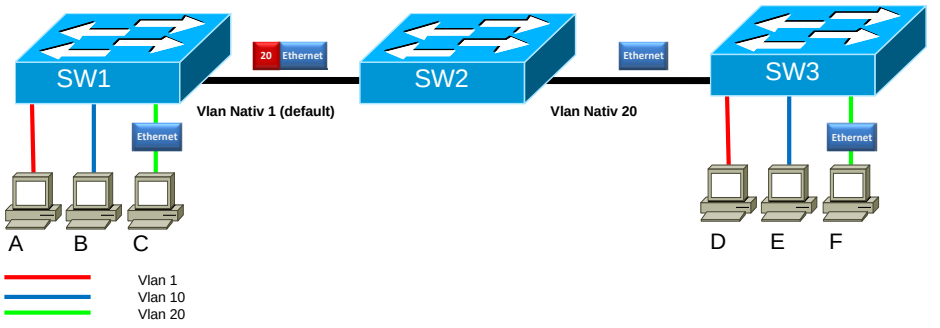
Un pachet destinat VLAN-ului nativ de pe o linie trunk va trece peste acea legătură fără nici un VLAN tag. Pe fiecare legătură trunk existentă poate fi configurat un alt VLAN nativ.

Marcarea folosind dot1q



Spre deosebire de situatia anterioara aici pachetul este trimis de la PC B la PC E , PC-uri ce se afla în VLAN-ul 10. Din aceasta cauza pachetul va circula atat pe link-ul SW1 - SW2 cat și pe SW2 – SW3 marcat cu VLAN-ul 10.

Marcarea folosind dot1q



Această situație este similară primei situații prezentate, numai că de această dată transmisia se realizează între **PC C** și **PC F**, ambele PC-uri fiind în VLAN-ul 20. Din această cauză pachetul va circula marcat pe legătura cu VLAN-ul nativ 1 și nemarcat pe legătura cu VLAN-ul nativ 20.

Crearea unui VLAN

- vlan database
  - scos din uz (probleme de folosire)

```
Sw# vlan database
Sw(vlan)# vlan 20 name Sales
```

- Din modul de configurare

```
Sw(config)# vlan 10
sw(config-vlan)# name Management
```

- La adăugarea unui port

```
Sw(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```


Un mod de configurare a VLAN-urilor ce a devenit actualmente legacy, este folosind comanda VLAN database. Pentru a accesa acest mod se folosea comanda **`vlan database`** din prompt-ul Privileged Exec. În acest mod folosind comanda **`vlan id_vlan name nume_vlan`** se configurează un vlan cu numele corespunzător. La ieșirea din acest mod, se aplicau toate configurațiile cu privire la VLAN-uri ce au fost introduse. Acest mod de configurare a fost înlocuit cu unul mai intuitiv. Crearea unui VLAN se realizează din modul de configurare folosind comanda **`vlan id_vlan`**. În urma executării acestei comenzi suntem introduși într-un mod de configurare de unde putem specifica diverse caracteristici ale VLAN-ului respectiv.

Pentru a asocia unei interfețe un VLAN este folosită comanda **`switchport access vlan vlan_id`** din modul de configurare al interfeței. Pe IOS-urile noi, la executarea acestei comenzi dacă VLAN-ul nu există în baza de date, el este creat automat.

Configurare mod port

- Un port poate fi în mod
  - access
  - trunk
  - dinamic
- **`switchport mode { access | trunk | dynamic }`**

```
Sw(config)# interface f0/1
sw(config-if)# switchport mode access
Sw(config)# interface f0/1
Sw(config-if)# switchport mode trunk
```


Un port pe care este configurat un singur VLAN și care este de obicei configurat pe o interfată către o stație, este un port access. Un port pe care sunt configurate mai multe VLAN-uri este un port trunk.

Porturile aflate în mod dinamic autonegociază modul în care se află portul respectiv folosind protocolul DTP (Dynamic Trunking Protocol). Acesta poate avea următoarele stări pe fiecare port:

- auto: portul dorește pasiv negocierea unui trunk. Portul va deveni trunk dacă portul aflat la capătul opus este configurat cu modul on sau desirable
- on: portul va fi trunk indiferent de modul vecinului
- off: forțează legătura să nu fie trunk, indiferent de modul vecinului
- desirable: portul va dori activ negocierea unui trunk
- nonegociate: portul va fi trunk, dar nu va schimba mesaje DTP

Configurare port access

- Un port access poate aparține unui singur VLAN
- Portul implicit aparține VLAN-ului 1
- **`switchport access vlan VLAN_NO`**

