Lucrarea de laborator N2
Rețele locale virtuale VLAN (Virtual LAN)

Scopul principal al acestei lucrări este de a forma abilitățile necesare pentru configurarea rețelelor locale virtuale VLAN.

Obiective:

- A explica conceptul de VLAN și a ilustra serviciile oferite de tehnologia VLAN în Cisco Packet Tracer
- A arăta modul de configurare a VLAN-urilor în rețelele ce constau din host-uri și switch-uri
- A arăta modul în care este implicat routerul pentru a asigura comunicarea între VLAN-uri și accesul la Internet
- A ilustra modul în care este utilizat switch-ul de nivel 3 pentru a asigura comunicarea între VLAN-uri

Tehnologia VLAN

I. Inițial vom considera următoarea configurație de rețea formată doar din host-uri și switch-uri (a se vedea Figura 1):

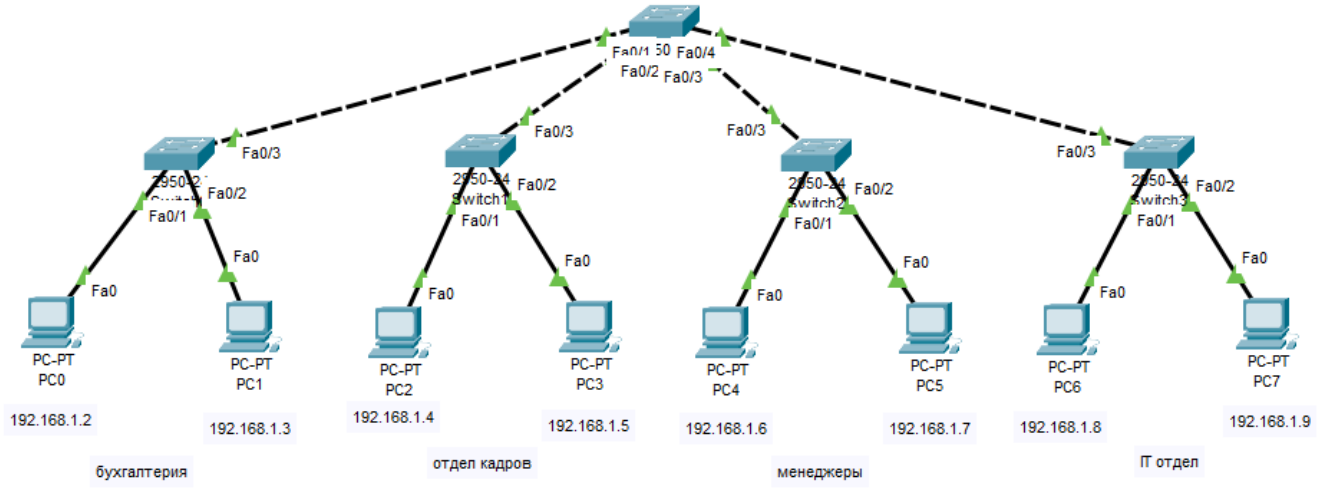


Figura 1

Toate host-urile (din departamente) se află în aceeași subrețea 192.168.1.0/24, care formează un domeniu broadcast. Dacă un host din Contabilitate va încerca să contacteze un alt host (de exemplu, host-ul cu adresa IP 192.168.1.9), atunci frame-ul broadcast va fi trimis către toate switch-urile și către toate host-urile. Dacă trecem în modul de simulare, atunci ne putem convinge că în mare parte switch-urile procesează nu traficul dintre utilizatori (datele utile), ci pachetele broadcast. Numărul mare de pachete broadcast (de la protocoalele ARP, DHCP și altele) va încărca rețeaua.
Fiecare host generează în mod constant frame-uri broadcast, care ajung la toate host-urile din respectivul domeniu broadcast.
Dacă se vaq întâmpla o furtună broadcast => procesorul switch-ului va procesa frame-urile broadcast prea mult timp și la un anumit moment rețeaua nu va mai funcționa.

II. *Schema în care pe fiecare switch avem definit un singur VLAN*
Avem ca scop să formăm grupuri izolate, astfel încât host-urile din Contabilitate (la fel și cele din departamentul Cadre, departamentul Managerial și departamentul IT) să schimbe date doar în grupul lor (inclusiv și pachetele broadcast să rămână în subrețeaua lor), iar host-urile din exterior să nu aibă acces la acestea. Astfel, se urmărește ca departamentele la nivelul informației transmise între host-uri să fie izolate între ele.

În acest sens există două probleme:

- În configurația actuală, când toate host-urile se află într-o singură rețea, nu există vreun obstacol pentru ca host-urile dintr-un departament să transmită date către host-uri din oricare alt departament (a se vedea Figura 1).
- Din cauza pachetelor broadcast avem canale aglomerate.

=> pentru a depăși aceste două probleme a fost inventată tehnologia VLAN

a) Prima idee este să plasăm host-urile din departamente în subrețele separate (a se vedea Figura 2):
Contabilitate - subrețeaua 192.168.2.0/24
Resurse umane - subrețeaua 192.168.3.0/24
Administratori - subrețeaua 192.168.4.0/24
Departamentul IT - subrețeaua 192.168.5.0/24

