Lucrarea de laborator №1

Construirea topologiilor logice de reţea cu Cisco Packet Tracer şi studierea procesului de transmitere a pachetelor de date în reţea

Scopul lucrării constă în formarea unor abilităţi practice de construire a topologiilor logice de reţea cu Cisco Packet Tracer si ilustrarea modului de functionare al switch-urilor, routerelor şi a protocolului ARP

Obiective:

- Construirea unei reţele simple în spaţiul de lucru pentru topologia logică
- Configurarea dispozitivelor din reţea
- Verificarea conexiunii între dispozitivele din reţea, folosind comanda ping
- Stabilirea numărului de hop-uri pe traseul de la sursă la destinaţie, folosind comanda tracert
- Ilustrarea procesului de completare şi aplicare a tabelului MAC la switch-uri
- Ilustrarea procesului de completare şi aplicare a tabelului ARP la host-uri
- Ilustrarea procesului de completare şi aplicare a tabelului ARP la router

1. Instalarea programului Cisco Packet Tracer

Pentru a instala *Cisco Packet Tracer* se vor urma paşii:

1. Creaţi un cont Cisco, accesând link-ul https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui
2. Introduceţi datele contului Cisco, completând câmpurile formularului din fereastra încărcată
3. Accesaţi email-ul indicat la formarea contului Cisco pentru a activa contul
4. Accesaţi site-ul https://www.netacad.com şi logaţi-vă (în dreapta sus este Login-ul)
5. În meniul **Resources** alegeţi opţiunea *Download Cisco Packet Tracer*
6. În partea de jos a ferestrei încărcate daţi un click pe link-ul către pachetul de instalare, în dependenţă de sistemul de operare al dispozitivului pe care îl utilizaţi.
7. Instalaţi Cisco Packet Tracer. La deschiderea programului, introduceţi e-mailul şi parola care au fost indicate la crearea contului Cisco.

2. Conectarea a două host-uri în reţeaua locală

Din End Devices selectaţi două calculatoare PC-PT (staţii de lucru) şi plasaţi-le în zona de lucru. Din Network Devices selectaţi un switch (comutator) de model Cisco Catalyst 2950-24 pe 24 de porturi şi plasaţi-l în zona de lucru (a se vedea Figura 1).

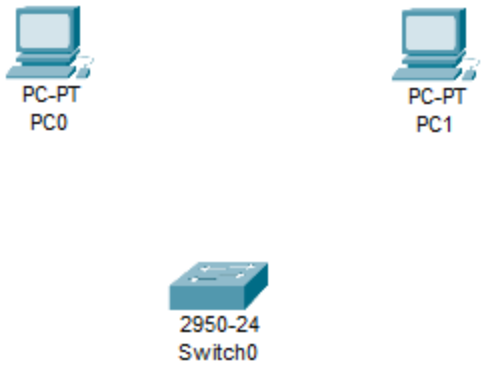

Figura 1

În continuare, conectăm calculatoarele cu switch-ul. Pentru aceasta din Connections (pictograma sub formă de fulger) selectăm linia de comunicaţie automată - de asemenea, pictograma sub formă de fulger (a se vedea Figura 2).

Figura 2

Ţinând apăsată tasta CTRL, faceţi clic pe dispozitivele pe care doriţi să le conectaţi (vezi Figura 3). La final, apăsaţi tasta Esc pentru a ieşi din modul de conectare.

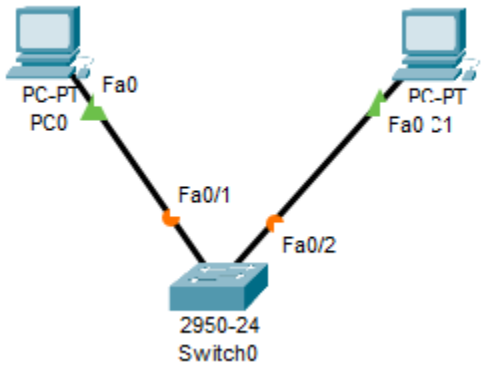

Figura 3

Aşteptăm până când cercurile de culoare portocalie se transformă în triunghiuri verzi - conexiunea este stabilită (vezi Figura 4).

