Lucrare de laborator №3.

Configurări VLAN. Configurări Trunk.
Configurarea protocoalelor IPv4/IPv6 și rutării statice.

Un VLAN (prescurtare de la virtual local area network, în română rețea locală virtuală) este un grup de gazde ce pot comunica, indiferent de locația lor fizică, ca și cum s-ar afla în același domeniu de difuzare. Un VLAN are aceleași atribute ca o rețea locală fizică, dar permite stațiilor să nu fie legate în același switch de rețea. Apartenența la un VLAN poate fi configurată la nivelul 3 al stivei OSI, poate fi configurat atit pe rutere cit si pe comutatoare de tip multilayer. În cadrul lucrării date, utilizînd softul aplicativ Cisco Packet Tracer se va modela procesul de Configurarea VLAN-urilor în Cisco IOS.

Scopul: de a]n'elege ce sunt rețelele locale virtuale (Virtual Local Area Networks – VLAN)
Perioada executarii lucrarii de laborator: 90 minute.

Material teoretic: VLAN

VLAN-urile **(Virtual Local Area Network)** ne permit sa separam (din punct de vedere logic) mai multe device-uri (PC-uri, Laptop-uri) conectate la acelasi Switch. Acestea sunt folosite peste tot:

#Ex1: Retea Wireless Guest si Internal; provin de la acelasi Router Wi-Fi dar sunt separate din punct de vedere logic, adica nu poti avea acces din Guest in Internal si nici din Internal in Guest)

#Ex2: in toate companiile medii si mari unde se doreste o separare a traficului din mai multe departamente (exemplu: departamentul de IT (ex: VLAN 45) nu va putea accesa toate resursele din departamentul de Marketing (ex: VLAN 91))

Un VLAN = O Retea = Un Domeniu de Broadcast

Asadar un VLAN reprezinta o retea. Daca alegem sa creeam 2 VLAN-uri, inseamna ca vom avea 2 retele diferite (asadar si 2 domenii de Broadcast).
VLAN-urile sunt folosite peste tot in marile companii. Da-mi voie sa-ti dau cateva exemple:

#Ex1: Reteaua Wireless **Guest** si **Internal**; provin de la acelasi Router Wireless, dar sunt separate din punct de vedere logic. Asta inseamna ca, by default, nu poti avea acces din reteaua Guest in reteaua Internal si nici invers.

NOTA: Deci astfel obtinem o separare dpvd. logic care duce la **segmentare** si la o crestere a **nivelului** de **securitate** din retea.

#Ex2: in toate companiile medii si mari unde se doreste o separare dispozitivelor pe departamentele companiei (exemplu: departamentul IT (ex: VLAN 45) nu va putea accesa toate resursele din departamentul Marketing (ex: VLAN 91))

NOTA: pentru a identifica diferite departamente, VLAN-urile folosesc un ID (un numar de identificare) unic caruia ii poate fi asociat un nume (pentru identificarea mult mai usoara).

Astfel, ID-ul unui VLAN poate fi in urmatoarele categorii:

- **Standard** VLAN ID – **1 – 1005**
- **Extended** VLAN ID – **1006 – 4094**

Dupa cum poti vedea exista si un range extended de ID-uri care a fost adaugat ulterior, dupa crearea standardului pentru VLAN-uri, scopul acestui range fiind pentru extinderea numarului total de VLAN-uri care pot exista pe un Switch cat si pentru folosirea aplicatilor de rutare pe Switch-uri de nivelul 3.

Tehnologia VLAN-ul este un standard in industrie si este identificata prin **IEEE 802.1q**. Asta face ca tehnologia sa fie disponibila pe toate echipamentele de retea (a vendorilor precum Juniper, Huawei, HP etc.) si nu doar pe echipamentele Cisco.