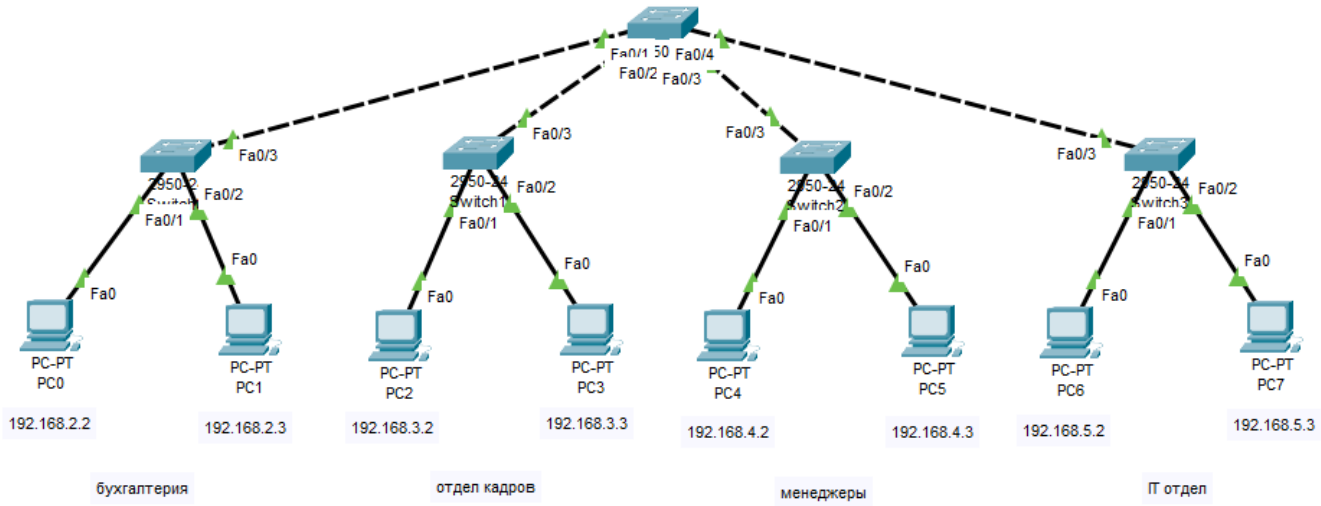


Figura 2

Dacă dăm un ping, de exemplu, de pe host-ul PC0 către PC1, care se află în aceeași subrețea, atunci solicitarea ARP broadcast se va răspândi în toate subrețelele. Pachetul broadcast ajunge la Switch 4 (switch-ul central), apoi la Switch1, Switch2 și Switch3 și la host-urile care sunt conectate la acestea (treceți în modul de simulare și verificați acest lucru). Dacă se instalează un router în loc de switch-ul Switch4, atunci se va limita propagarea pachetelor broadcast în limitele subrețelei. Totuși, utilizarea unui router numai pentru a uni câteva subrețele este irațională, deoarece în cazul examinat avem nevoie de patru interfețe pe router, iar modulele pentru interfețele routerului sunt costisitoare.

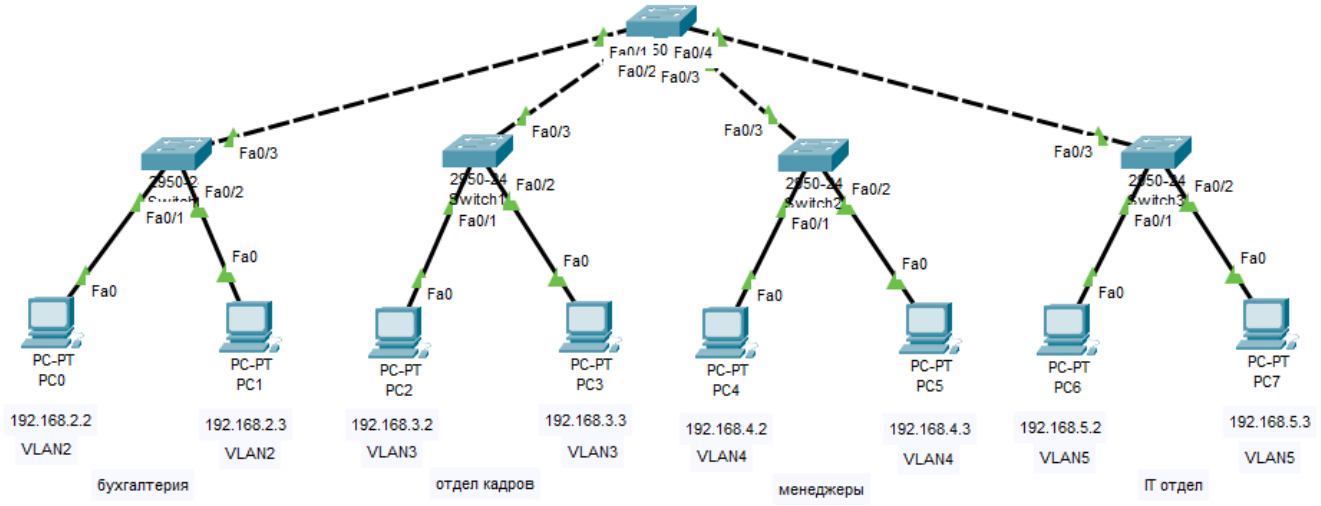


Figura 3

Dacă creăm pentru host-urile din fiecare departament propriul VLAN (a se vedea Figura 3), atunci pachetele broadcast nu vor ieși din VLAN-ul în care au fost generate. Dacă dăm un ping, de exemplu, de pe PC0 către PC1, atunci solicitarea ARP broadcast, pe lângă PC1, va fi trimisă și la Switch4, iar de acolo - la Switch1, Switch2 și Switch3. Acest lucru se datorează faptului că în VLAN 2 pot exista host-uri care nu sunt conectate direct la Switch0, ci prin alte switch-uri. În acest caz, switch-urile Switch1, Switch2 și Switch3 vor renunța la pachetele ARP, deoarece nu vor găsi pe porturile lor careva legături la host-urile din VLAN 2.
Ulterior, vom putea înlocui Switch4 cu un router pentru a asigura legătura între VLAN-uri, dar acest lucru va fi în continuare ineficient, deoarece vor fi utilizate 4 interfețe de router, al căror cost este semnificativ.
Astfel, aplicarea tehnologiei VLAN asigură:

- Segmentarea logică a rețelei
- Un anumit nivel de securitate
- Limitarea dimensiunii traficului broadcast

Dispozitivele aceluiași VLAN aparțin aceleiași subrețele => fiecare departament formează un VLAN separat și o subrețea
Dimensiunea traficului broadcast este în limitele unui VLAN
Traficul broadcast de la primul VLAN nu ajunge în VLAN-urile doi, trei etc. => în acest mod rețeaua este mai puțin încărcată
Host-urile din VLAN2 nu au acces la host-urile din VLAN3, VLAN4 și VLAN5.
În Figura 3 am examinat schema în care fiecare VLAN este deservit de propriul switch.

Rețeaua virtuală reprezintă un grup de host-uri din rețea al căror trafic (inclusiv pachetele broadcast) de la nivelul legătură de date, este complet izolat de alte host-uri din rețea. Aceasta înseamnă că este imposibilă transmiterea frame-urilor între diferite rețele locale virtuale în baza adresei de la nivelul legătură de date (adresa MAC), indiferent de tipul de adresă - unicast, multicast sau broadcast. În același timp, în cadrul rețelei virtuale, frame-urile sunt transmise conform tehnologiei de comutare, adică numai către portul asociat adresei MAC a destinației.
Din cele menționate rezultă că rețeaua virtuală formează un domeniu broadcast.
Scopul tehnologiei VLAN este de a facilita crearea de rețele izolate, care ulterior por fi conectate prin intermediul routerelor, care la nivelul rețea implementează protocolul IP. Acest design de rețea creează bariere serioase în calea traficului broadcast de la o rețea la alta.
Tehnologia rețelelor virtuale creează un fundament pentru construirea unor rețele mari. Astfel, folosind unele aplicații software, pe switch-uri sunt configurate VLAN-uri, iar acestea din urmă sunt conectate între ele prin intermediul routerelor.
Aplicarea pe switch-uri a tehnologiei de rețea virtuală VLAN rezolvă problema izolării reciproce a rețelelor, care permite gestionarea drepturilor de acces ale utilizatorilor și crează bariere în fața furtunilor broadcast.