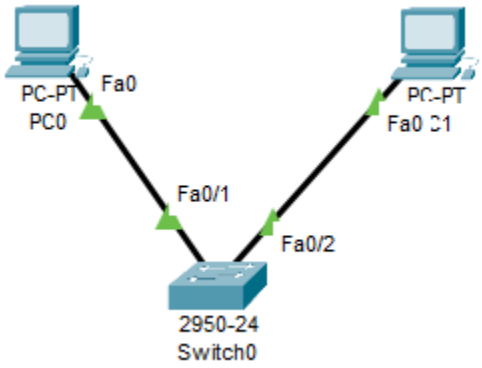

Figura 4

Figura arată numele Fa0 al interfeţelor plăcilor de reţea ale calculatoarelor PC0 şi PC1, precum şi numele Fa0/1 şi Fa0/2 ale porturilor switch-ului. Dacă aceste nume nu sunt vizibile, atunci acestea pot fi activate, bifând caseta de selectare Always show port labels in logical workspace din meniul Opţiuni, submeniul Preferences -> Interface. Deşi am conectat calculatoarele PC0 şi PC1, pentru a putea trimite date între ele, trebuie să setăm adresele IP pe PC0 şi PC1. Pentru a face acest lucru, daţi un click pe pictograma calculatorului PC0 şi în fereastra care se deschide, selectaţi Config şi apoi interfaţa plăcii de reţea FastEthernet0 (vezi Figura 5).