```
Sw(config)# interface f0/1
Sw(config-if)# switchport mode access
Sw(config-if)# switchport acess vlan 10
```


Pe un port aflat în modul access putem seta un singur VLAN. Pentru a configura un port în modul access sunt necesari doi pași.

Primul constă în setarea modului portului folosind comanda **`switchport mode access`** din modul de configurare al interfeței.

Al doilea pas constă în setarea VLAN-ului care este permis pe port folosind comanda **`switchport access vlan`** ***`id_vlan.`*** Implicit VLAN-ul permis pe toate porturile unui switch este vlan-ul 1. Dacă comanda este folosită ulterior folosind alt VLAN, aceasta va suprascrie comanda anterioară.

De obicei acest tip de port este folosit atunci când conectăm echipamente terminale, deoarece acestea fac parte dintr-o singură rețea.

Configurare port trunk

- Un port trunk poate permite anumite VLAN-uri
- Implicit transportă toate VLAN-urile
- **`switchport trunk allow vlans { add, delete, VLAN_LIST }`**

```
Sw(config)# interface f0/1
Sw(config-if)# switchport mode trunk
Sw(config-if)# switchport trunk allowed vlan 1,10,20
```


Un port configurat în modul trunk poate permite mai multe VLAN-uri pe aceeași legătură. Un port se configurează în modul trunk folosind comanda **`switchport mode trunk`**. Implicit un port configurat în modul trunk permite trafic de pe toate VLAN-urile existente pe switch la acel moment.

Pentru a specifica doar VLAN-urile ce se doresc a fi transmise pe o legătură de tip trunk se folosește comanda **`switchport trunk allowed vlan id_vlan`** în modul interfață unde id-urile VLAN-urilor sunt specificate cu virgulă între ele.

Pentru a adăuga un VLAN la lista celor permise pe un anumit port se folosește comanda **`switchport trunk allowed vlan add id_vlan,`** iar pentru a șterge un VLAN se folosește comanda **`switchport trunk allowed vlan delete id_vlan.`**

Comenzi de vizualizare asignare VLAN

- **show vlan [brief]**

```
Sw# show vlan

VLAN Name                 Status    Ports
---- -------------------- --------- ----------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/7, Fa0/8, Fa0/10, Fa0/11
10   Management           active
20   Sales                active
30   VLAN0030             active    Fa0/5, Fa0/6
99   VLAN0099             active
```


Pentru a vedea asocierile dintre VLAN-urile configurate pe un switch și interfețele acestui echipament se folosește comanda **show vlan**. În output-ul rezultat, prima coloană reprezintă id-ul VLAN-ului, a doua coloană definește numele atribuit VLAN-ului, iar a treia coloană specifică starea de functionare a VLAN-ului. În cazul în care VLAN-ul este functional, valoarea câmpului va fi “active”. Ultima coloană reprezintă porturile ce sunt în modul access pentru VLAN-ul respectiv.

În output-ul acestei comenzi nu vor fi afișate interfețele ce se găsesc în modul trunk, deoarece o interfață aflată în acest mod aparține mai multor VLAN-uri în același timp, astfel neputând fi asociată unui singur VLAN.

Un switch pe care nu au fost realizate configurații de VLAN va afișa toate interfețele sale în VLAN-ul 1.

Comenzi de vizualizare trunk-uri

- **show interfaces trunk**

```
S2#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/9       desirable    802.1q         trunking      1
Fa0/12      desirable    802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/9       1-4094
Fa0/12      1-4094

Port        Vlans allowed and active în management domain
Fa0/9       1,10,20,30,99
Fa0/12      1,10,20,30,99

Port        Vlans în spanning tree forwarding state and not pruned
Fa0/9       1,10,20,30,99
Fa0/12      1,10,20,30,99
```


Pentru depanarea problemelor apărute și aflarea informațiilor despre interfețele care se găsesc în modul trunk se folosește comanda **show interfaces trunk** din modul de configurare global config.

Pentru fiecare port este afișat modul în care este configurat, încapsularea folosită, starea de funcționare și VLAN-ul nativ pe respectivul trunk.

În continuarea output-ului este afișată o secțiune care descrie ce VLAN-uri au fost configurate pe fiecare port, ce VLAN-uri sunt active pe fiecare port și la final o listă cu VLAN-urile ce sunt active în urma aplicării algoritmului Spanning-tree.

Rezumat

- VLAN-uri
- Trunking
- 802.1Q

1. Care este numarul maxim de VLAN-uri acceptat de 8021.Q?
2. Cum va traversa un packet apartinand unui VLAN nativ link-ul trunk?
3. Precizati starile protocolului DTP.
4. Ce echipamente sunt necesare pentru comunicarea intre VLAN-uri?
5. Precizati un protocol de trunking proprietar Cisco.