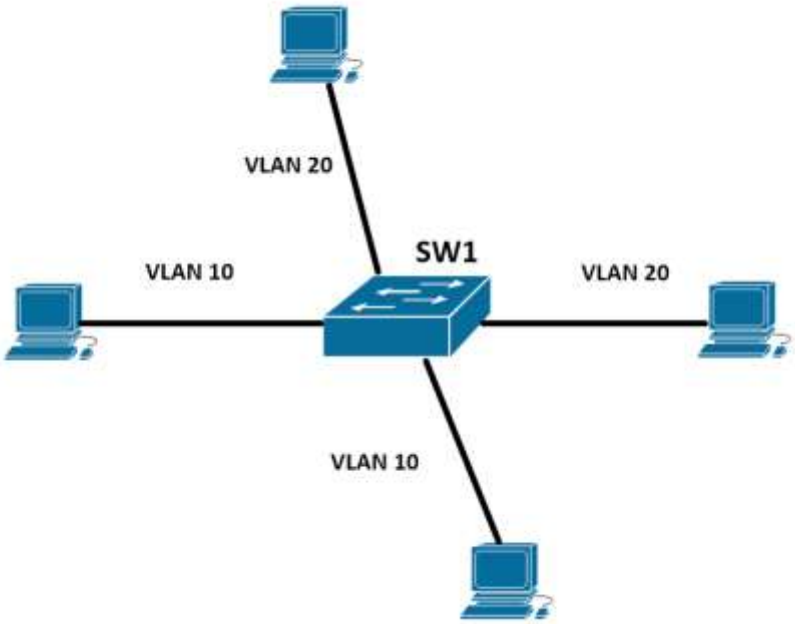

Figura 3

Iata in figura 3 o reprezentare mai clara a PC-urilor care pot comunica intre ele. Astfel, dupa cum se vede, doar PC-urile din acelasi VLAN pot comunica intre ele.

Toate echipamentele sunt conectate fizic la acelasi Switch, dar dpvd. logic ele sunt separate. De ce? Pentru ca Switch-ul adauga un tag (eticheta) care specific clar faptul ca doar echipamentele care au acelasi tag (aka. VLAN ID) pot comunica intre ele (in acest scenariu, doar PC-urile din cercul verde, respectiv cele din cercul rosu).

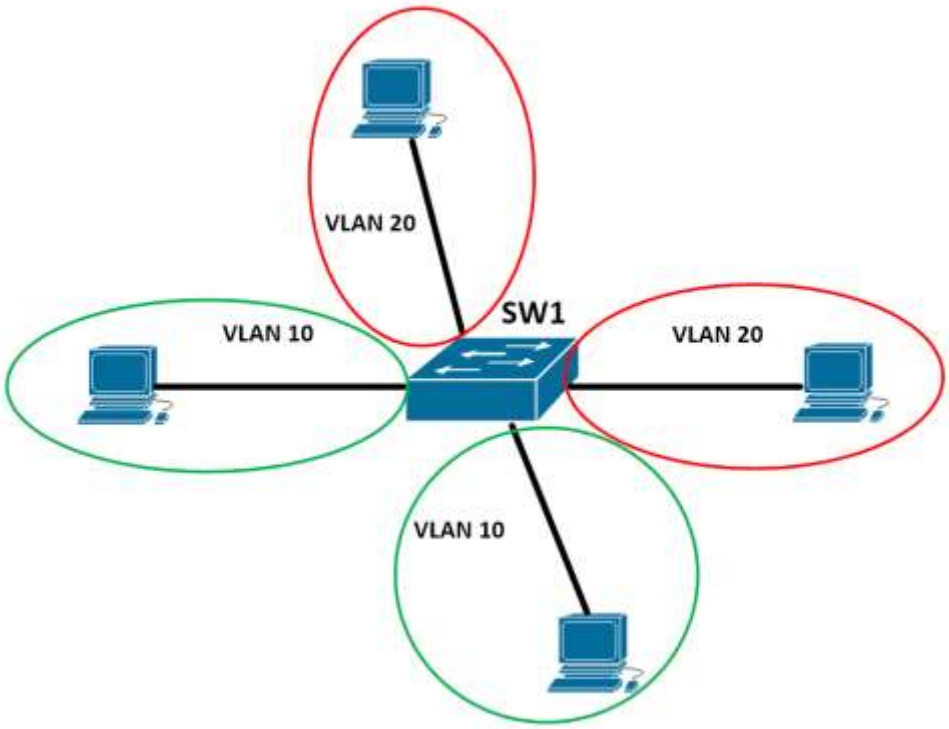

Figura 4

Beneficiile VLAN-urilor:

1. *Securitate* – separarea retelelor la nivel logic
2. *Design mai bun* – impartirea unei companii in departamente (fiecare departament reprezentand cate un VLAN (Retea))
3. *Cresterea Performantei*
4. *Scalabilitate* – se pot adauga foarte usor alte VLAN-uri fara a impacta fluxul retelei

Acestea sunt **reprezentate** printr-un **ID** (un numar de la 1 – 4094). Pe Switch-urile Cisco exista cateva ID rezervate, care nu pot fi utilizate, acestea fiind (1, 1002 – 1005):

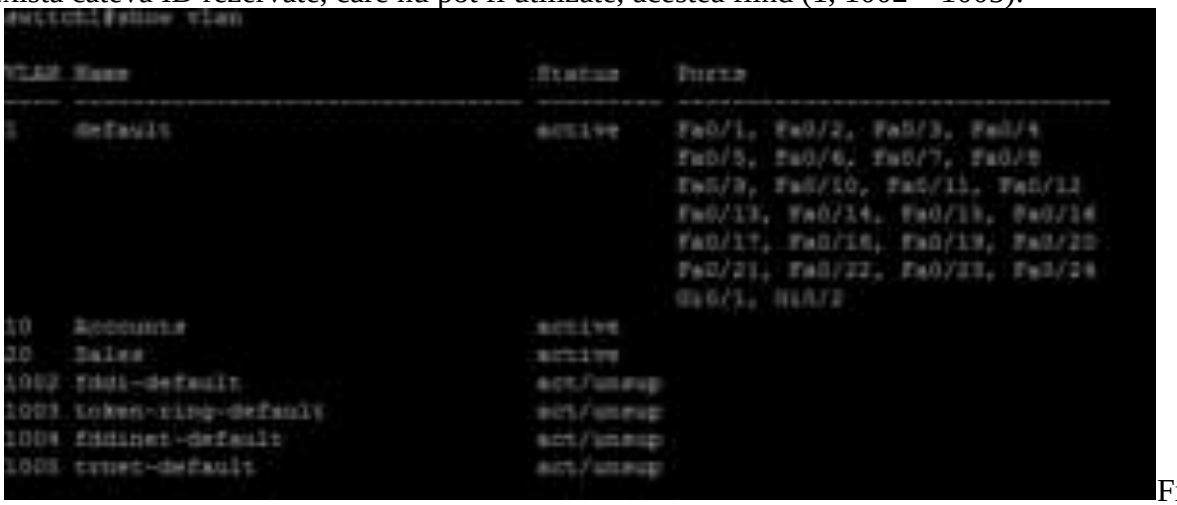

Figura 5

Lucrarea practica 1-1.
VLAN de management

Rețelele locale virtuale (*Virtual Local Area Networks* – VLANs) sunt moduri de a realiza o separație logică a unei rețele locale (LAN) în mai multe subrețele pe aceeași infrastructură fizică. Separația este realizată la nivelul Legătură de Date prin introducerea unui câmp suplimentar în antetul de nivel 2. VLAN-urile sunt identificate în cadrul frame-ului printr-un VLAN ID.

Configurarea VLAN-urilor se realizează pe switch-uri, mai exact pe interfețele/porturile switch-urilor. Stațiile nu au cunoaștere despre existența unor VLAN-uri; perspectiva lor este aceea a unei rețele locale, adică rețeaua virtuală aferentă unui VLAN ID. O stație se va găsi în VLAN-ul specific portului la care este conectată (configurație existentă pe switch).

În topologia Packet Tracer <lab03_introducere-vlan.pkt>[1] stațiile [PC0] și [PC2] fac parte din [VLAN 10], iar stațiile [PC1] și [PC3] din [VLAN 20]. Observați că pot comunica doar două câte două, deși adresele lor IP sunt din același spațiu de adrese.