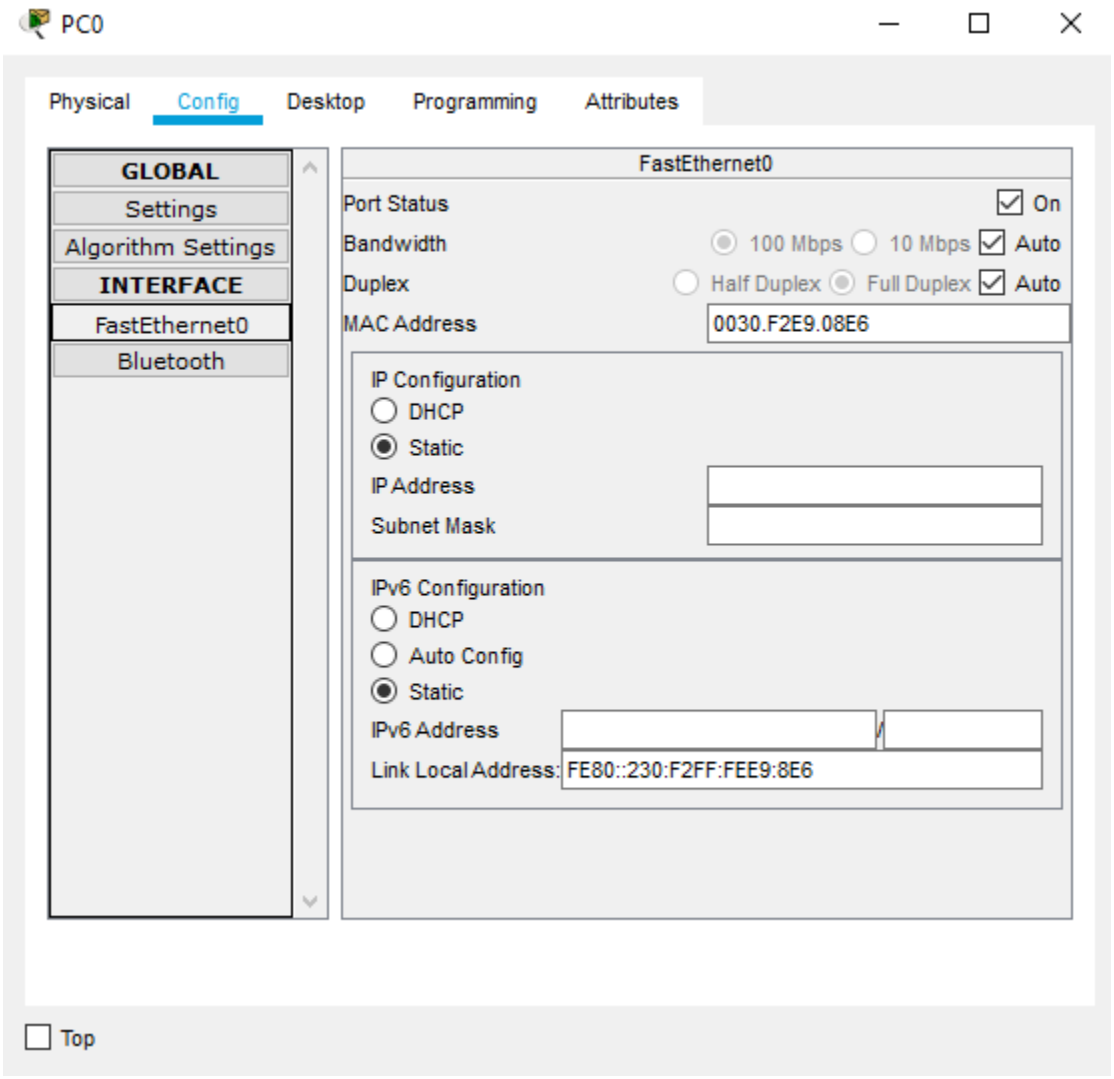

Figura 5

Completăm manual câmpul IP Address cu valoarea 192.168.0.1 şi dăm un click pe câmpul de la Subnet Mask - acolo va fi generată automat masca de subreţea 255.255.255.0. Închidem fereastra.

În acelaşi mod, configurăm al doilea calculator PC1, atribuind acestuia adresa IP 192.168.0.2.

Pentru a verifica dacă există conexiune între PC0 şi PC1, trimitem un ping de la PC0 la PC1. Pentru a face acest lucru, dăm un click pe PC0 -> Desktop -> Command Prompt şi culegem în linia de comandă ping 192.168.0.2.

Apăsând Enter, vom vedea peste ceva timp că au fost trimise şi primite 4 pachete de date, ceea ce dovedeşte că există conexiune cu PC1. În mod similar, verificăm dacă calculatorul PC0 este accesibil de la calculatorul PC1.

Adăugăm încă un dispozitiv în reţeaua noastră - selectăm un Server din End Devices şi îl conectăm la switch (vezi Figura 6). De asemenea, setăm adresa IP 192.168.0.3.

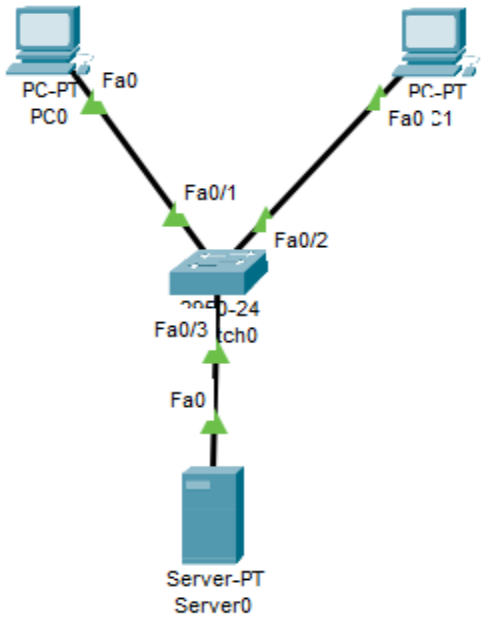

Figura 6

Datele dintre host-uri sunt transmise prin switch, iar topologia reţelei rezultată este o topologie stea. Dacă datele pot fi transmise în ambele direcţii în acelaşi timp, atunci cu ajutorul unui switch se evită coliziunile = semnale suprapuse în canalul de transmisie = datele sunt distruse.

Datele trimise de calculator ajung la un anumit port al switch-ului, mai exact în buffer-ul portului de intrare. Apoi, switch-ul determină portul de ieşire şi transferă datele în buffer-ul acestuia. Dacă canalul corespunzător portului dat este liber, atunci datele sunt trimise la calculatorul corespunzător. Dacă datele de la două calculatoare au ajuns în acelaşi buffer => atunci acestea sunt stocate acolo separat şi sunt trimise pe rând => astfel nu au loc coliziuni. Mai înainte au existat dispozitive numite hub-uri (concentratoare) -> nu aveau memorie buffer -> de aceea aveau loc coliziuni.

Dacă reţeaua implică doar host-uri care sunt conectate prin switch-uri, atunci o astfel de reţea se numeşte domeniu broadcast (sau domeniu de difuzare).