III. *Schema în care switch-ul poate gestiona mai multe VLAN-uri* (a se vedea Figura 4)
Pachetul broadcast generat în VLAN2 se va transmite prin switch-uri spre toate host-urile ce se află în VLAN2 (și doar acolo).

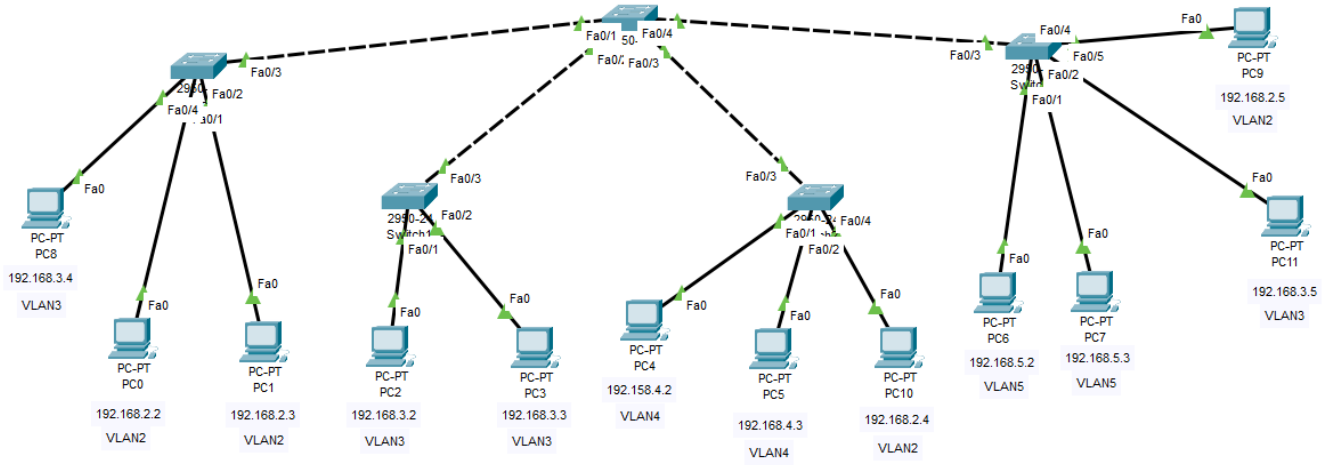


Figura 4

Ceva mai târziu vom reveni și vom arăta cum sunt create VLAN-uri pentru rețeaua prezentată în Figura 4. Deocamdată, vom analiza unele exemple mai simple.

IV. În primul rând, vom arăta printr-un exemplu de ce sunt necesare VLAN-urile dacă furtuna broadcast poate fi limitată prin divizare în subrețele. Să considerăm configurația de rețea din Figura 5.

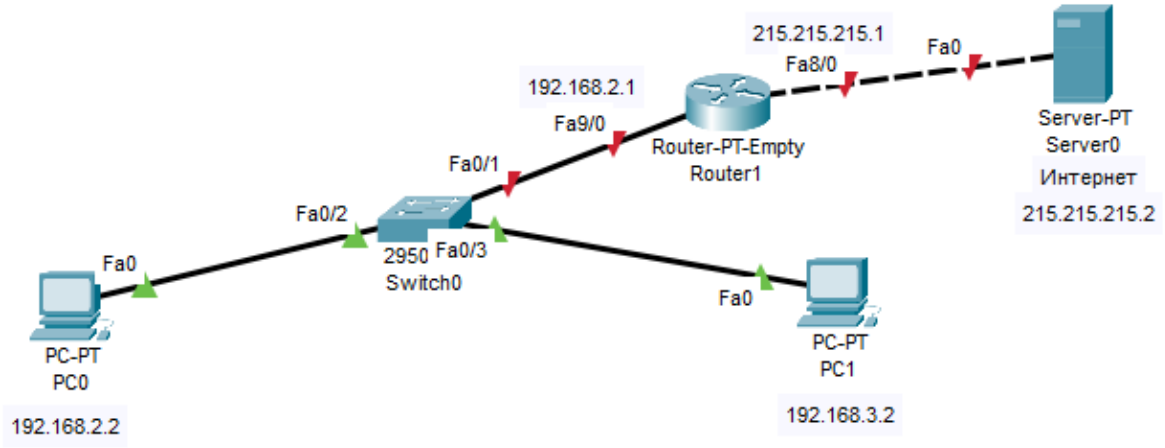


Figura 5

În cadrul rețelei este utilizat un router de model Router-PT-Empty, care presupune adăugarea manuală a modulelor de interfață. Intenționăm să adăugăm 3 module la acest router. Pentru aceasta, dăm un click pe router -> Physical-> Physical Device View și mutăm în dreapta glisorul astfel încât să vedem butonul de oprire/pornire. Dăm un click pe acest buton pentru a stopa funcționarea routerului, după care selectăm, de exemplu, modulul de tip PT-Router-NM-1CFE și îl tragem de trei ori peste sloturile de port. Apăsăm butonul de pornire. După aceasta conectăm deja routerul cu serverul și cu switch-ul.

Pe server setăm IP-ul 215.215.215.2 și adresa de gateway 215.215.215.1.

Pe interfața routerului Fa 8/0 din partea serverului, setăm IP-ul 215.215.215.1, iar pe interfața Fa 9/0 din partea switch-ului - 192.168.2.1 (nu uităm să punem bifa la On - activăm interfața).

Pe host-uri setăm IP-ul 192.168.2.2 și, respectiv, 192.168.3.2.

Apoi, precizăm adresele de gateway pe host-uri. Aici și intervine problema noastră. Pe host-ul cu IP-ul 192.168.2.2 setăm adresa de gateway 192.168.2.1, care este setată și pe interfața corespunzătoare a routerului. Ce gateway ar trebui să instalăm atunci pe PC1? Ar trebui să fie 192.168.3.1, dar pe interfața routerului deja este fixată adresa IP 192.168.2.1 ??????

Există două soluții:

1) se pot utiliza două fire ce conectează două porturi ale switch-ului, corespunzător la două interfețe ale routerului. Pe interfața Fa 9/0 se va seta IP-ul 192.168.2.1, iar pe interfața Fa 7/0 - 192.168.3.1 (a se vedea Figura 6). Pe host-ul PC1 se va seta adresa de gateway - 192.168.3.1.