Configurarea celor două VLAN-uri a fost realizată pe switch-ul [Switch0]. Pentru a investiga configurația de VLAN-uri de pe switch-ul [Switch0], rulați comenzile de mai jos și urmăriți output-ul acestora. Pentru a accesa intefața de configurare a switch-ului, urmații pașii:

1. Dați click pe [switch].
2. Accesați tab-ul [CLI].
3. Apăsați tasta [Enter] pentru a apărea promptul de transmitere de comenzi pentru switch.
4. Folosiți comanda [enable] (urmată de apăsarea tastei [Enter]) pentru a accesa modul privilegiat de configurare a switch-ului.

Afișați configurația vlan-urilor.

Urmăriți că VLAN-ul cu ID-ul 10 (denumit “zece”) conține porturile [Fa0/1] și [Fa2/1] adică porturile aferente stațiilor [PC0] și [PC2]. La fel, VLAN-ul cu ID-ul 20(denumit “douăzeci”) conține porturile [Fa1/1] și [Fa3/1] adică porturile aferente stațiilor [PC1] și [PC3].
Afisati configurația curentă. Din output-ul comenzii observați că porturile sunt configurate în modul acces în VLAN-urile respective.

În topologia Packet Tracer <lab03_de-ce-vlan.pkt>[2] se află o rețea cu un switch (Switch0) și trei stații. Toate stațiile sunt conectate una la cealaltă și inclusiv la switch-ul [Switch0] (și switch-ul are adresă IP).

În Cisco IOS primul pachet trimis poate să nu fie de fapt trimis din cauza absenței tabelei ARP. De aceea când trimiteți un pachet în Packet Tracer la sau de la switch, prima oară nu va funcționa. Următoarele pachete, însă, vor funcționa.

În general un switch poate fi configurat direct în consola acestuia sau de la distanță conectându-vă la switch folosind comanda [telnet] urmată de adresa IP a acestuia. Conectați-vă la switch-ul [Switch0] de pe fiecare dintre cele 3 stații urmând pașii:

1. Dați click pe stație.
2. Alegeți tab-ul [Desktop].

[1] https://drive.google.com/file/d/1rXxLdxHHC0T6zehf8DdsnDI4-MRkKdrF/view?usp=sharing
[2] https://drive.google.com/file/d/1Hq3GUmg9vOhnd4axpB1W6A9oDe9h3n2J/view?usp=sharing

3. Dați click pe icon-ul [Command prompt].
4. Executați comanda: [telnet 192.168.1.254].

unde 192.168.1.254 este adresa IP a switch-ului.

Observați că vă puteți conecta la switch-ul [Switch0] de pe oricare stație.

Dorim să securizăm accesul la switch-ul [Switch0], permițând doar stației [Management] să se conecteze la acesta. Pentru acest lucru vom configura un nou VLAN, având ID-ul 100; din acest VLAN va face parte doar stația [Management]. Deseori acest VLAN poartă numele de "*VLAN de management"*.

Pentru a configura un VLAN pe un port al switch-ului, urmăm pașii:

1. În consola de configurare activam modul privilegiat (folosiți parola "student").
2. Intrăm în modul de configurare.
3. Creăm VLAN-ul cu ID-ul 100: {vlan 100}
   - Opțional putem configura și un nume pentru VLAN, să zicem "management".
4. Intrăm în modul de configurare al interfației relevante.
5. Configurăm interfața/portul pentru modul acces.
6. Configurăm pe interfața de tip acces numărul VLAN-ului.

În acest moment stația [Management] se află în VLAN-ul 100. Trebuie să configurăm și switch-ul pentru a răspunde cererilor de configurare tot pe VLAN-ul 100. Pentru a putea fi configurat corespunzător, unui switch i se pot crea interfețe virtuale de forma [vlan X], unde X este numărul VLAN-ului de pe care poate fi accesat în vederea configurării. Interfața implicită pentru orice switch este [vlan 1] pe care va trebui să o dezactivăm și să ștergem adresa. IP

Vom configura adresa IP pe interfața [vlan 100] aferentă VLAN-ului 100.

După această configurare, switch-ul [Switch0] va fi accesibil la adresa IP [192.168.1.254] doar de pe stația [Management]. Folosiți comanda [telnet 192.168.1.254] din interfața [CLI] a fiecărei stații pentru a verifica faptul că vă puteți conecta sau nu la switch-ul [Switch0]. Observați că doar de pe stația [Management] poate fi realizată conectarea.