Datele care sunt transmise în limitele unui domeniu broadcast se numesc frame-uri.

Dacă reţeaua este compusă din două sau mai multe domenii broadcast => atunci acestea sunt conectate printr-un router.

3. Protocolul ARP

Adresarea IP funcţionează indirect într-un domeniu broadcast. De bază aici este adresa MAC.

Când transmitem un frame de la PC0 la server => frame-ul este transmis în baza adresei MAC a serverului, şi nu în baza adresei IP acestuia.

Adresa MAC este stocată în memoria echipamentelor de reţea de către producător.

Folosind protocolul ARP => adresa IP a serverului este convertită la o adresă MAC.

Un switch obişnuit nu poate opera cu adrese IP, ci lucrează doar cu adrese MAC.

În baza unui mecanism, switch-ul determină pe care port să transfere frame-ul primit.

Mecanismul asociază fiecărui port al switch-ului o anumită adresă MAC (ce aparţine unui dispozitiv din reţea).

Când un frame vine de la PC0 la switch şi este destinat serverului => switch-ul ştie exact unde să trimită acest frame.

Mecanismul este definit de tabelul MAC al switch-ului

Când switch-ul est conectat în reţea pentru prima dată => tabelul MAC al acestuia nu conţine elemente.

Primul frame primit este direcţionat de switch către toate porturile sale, cu excepţia acelui port din care a venit (procedura este numită unicast flooding).

Imediat ce switch-ul primeşte frame-ul de la PC0, acesta notează în tabelul său MAC că portului Fa0/1 îi corespunde adresa MAC a lui PC0.
Calculatorul către care a fost trimis frame-ul trimite ca răspuns un alt frame.
Când frame-ul răspuns ajunge la switch, acesta scrie adresa MAC a calculatorului care a răspuns în tabelul său MAC şi trimite frame-ul prin portul Fa0/1 către PC0 (a transferat adresa MAC corespunzătoare dintr-un buffer în altul).
Switch-ul a trimis frame-ul de răspuns exact acolo unde era necesar, deoarece în tabelul MAC a găsit că adresa destinatarului se află în spatele acestui port.
Dacă al treilea calculator va trimite un frame, atunci switch-ul va completa tabelul MAC şi va trimite acest frame prin portul corespunzător.
Dimensiunea tabelului de adrese MAC pentru diferite modele variază de la 1000 la 8000 de intrări.
Dacă toate celulele din tabelul MAC sunt deja completate şi switch-ul primeşte un frame de la un dispozitiv pentru care nu are o înregistrare => atunci switch-ul va trimite acest frame la toate calculatoarele şi dacă pentru o perioadă de timp nu există niciun mesaj de răspuns de la vreun calculator, atunci switch-ul va crede că acel calculator la moment nu este funcţional şi va şterge intrarea corespunzătoare din tabelul MAC. Intrarea mai veche este ştearsă, iar cea nouă este scrisă.
Concluzie despre switch-uri
Astfel, switch-ul L2 este utilizat pentru:
1. conectarea host-urilor
2. a preveni coliziunile
3. că foloseşte tabelul de adrese MAC, care permite transferul frame-ului de pe un port pe altul necesar => reduce încărcarea reţelei

În colţul din dreapta jos al Cisco Packet Tracer există un buton de trecere în modul Simulation (Modelare) => dăm un click pe butonul Simulation => am trecut în acest mod
Apăsăm pe pictograma PC0 şi selectăm Command Prompt -> ping 192.168.0.2
S-au format două pachete la PC0 (ICMP şi ARP), dar nu avem dinamică => se aşteaptă apăsarea butonului de trecere dintr-o stare în alta 
În primul rând, este trimis un pachet ARP - astfel, PC0 încearcă să afle adresa MAC a calculatorului cu acest IP: 192.168.0.2.
Să vedem ce se întâmplă cu pachetul de date când facem clic pe butonul Capture/Forward => pachetul trece pe switch.
La următoarea apăsare a butonului Capture/Forward, pachetul este trimis către PC1 şi server, dar serverul vede că pachetul nu este destinat lui (o altă adresă MAC) şi îl respinge (un x pe pachet).
La următoarea apăsare a butonului Capture/Forward, PC1 trimite un răspuns care vine la switch.
Pachetul este direcţionat către PC0 şi nu către server, deoarece switch-ul a învăţat adresa MAC a lui PC0.
În Cisco Packet Tracer, switch-ul poate fi configurat => putem accesa interfaţa sa şi să vedem tabelul MAC al acestuia. Dăm un click pe pictograma switch-ului şi selectăm modul CLI => acest mod este o emulare a unei conexiuni la terminal (fereastra care a fost deschisă este identică cu fereastra de interfaţă dacă ne-am fi conectat printr-un cablu de consolă la un port special al switch-ului) => ne-am conectat la dispozitiv şi îl putem configura
Switch-ul adevărat Cisco Catalyst are un port special pentru consolă:
În comutator - RJ45; în calculator - un port COM sau USB (a se vedea Figura 7)