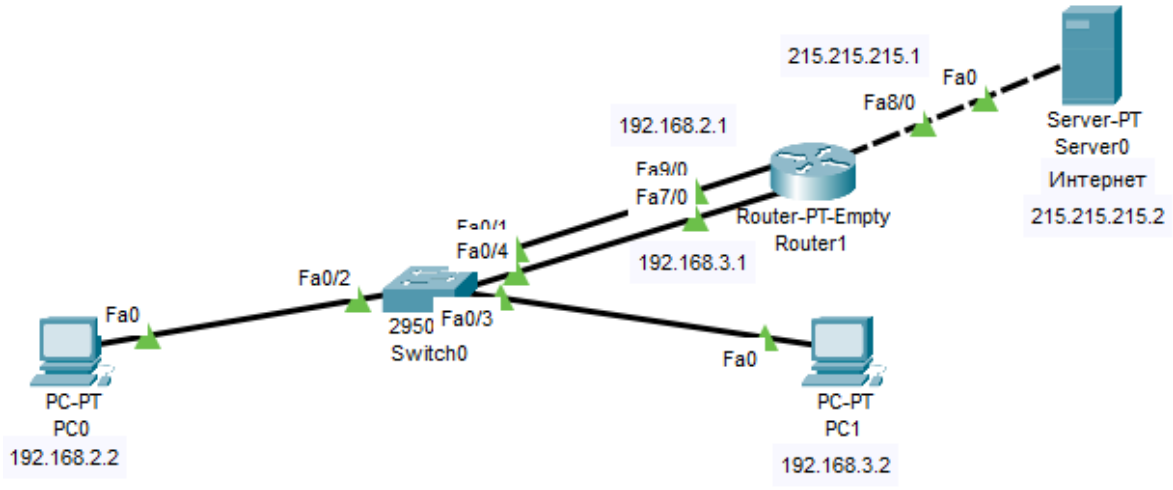


Figura 6

Verificăm conexiunea cu serverul de Internet de pe host-ul PC0 – ping 215.215.215.2 => este conexiune
Verificăm conexiunea cu serverul de Internet de pe host-ul PC1 – ping 215.215.215.2 => este conexiune

Dar totuși există un mare dezavantaj. Dacă switch-ul va conecta, de exemplu, 50 de subrețele => vor fi necesare 50 de cabluri și, cel mai important, 50 de interfețe de router (adică, de fapt, câteva routere). Dacă se ține cont că modulul pentru interfața de router Cisco costă nu mai puțin de 8000 de lei, atunci putem ușor deduce că vom avea cheltuieli semnificative
2) A doua soluție este bazată pe utilizarea VLAN-urilor. Dacă host-ul PC0 este inclus în VLAN2, iar PC1 în VLAN3, atunci în baza unei interfețe fizice de router și a unui singur cablu vom putea accesa Intrenet-ul
V. *Detalii privind configurarea VLAN-urilor*
În continuare vom prezenta modul în care sunt configurate VLAN-urile
În anul 1998 a fost adoptat standardul IEEE 802.1q, care stabilește regulile de bază utilizate în construcția rețelelor locale virtuale VLAN, reguli care nu depind de protocolul de nivel legătură de date utilizat la nivelul switch-ului.

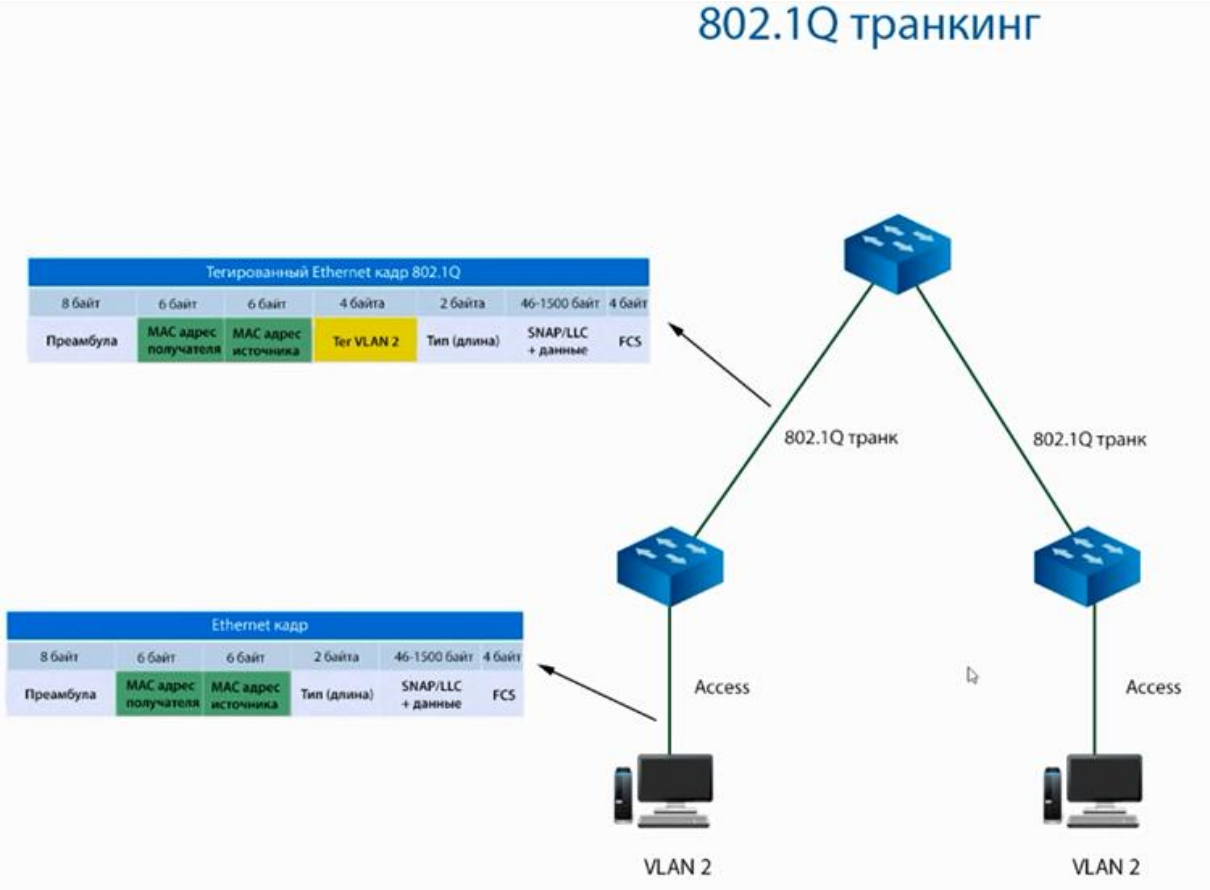
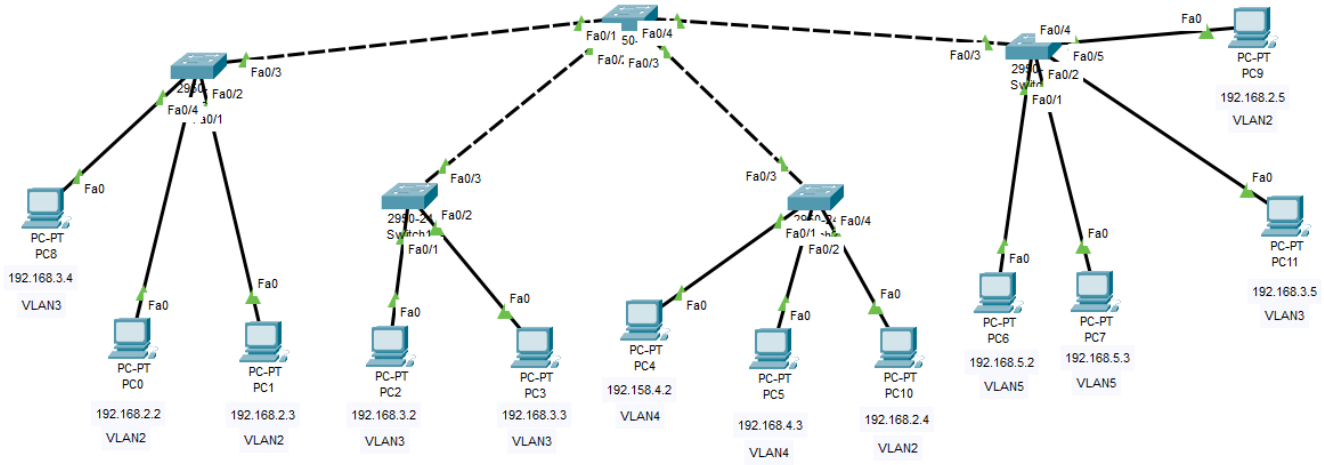