Conectivitatea între stații s-a păstrat. Nu a fost afectată de configurarea VLAN-ului de management.

Lucrarea practica 1-2.
Porturi în modul acces

În topologia Packet Tracer <lab03_vlan-access.pkt>[3] se află o rețea cu un switch, o stație de management și 4 stații (PC1, PC2, PC3, PC4) folosite de utilizatori. Observați că cele 4 stații pot comunica între ele fiecare cu fiecare.

Dorim să izolăm PC1 și PC3 de celelalte două stații (PC2 și PC4) astfel încât PC1 să poată comunica doar cu PC3. Acest lucru se poate realiza configurând porturile aferente lui PC1 și PC3 să facă parte din VLAN-ul 10, iar porturile aferente lui PC2 și PC4 să facă parte din VLAN-ul 20. Vom crea cele două VLAN-uri:

```
Switch0>enable
Password:
```

[3] *https://drive.google.com/file/d/1kG9a-X3olxagYjZyCXqBPtvdIkG6WFh7/view?usp=sharing*

```
Switch0#configure terminal
Switch0(config)#vlan 10
Switch0(config-vlan)#name zece
Switch0(config-vlan)#exit
Switch0(config)#vlan 20
Switch0(config-vlan)#name douazeci
Switch0(config-vlan)#exit
```

Putem verifica adăugarea celor două VLAN-uri prin rularea comenzii show vlan brief. Comanda poate fi rulată și din modul de configurare dacă este prefixată de comanda do:

```
Switch0(config)#do show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa1/1, Fa2/1, Fa3/1, Fa4/1
                                                 Fa5/1, Fa6/1, Fa7/1
10   zece                              active
20   douazeci                          active
100  VLAN0100                          active    Fa0/1
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Se observă adăugarea celor două noi VLAN-uri: 10 și 20.

După ce am creat VLAN-urile în baza de date a switch-ului, trebuie să configurăm porturile să facă parte din acest VLAN-uri, după cum urmează:

- Fa1/1 - PC1 - VLAN 10
- Fa2/1 - PC2 - VLAN 20
- Fa6/1 - PC3 - VLAN 10
- Fa3/1 - PC4 - VLAN 20

Înainte de a fi configurate VLAN-urile porturile trebuie trecute în mod acces. Comenzile care trebuie rulate sunt cele de mai jos:

```
Switch0#configure terminal
Switch0(config)#interface fa1/1
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 10
Switch0(config-if)#exit
Switch0(config)#interface fa2/1
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 20
Switch0(config-if)#exit
Switch0(config)#interface fa6/1
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 10
```

```
Switch0(config-if)#exit
Switch0(config)#interface fa3/1
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 20
Switch0(config-if)#exit
```

Pentru a verifica adăugarea porturilor în VLAN-uri, folosim, din nou, comanda [show vlan brief]:

```
Switch0(config)#do show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa4/1, Fa5/1, Fa7/1
10   zece                              active    Fa1/1, Fa6/1
20   douazeci                          active    Fa2/1, Fa3/1
100  VLAN0100                          active    Fa0/1
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch0(config)#
```

Se poate observa că VLAN-ul 10 conține porturile Fa1/1 și Fa6/1, iar VLAN-ul 20 conține porturile Fa2/1 și Fa3/1, așa cum am dorit.

Verificați conectivitatea între fiecare pereche de două stații. Observați faptul că doar stațiile din același VLAN pot să comunice între ele.

Lucrarea practica 1-3.
Subnetare și VLAN-uri

În topologia Packet Tracer <lab03_subnetare-vlan.pkt>[4] s-am mai adăugat un switch (Switch1) la care au fost conectate alte 4 stații (PC5, PC6, PC7, PC8). Configurați switch-ul Switch1 astfel încât PC5 și PC7 să facă parte din VLAN-ul 10, iar celelalte 2 (PC6 și PC8) din VLAN-ul 20.

Împărțiți spațiul 172.16.234.96/27 în două subrețele de dimensiuni egale și configurați stațiile (PC1, PC3, PC5, PC7) din VLAN-ul 10 cu adrese IP din prima subrețea obținută, iar cele din VLAN-ul 20 (PC2, PC4, PC6, PC8) cu adrese IP din a doua subrețea.

Verificați conectivitatea între stațiile din același VLAN, două câte două, precizând de ce nu funcționează atunci când este cazul.

Nu verificați conectivitatea între două stații din switch-uri diferite întrucât între aceste switch-uri NU există legătură fizică.

Lucrarea practica 1-4.
Legătură de tip trunchi (trunk)

[4] https://drive.google.com/file/d/1x6LjPBOFYuMIYT-5bVNTyZ82aHNQRQGP/view?usp=sharing

Pe topologia <lab03_subnetare-vlan.pkt>[5], realizați o legătură de fibră între switch-urile [Switch0] și [Switch1] pe portul [Fa4/1] al fiecărui switch. Testați conectivitatea între stații din același VLAN, dar switch-uri diferite. Observați că nu există conectivitate din cauză că nu există nici un mecanism activat prin care VLAN-urile de pe switch-uri diferite să comunice între ele.

Pentru a permite conectivitatea între stații aflate în același VLAN dar conectate switchuri diferite, trebuie să configurăm legătura dintre switch-uri în mod trunchi (*trunk*); această legătură permite încapsularea pachetelor cu VLAN-uri diferite. Identificați numărul portului de interconectare pe fiecare din switch-uri. Pe fiecare switch, intrați pe interfața aferentă și setați legătura în mod trunchi.

Pe switch-ul [Switch0] configurați interfața [Fa4/1]:

```
Switch0>enable
Password:
Switch0#configure terminal
Switch0(config)#int fastEthernet 4/1
Switch0(config-if)#switchport mode trunk
Switch0(config-if)#switchport trunk allowed vlan all
Switch0(config-if)#
```

Pe switch-ul [Switch1] configurați interfața [Fa4/1]:

```
Switch1>enable
Password:
Switch1#configure terminal
Switch1(config)#int fastEthernet 4/1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk allowed vlan all
Switch1(config-if)#
```

Investigați configurația de tip trunk prin rularea comenzii {show interfaces trunk} pe ambele switch-uri:

```
Switch0#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa4/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa4/1       1-1005

Port        Vlans allowed and active in management domain
Fa4/1       1,10,20,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa4/1       1,10,20,100
Switch0#

Switch1#show interfaces trunk
```

[5] https://drive.google.com/file/d/1x6LjPBOFYuMIYT-5bVNTyZ82aHNQRQGP/view?usp=sharing

```
Port      Mode       Encapsulation  Status        Native vlan
Fa4/1     on         802.1q         trunking      1

Port      Vlans allowed on trunk
Fa4/1     1-1005

Port      Vlans allowed and active in management domain
Fa4/1     1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa4/1     1,10,20
Switch1#
```

Se observă că interfața [Fa4/1] este o interfață de tip trunk care transportă VLAN-urile 1 (cel implicit), 10 și 20. În cazul switch-ului [Switch0] transferă și VLAN-ul de management (100). Aceasta se întâmplă întrucât ultimul argument al comenzii {switchport trunk …} a fost {all}, reprezentând toate VLAN-urile.

Verificați că stațiile din același VLAN pot comunica între ele indiferent de switch-ul la care sunt interconectate.

Lucrarea practica 1-5.
Extindere VLAN de management

În topologia configurată <lab03_subnetare-vlan.pkt>[6], dorim să putem configura și switch-ul [Switch1] de pe stația [Management].

Adică switch-ul [Switch1] trebuie să fie accesat prin [telnet] de pe stația [Management].

Pentru aceasta configurați adresa IP {192.168.1.252} pe switch-ul [Switch1] pe interfața aferentă VLAN-ului de management (vlan 100).

Trebuie să creați VLAN-ul 100. Nu este suficient să configurați interfața aferentă (vlan 100).

Testați prin conectarea prin {telnet} de pe stația [Management] la [Switch1].

Salvați topologia rezolvată si prezentati atasat raportului privind realizarea lucrarii de laborator

[6] https://drive.google.com/file/d/1x6LjPBOFYuMIYT-5bVNTyZ82aHNQRQGP/view?usp=sharing