Figura 7

În realitate, switch-ul este configurat, folosind o interfaţă web pe calculator (cu calculatorul conectat la switch)
Conexiunea se poate realiza nu numai prin consolă, ci şi prin reţea (de la distanţă, folosind Telnet sau SSH)
Toate configurările sunt realizate, folosind linia de comandă
Deci, am încărcat terminalul din linia de comandă. În continuare ne familiarizăm cu interfaţa liniei de comandă
Pentru a obţine o listă de comenzi disponibile, trebuie să tastăm un semn de întrebare:
Obţinem o listă din 12 comenzi: connect, disable, disconnect, enable, exit, logout, ping, resume, show, telnet, terminal, traceroute
Trebuie să trecem la modul de vizualizare completă, numit mod privilegiat
Scriem comanda enable => vom obţine switch# în loc de switch>
Tastăm semnul întrebării => obţinem o listă cu 28 de comenzi disponibile: clear, clock, configure, connect, copy, debug, delete, dir, disable, disconnect, enable, erase, exit, logout, more, no, ping, reload, resume, setup, show, ssh, telnet, terminal, traceroute, undebug, vlan, write
De ce este necesar modul privilegiat? Când dispozitivul este configurat, nu ne va permite din prima să accesăm modul privilegiat, ci va cere să ne autorizăm prin introducerea unei parole (dacă nu ştim parola, nu ne va permite să intrăm)
exit - ieşire din modul privilegiat
putem scrie în formă prescurtată: de exemplu, în loc de comanda enable putem scrie doar en şi să apăsăm tasta Tab => comanda va fi scrisă integral
La fel, putem scrie doar en şi direct să apăsăm Enter
Vrem să vedem tabelul adreselor MAC (se face din modul privilegiat)
Scriem comanda show şi semnul ? => vom vedea comenzile care pot fi utilizate cu comanda show
switch # show mac-address-table => vedem ce adresă MAC este asociată cu fiecare port al switch-ului:

Vlan	MAC address	Type	Ports
1	0001.63ce.679e	Dynamic	Fa0/1
1	0006.2ae8.96be	Dynamic	Fa0/2

În baza datelor din tabel avem:
0001.63ce.679e - adresa MAC a lui PC0
0006.2ae8.96be - adresa MAC a lui PC1
Documentaţia pentru comenzile Cisco poate fi găsită în fişierul
“Команды Cisco, часть I”
Comanda show mac-address-table int fa 0/2 arată doar interfaţa specificată a tabelului MAC