Figura 7

Conexiunea dintre switch și host este numită legătură Access. Conexiunea dintre două switch-uri sau dintre switch și router este numită legătură Trunk. Atunci când un frame trimis de un careva host ajunge pe portul de tip Access al switch-ului, pentru a fi transferat printr-o legătură de tip Trunk, în cadrul frame-ului este inserată o etichetă numită teg. Atunci când frame-ul cu teg ajunge la un switch și urmează a fi transferat printr-o legătură de tip Access, switch-ul elimină teg-ul corespunzător.
Astfel, prin porturile de tip Trunk se transmit frame-uri cu teg, iar prin porturile de tip Access – frame-uri standard fără teg.
În rețeaua din Figura 7 host-ul din stânga constituie un frame Ethernet standard (host-ul nu știe că se află în careva VLAN) pe care îl transmite switch-ului. Switch-ul stabilește că a recepționat un frame din VLAN2 și formează un frame Ethernet cu teg, pe care îl transmite printr-un port trunk următorului switch, care la rândul său îl transmite fără modificări următorului switch. Următorul switch examinează dacă are dreptul să opereze cu acest frame. Dacă da, atunci switch-ul elimină teg-ul și transmite frame-ul „curățat" către host. Dacă host-ul s-ar fi aflat într-un alt VLAN decât cel indicat în teg, atunci switch-ul ar fi eliminat frame-ul.

În continuare, revenim la rețeaua din Figura 4 și descriem procedura de configurare a VLAN-urilor.
1) Mai întâi setăm pe host-uri IP-urile corespunzătoare.
2) Stabilim legăturile de tip Access între switch-uri și host-uri. Fiecare port al switch-ului îl asociem cu un VLAN concret. Implicit, portul se află în VLAN1 (adică la început toate porturile sunt asociate cu VLAN1). VLAN-ul este creat pe switch și se asociază cu un port.



Accesăm linia de comandă CLI a switch-ului Switch0 și executăm comenzile următoare:

Switch>en	Trecem în modul privilegiat
Switch#conf ter	Trecem în modul de configurare globală
Switch(config)#int range fa 0/1-2	Accesăm interfețele fa 0/1 și fa 0/2
Switch(config-if-range)#switchport mode access	Switch-ul va insera teg-uri în frame-urile recepționate prin aceste porturi (adică creăm legături de tip Access)
Switch(config-if-range)#switchport access vlan 2	Se precizează VLAN-ul din care vor face parte host-urile PC0 și PC1
Switch(config-if-range)#exit	Ieșim din modul de configurare a interfeței selectate
Switch(config)#int fa 0/4 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 3 Switch(config-if)#exit	Accesăm modul de configurare a interfeței fa 0/4 și executăm aceleași comenzi, cu diferența că host-ul PC8 va face parte din VLAN3

Pentru a vizualiza legăturile de tip Access stabilite pe switch vom folosi comanda:

Switch#show vlan brief

În mod analog se configurează legăturile de tip Access pe switch-urile Switch1, Switch2 și Switch3. În acest mod am stabilit toate legăturile de tip Access.

3) În continuare se stabilesc legăturile de tip trunk dintre switch-ul central (Switch4) și celelalte switch-uri (Switch0, Switch1, Switch2, Switch3). Pentru aceasta este suficient să se stabilească porturi trunk pe Switch4.

```
Switch>en
Switch#conf ter
Switch(config)#int range fa 0/1-4
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#exit
```

Pentru a vizualiza porturile trunk pe un switch se va utiliza comanda

Switch# show interface trunk

4) Switch-ul central trebuie să știe identificatorii VLAN-urilor, ai căror frame-uri cu teg acesta urmează să le retransmită. Pentru aceasta creăm pe switch aceste VLAN-uri.

```
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#exit
Switch(config)#vlan 5
Switch(config-vlan)#exit
Switch(config)#show vlan
```

Pentru a modifica numele VLAN-ului (pentru o identificare mai simplă a acestora) vom folosi comanda *name*:

```
Switch#conf ter
Switch(config)#vlan 2
Switch(config-vlan)#name Buhgalteria
Switch(config-vlan)#exit
Switch(config)#do show vlan
```

Verificați dacă există conexiune între PC0 și PC9:
ping 192.168.2.5 => există conexiune
Examinați de sine stătător în modul Simulation cum are loc inserarea teg-ului în frame (urmăriți conținutul câmpului TCI în frame-urile ARP, atunci când acestea trec prin link-urile trunk) și cum are loc eliminarea acestuia.
De unde știe Switch4 că pachetul din VLAN2 urmează să fie transmis către Switch2 și Switch3 și nu trebuie să fie transmis către Switch1? Pentru că în tabelul de MAC adrese al Switch4 avem nu doar corespondența dintre MAC-uri și porturi, dar și corespondența dintre porturi și VLAN-uri. În modul Simulation se poate verifica cu *show mac-address-table* veridicitatea afirmației:

Vlan	Mac Address	Type	Ports
1	0001.63ee.e903	DYNAMIC	Fa0/1
1	0001.97e1.5803	DYNAMIC	Fa0/2
1	000c.cf5c.5103	DYNAMIC	Fa0/4
1	00d0.d39d.ea03	DYNAMIC	Fa0/3
2	0001.63ee.e903	DYNAMIC	Fa0/1
2	000c.cf5c.5103	DYNAMIC	Fa0/4
2	0090.0c42.80e6	DYNAMIC	Fa0/1
2	00d0.d39d.ea03	DYNAMIC	Fa0/3
3	0001.63ee.e903	DYNAMIC	Fa0/1
3	0001.97e1.5803	DYNAMIC	Fa0/2
3	000c.cf5c.5103	DYNAMIC	Fa0/4
4	00d0.d39d.ea03	DYNAMIC	Fa0/3
5	000c.cf5c.5103	DYNAMIC	Fa0/4