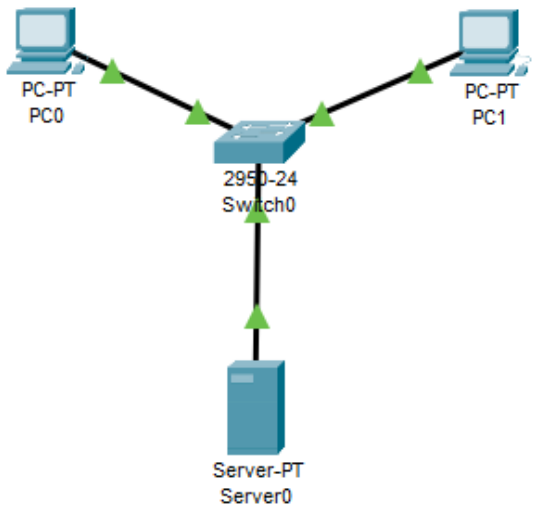

Figura 8

În limitele unui domeniu broadcast, adresarea nu se face prin adrese IP, ci prin adrese MAC
Datele sunt trimise la adrese MAC
Address Resolution Protocol = ARP permite realizarea de corespondenţe între adresele IP şi adresele MAC
Protocolul funcţionează în modul următor:
Când încercăm să accesăm un host după adresa lui IP, se generează un pachet ARP - un mesaj broadcast special, care solicită adresa MAC a host-ului cu adresa IP indicată. Calculatorul cu acest IP răspunde calculatorului iniţial cu adresa sa de MAC. Calculatorul iniţial scrie în tabelul său ARP o intrare cu adresa IP şi adresa MAC corespunzătoare
Tabelul ARP poate fi vizualizat:
În linia de comandă a lui PC0 scriem:

```
arp -a
```

Rezultatul va fi că în acest moment nu există înregistrări în tabel.
Dăm un ping de la PC0 la PC1. Activăm modul Simulation

```
ping 192.168.0.2
```

După ping, se formează două pachete: ICMP şi ARP => dăm un click pe mesajul ARP => o fereastră în care putem vedea că acest mesaj are adresa broadcast: FFFF.FFFF.FFFF ARP Packet
Apăsăm pe Capture/Forward => mesajul ARP este trimis tuturor dispozitivelor din reţea => dar doar un dispozitiv răspunde la acest mesaj - acel cu IP-ul 192.168.0.2.
Şi răspunde exact calculatorului iniţial PC0 (prin switch)
De îndată ce PC0 a primit adresa MAC dorită => îi trimite un pachet de date
Ce s-a întâmplat cu tabelul ARP?

```
arp -a
```

Internet Address	Physical Address	Type
192.168.0.2	0005.5e59.6d45	dynamic

Dacă în continuare vom da ping-uri către calculatorul cu adresa IP 192.168.0.2 => mesajul ARP nu va mai fi generat, deoarece în tabelul ARP al calculatorului ce transmite ping-uri se conţine deja adresa MAC necesară.
În mod similar, dacă se dă de pe PC0 un ping către serverul cu IP-ul 192.168.0.3 => atunci va avea loc un proces analog de determinare a adresei MAC, iar tabelul ARP se va fi completa cu încă o linie (o înregistrare).

Internet Address	Physical Address	Type
192.168.0.2	0005.5e59.6d45	dynamic
192.168.0.3	0080.7049.3a35	dynamic

Dacă dăm comanda *arp -a* pe PC1=>

192.168.0.1	00d0.d394.56eb	dynamic

Atunci când PC0 a trimis o solicitare broadcast de tip ARP către PC1 şi către server, iată atunci calculatorul PC1 a notat în tabelul său ARP adresele IP şi MAC ale lui PC0 (de unde a venit cererea).
În continuare, vom considera o reţea ceva mai complexă, care reprezintă un domeniu broadcast (Figura 1):