VI. *Asigurarea legăturii dintre VLAN-uri*
Pentru ca să existe posibilitatea de schimb de date între VLAN-uri se va utiliza routerul, iar procedeul este numit Inter VLAN Routing
Deoarece VLAN-urile se află în subrețele diferite => pentru a asigura comunicarea între subrețele este necesar un router
Să examinăm configurația de rețea din Figura 8 în care switch-ul central este conectat la un router ce va asigura comunicarea între anumite VLAN-uri

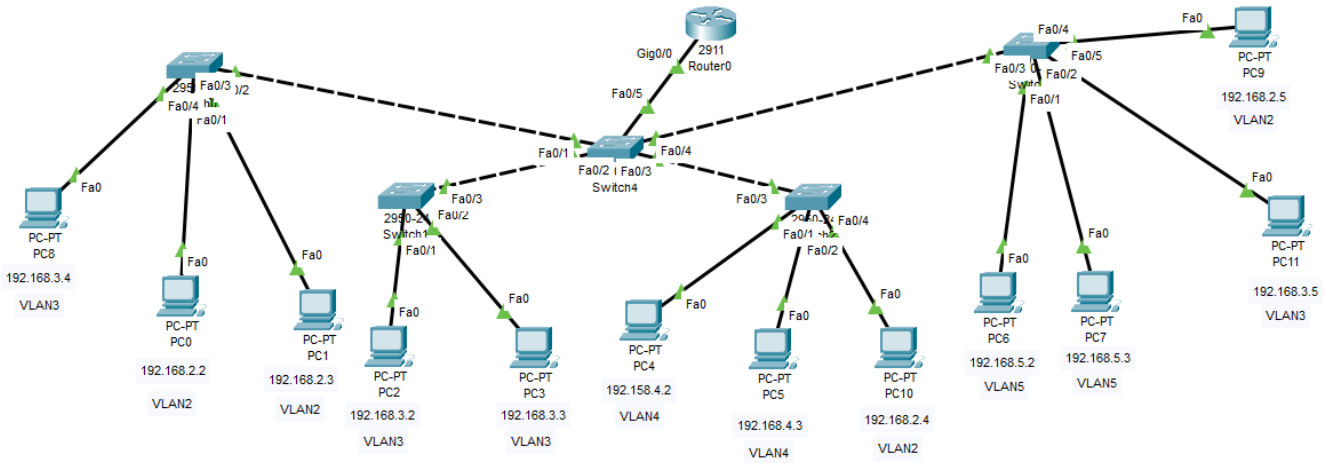


Figura 8

Definim portul Fa 0/5 al switch-ului Switch4 ca un port trunk:

```
Switch>en
Switch#conf ter
Switch(config)#int fa 0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

În continuare, accesăm modul CLI pe router și configurăm patru subinterfețe (tot atâtea subinterfețe câte VLAN-uri avem):

```
Router>en
Router#conf ter
Router(config)#int gig 0/0.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip add 192.168.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int gig 0/0.3
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip add 192.168.3.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int gig 0/0.4
Router(config-subif)#encapsulation dot1q 4
Router(config-subif)#ip add 192.168.4.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int gig 0/0.5
Router(config-subif)#encapsulation dot1q 5
Router(config-subif)#ip add 192.168.5.1 255.255.255.0
Router(config-subif)#exit
```

Pe interfața grafică corespunzătoare lui Gigabit Ethernet 0/0 punem bifa la *On* în drept cu *Port Status*. Lucrul acesta poate fi făcut și prin următoarele comenzi:

```
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# no shutdown
Router(config-if)# exit
```

Pe portul Fa 0/5 al switch-ul central se poate preciza lista cu VLAN-urile ce au acces la router (sau de la router), folosind comanda (se scrie în modul de configurare a interfeței Fa 0/5 după *switchport mode trunk*, de exemplu)

switchport trunk allowed vlan 2,3 (se indică VLAN-urile permise => în cazul dat vor trece doar pachetele din VLAN-urile 2 și 3)

Pe fiecare host setăm adresa de router implicit (Default Gateway)

Dăm un ping între două host-uri ce se află în VLAN-uri diferite

Se va examina procesul în modul Simulation (se lasă pentru vizualizare doar pachetele ARP și ICMP)

Dacă se dă ping de la host-ul PC0, care se află în VLAN2, către host-ul PC11, care se află în VLAN3, avem următoarea situație: pachetul ARP ajunge la switch-ul central, care îi permite să treacă prin portul său Fa 0/5 (deoarece vine din VLAN2) la router; routerul îi transmite lui PC0 adresa sa MAC. PC0 îi transmite routerului pachetul de date utile. Routerul formează un pachet ARP în care modifică în 3 eticheta 2 a VLAN-ului (aceasta este scrisă în câmpul TCI – 0x0003) și transmite pachetul în VLAN3 pentru a afla adresa MAC a host-ului destinație. Host-ul destinație transmite routerului adresa sa MAC, iar routerul îi transmite pachetul de date utile.

Dacă se dă ping de la host-ul PC0, care se află în VLAN2, către host-ul PC7, care se află în VLAN5, avem următoarea situație: pachetul ARP ajunge la switch-ul central, care îi permite să treacă prin portul său Fa 0/5 (deoarece vine din VLAN2) la router; routerul îi transmite lui PC0 adresa sa MAC. PC0 îi transmite routerului pachetul de date utile. Routerul formează un pachet ARP în care modifică în 5 eticheta 2 a VLAN-ului (aceasta este scrisă în câmpul TCI – 0x0005) și transmite pachetul în VLAN5 pentru a afla

adresa MAC a host-ului destinație. Însă pachetul este stopat de către switch-ul central (în portul Fa 0/5), deoarece este setată permisiune doar pentru pachetele din VLAN-urile 2 și 3.
Astfel, se vede că routerul are capacitatea de a modifica eticheta VLAN-ului (în cazul dat 2 prin 3 (sau prin 5)) și, prin urmare, poate transmite pachetele între VLAN-uri

Lucru individual - Rezolvați problema cu două host-uri din VLAN-e diferite, un switch, un router și un server de internet (a se vedea Figura 6b), astfel încât conexiunea dintre switch și router să se realizeze printr-un singur cablu și o singură interfață de router (trebuie să configurați două subinterfețe pe router).

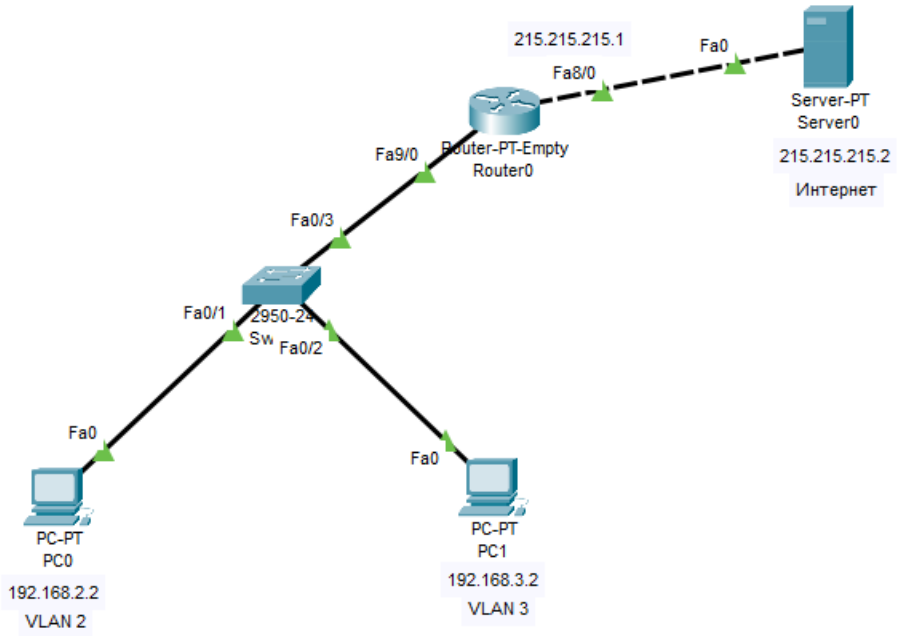


Figura 6b

VII. *Asigurarea legăturii dintre VLAN-uri prin intermediul switch-ului de nivel 3*
Pentru a conecta rețelele virtuale într-o rețea comună este necesar să se implice protocolul IP de la nivelul rețea. Acesta din urmă poate fi implementat printr-un router sau printr-un switch de nivel 3.
Să considerăm configurația de rețea din Figura 9 și să configurăm switch-ul L3.

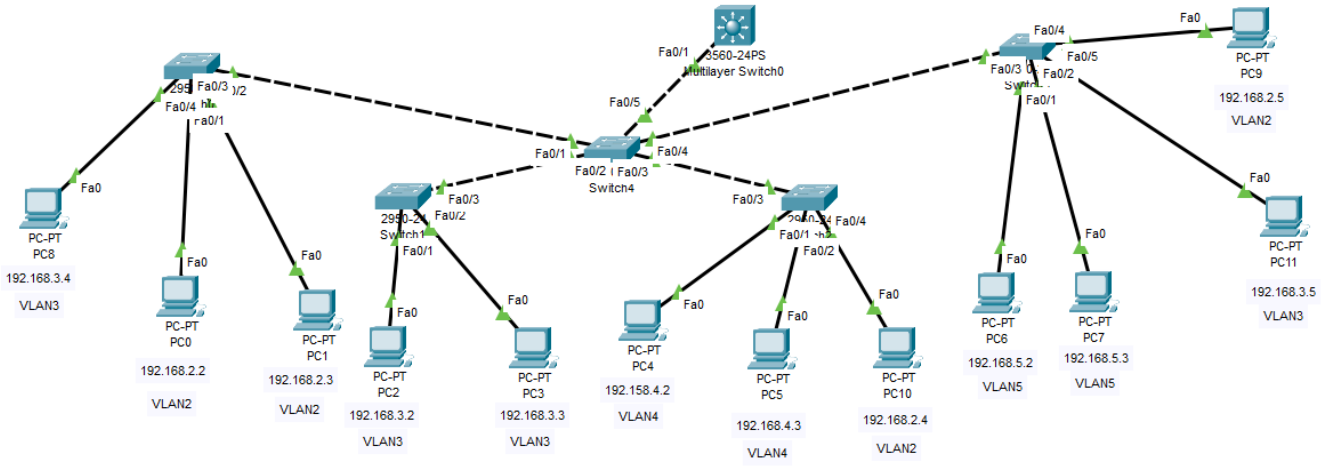


Figura 9

Trecem în modul CLI al switch-ului L3 și executăm următoarele comenzi:

```
Switch>en
Switch#conf ter
Switch(config)#int fa 0/1
% nu va trece direct switchport mode trunk, deoarece în acest caz există și ISL
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#exit
% делаем VLAN-ы:
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#exit
Switch(config)#vlan 5
Switch(config-vlan)#exit
% Pentru a atribui adrese IP, în loc de subinterfețe se generează interfețe virtuale:
Switch(config)#int vlan 2  % am generat interfața virtuală ce va deservi VLAN-ul 2
Switch(config-if)#ip add 192.168.2.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vlan 3
Switch(config-if)#ip add 192.168.3.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vlan 4
Switch(config-if)#ip add 192.168.4.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#int vlan 5
Switch(config-if)#ip add 192.168.5.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip routing
```

De pe host-ul PC0 (care se află în VLAN2) dăm un ping către host-ul PC11 (din VLAN3). În modul Simulation vom vedea că solicitarea ARP este transmisă tuturor host-urilor din VLAN2, inclusiv și switch-ului L3. Switch-ul L3 îi răspunde lui PC0 cu adresa sa MAC. PC0 îi transmite frame-ul cu date utile switch-ului L3. În continuare, switch-ul L3 transmite o solicitare ARP tuturor host-urilor din VLAN3. Host-ul PC11 îi răspunde switch-ului cu adresa sa MAC. Switch-ul L3 transmite pachetul cu date utile către PC11.
Cum se poate modifica VLAN-ul implicit Native VLAN (VLAN1)? De ce este necesar să fie modificat? – deoarece în pachetele ARP din VLAN1 nu se indică eticheta VLAN-ului, iar acest fapt a fost exploatat prin construcția unor atacuri asupra Native VLAN, care combat securitatea rețelei
Accesăm portul switch-ului și dăm comanda:

```
Switch(config)# int fa 0/3
Switch(config-if)# switchport trunk native vlan 50
(de exemplu, 50 => datele din VLAN-ul 50 nu vor fi marcate cu teg)
```

Același lucru se face și pe celelalte porturi trunk

Cerințe pentru realizarea lucrării de laborator №2

În Cisco Packet Tracer, efectuați următoarele:

1. Construiți topologia logică de rețea prezentată în Figura 10.
2. Folosind datele din Tabelul 1, configurați dispozitivele rețelei construite la punctul 1. Construiți și configurați cele trei VLAN-uri (cu ID-urile k+1, k+2 și k+3) indicate în Figura 10. În calitate de router se va utiliza modelul Router-PT-Empty, la care se vor adăuga două module de interfață (unul pentru subinterfețele ce asigură legătura cu VLAN-urile și altul pentru a asigura legătura la serverul de Internet).
   Salvați configurația creată cu numele **Nume_Prenume_Grupa_Retea2a.pkt**.

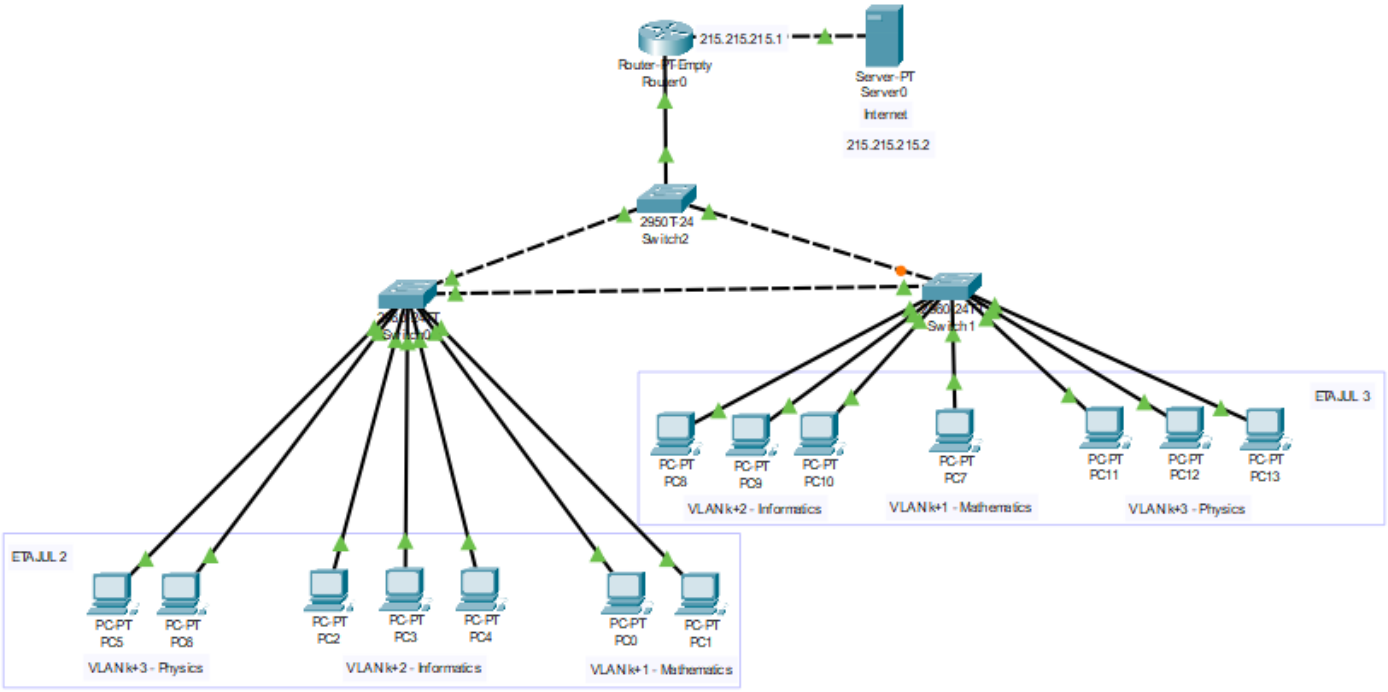


Figura 10

3. Arătați cum se deplasează pachetul ARP și pachetul ICMP între host-urile
   a) care se află în VLAN-ul k+2
   b) din VLAN-urile k+2 și k+3 (sursa în VLAN k+2, destinația în VLAN k+3 și invers)
   Explicați și ilustrați momentul în care un switch inserează în cadrul pachetului identificatorul VLAN-ului din care a venit pachetul și momentul în care identificatorul este eliminat.
4. Eliminați serverul de Internet. Înlocuiți routerul Router-PT-Empty cu un switch L3 de model 3560-24PS și efectuați configurările necesare pentru ca switch-ul să asigure legătura între VLAN-uri. Arătați cum se deplasează pachetele ARP și ICMP în cadrul aceluiași VLAN, precum și între VLAN-uri. Salvați configurația creată cu numele **Nume_Prenume_Grupa_Retea2b.pkt**.

Realizați o dare de seamă asupra lucrului efectuat, care să conțină răspunsuri explicite la fiecare punct formulat în cerințe.

Încărcați fișierul cu darea de seamă și fișierele .pkt în mapa corespunzătoare *Lucrarea de laborator N2* din pagina dedicată cursului de Rețele de Calculatoare a platformei educaționale moodle.usm.md.

Tabelul 1

Subrețea VLAN	Nume/Tip dispozitiv	Port de switch sau router	IP adresa	Masca subrețelei	Default Gateway
VLAN k+1	PC0	FastEthernet0	192.168.k+1.k+1	255.255.255.0	192.168.k+1.1

192.168.k+1.0 255.255.255.0	PC1	FastEthernet0	192.168.k+1.k+2	255.255.255.0	192.168.k+1.1
	PC7	FastEthernet0	192.168.k+1.k+3	255.255.255.0	192.168.k+1.1
VLAN k+2 192.168.k+2.0 255.255.255.0	PC2	FastEthernet0	192.168.k+2.k+1	255.255.255.0	192.168.k+2.1
	PC3	FastEthernet0	192.168.k+2.k+2	255.255.255.0	192.168.k+2.1
	PC4	FastEthernet0	192.168.k+2.k+3	255.255.255.0	192.168.k+2.1
	PC8	FastEthernet0	192.168.k+2.k+4	255.255.255.0	192.168.k+2.1
	PC9	FastEthernet0	192.168.k+2.k+5	255.255.255.0	192.168.k+2.1
	PC10	FastEthernet0	192.168.k+2.k+6	255.255.255.0	192.168.k+2.1
VLAN k+3 192.168.k+3.0 255.255.255.0	PC5	FastEthernet0	192.168.k+3.k+1	255.255.255.0	192.168.k+3.1
	PC6	FastEthernet0	192.168.k+3.k+2	255.255.255.0	192.168.k+3.1
	PC11	FastEthernet0	192.168.k+3.k+3	255.255.255.0	192.168.k+3.1
	PC12	FastEthernet0	192.168.k+3.k+4	255.255.255.0	192.168.k+3.1
	PC13	FastEthernet0	192.168.k+3.k+5	255.255.255.0	192.168.k+3.1
	Router PT-Empty	Subinterfețele primei interfețe: FastEthernet FastEthernet FastEthernet A doua interfață: FastEthernet	 192.168.k+1.1 192.168.k+2.1 192.168.k+3.1 215.215.215.1	 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	 - - - -
	Server-PT	FastEthernet	215.215.215.2	255.255.255.0	215.215.215.1
	Multilayer Switch 1	VLAN k+1	192.168.k+1.1	255.255.255.0	-
		VLAN k+2	192.168.k+2.1	255.255.255.0	-
		VLAN k+3	192.168.k+3.1	255.255.255.0	-

(***k = numărul de ordine alfabetică a studentului în registrul grupei***)