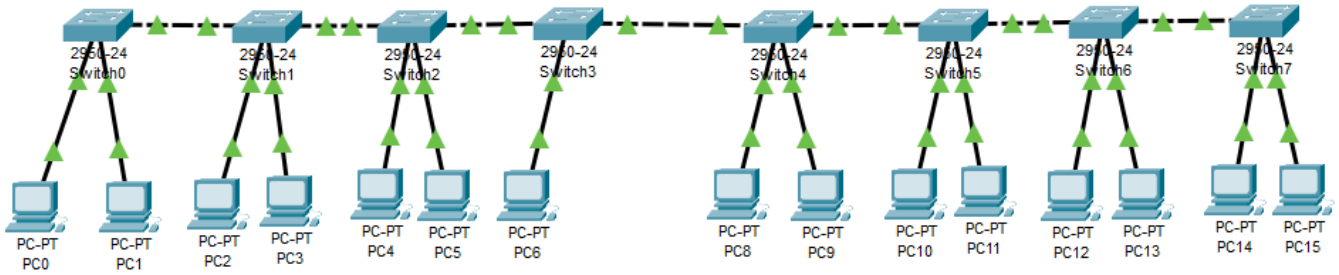

Figura 9

Orice PC poate trimite un frame broadcast şi acesta va ajunge până la fiecare PC din reţea.
Atribuim calculatorului PC0 adresa IP 192.168.0.1, iar lui PC15 - 192.168.0.2.
Pornim modul Simulation
De la calculatorul PC0 dăm un ping către calculatorul PC15: ping 192.168.0.2
Toate calculatoarele primesc mesajul ARP de la PC0 -> rezultă o furtună broadcast;
răspunsul de la PC15 va merge bine
Situaţia va fi foarte neplăcută atunci când în reţea există 1000 de calculatoare şi 500 de switch-uri, ţinând cont că calculatoarele primesc pachete de care nu au nevoie. Pachete broadcast sunt formate şi de multe alte protocoale (nu numai de ARP).

4. Utilizarea routerului

Pentru a limita furtuna broadcast şi dimensiunea domeniului broadcast, există routerele.
În diagrama anterioară vom plasa un router, de exemplu, de modelul 1841:

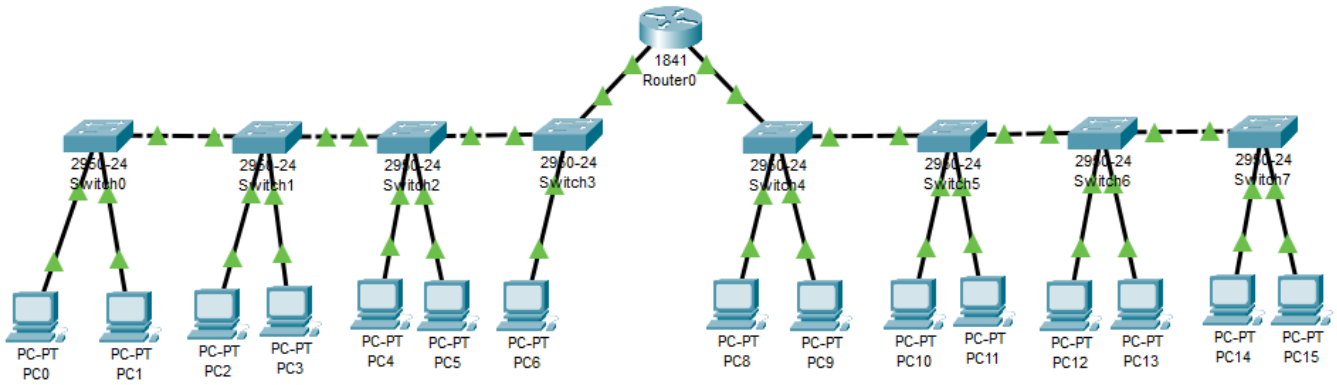

Figura 10

Am obţinut două domenii broadcast. Să arătăm că furtuna broadcast este limitată în limitele unui domeniu broadcast.
Acum PC0 nu poate trimite un mesaj către PC15. Atribuim lui PC0 adresa IP 192.168.0.1, iar lui PC15 - 192.168.0.2. De pe calculatorul PC0 dăm un ping către calculatorul PC15: ping 192.168.0.2. Activăm modul Simulation - pachetul va ajunge la router, dar nu va trece mai departe.
Routerul transferă pachetele de date dintr-un domeniu broadcast în altul => procedura se numeşte rutare de pachete.
Switch-urile (comutatoarele) realizează comutarea de pachete. În switch, în mod implicit, toate porturile sunt conectate. Dimpotrivă, într-un router toate interfeţele sunt dezactivate implicit. Routerul operează cu pachetele, iar switch-ul - cu frame-urile.

Pe interfeţele routerului se vor atribui IP adrese. Vom asigura legătura dintre cele două domenii broadcast prin configurarea interfeţelor routerului. Acest lucru se poate face în două moduri:
Prima metodă: accesăm routerul şi în interfaţa grafică a filei Config dăm un click pe numele FastEthernet0/0 (corespunzător domeniului broadcast din stânga) => setăm adresa IP 192.168.0.1 şi Subnet Mask 255.255.255.0, după care bifăm caseta On de la Port Status (în partea de sus dreapta) -> activăm interfaţa routerului.
Apoi, dăm un click pe numele FastEthernet 0/1 (corespunzător domeniului broadcast din dreapta) => setăm adresa IP 172.20.20.1 şi Subnet Mask 255.255.255.0, după care punem bifa pe On pentru Port Status (în partea de sus dreapta) -> activăm a doua interfaţă a routerului.
A doua metodă:
Accesăm routerul şi trecem în modul CLI (linie de comandă):
În fereastra grafică a apărut o întrebare despre configurarea automată a routerului => selectăm răspunsul No, deoarece vom configura manual routerul
Router> enable => Router #
1. Se atribuie adrese IP pe interfeţele routerului
2. Se activează aceste interfeţe
Comanda conf ter => Router (config) #
Trecem în modul de configurare a interfeţei:

interface fa0/0 => Router(config-if)# ip address 192.168.0.1 255.255.255.0
no shutdown

Configurăm interfaţa fa 0/1 în acelaşi mod. Există două modalităţi de a face acest lucru:
1) se iese cu exit şi se repetă procedura pentru interfaţa fa0/1
2) acolo unde ne aflăm la moment, adică în Router(config-if)#, scriem următoarele:

interface fa0/1 ip address 172.20.20.1 255.255.255.0
no shutdown

Închidem fereastra CLI
Oricărui calculator (de exemplu, PC11) al subreţelei din dreapta îi atribuim un IP, de exemplu, 172.20.20.25 cu masca 255.255.255.0.
Dăm un ping de pe calculatorul PC0 către PC11: ping 172.20.20.25 => nu există conexiune => deoarece trebuie să se specifice adresa routerului implicit (default gateway).
Dacă trebuie să transferăm datele dintr-un domeniu broadcast în altul => se va indica default gateway.
Pe PC0 -> Config -> Gateway: 192.168.0.1 (am indicat IP-ul interfeţei din stânga a routerului nostru)
Pe PC11 -> Config -> Gateway: 172.20.20.1 (am indicat IP-ul interfeţei din dreapta a routerului nostru)
Reamintim că IP-ul de pe PC0 este 192.168.0.2.
Acum, de pe PC0 dăm un ping către PC11: ping 172.20.20.25.
În continuare, vom explica de ce avem nevoie de un default gateway şi ce se întâmplă cu adresele MAC şi solicitările ARP într-o reţea cu mai multe domenii broadcast.
Calculatorul PC0 nu poate ajunge până la PC11 după adresa MAC a acestuia.
Calculatorul PC0 vede că adresa IP a lui PC11 este dintr-o altă subreţea => PC11 se află într-un alt domeniu broadcast => PC0 se adresează către default gateway => pachetul este trimis la router, iar routerul trimite pachetul primit către PC11.
Când scriem ping 172.20.20.25, PC0 trimite o cerere ARP în reţeaua sa (cine are adresa IP 192.168.0.1?) => Ruterul va răspunde lui PC0 cu adresa sa MAC => PC0 va trimite pachetul de date la adresa MAC a interfeţei routerului.
Routerul trebuie să cunoască adresa MAC a lui PC11 => trimite o solicitare ARP în a doua reţea => PC11 îi va răspunde routerului cu adresa sa MAC => routerul va trimite pachetul către PC11 în baza adresei MAC specificate.
Ilustrare: ping 172.20.20.25 de pe PC0 (ignorăm pachetele STP)

Pentru a vedea o informaţie succintă despre interfeţele routerului, dăm comanda:

```
show ip interface brief
```

Pentru a vedea tabelul ARP al routerului, trecem în linia de comandă CLI a routerului şi în modul privilegiat scriem comanda show arp:

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
Internet  172.20.20.1             -   0001.6417.4502  ARPA
FastEthernet0/1
Internet  192.168.0.1             -   0001.6417.4501  ARPA
FastEthernet0/0
Router#
```

Figura 11

Dacă traficul de date nu a trecut încă prin router, atunci vom vedea în tabelul ARP - IP-urile interfeţelor routerului şi adresele MAC corespunzătoare acestora (vezi Figura 11).

De fiecare dată când un pachet de date trece prin router, acesta va scrie în tabelul său ARP o linie nouă cu adresele IP şi MAC corespunzătoare ale host-urilor sursă şi destinaţie. De exemplu, dacă dăm un ping către calculatorul PC11 cu adresa IP 172.20.20.25 de pe PC0, atunci în tabelul ARP al routerului obţinem datele prezentate în Figura 12:

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
Internet  172.20.20.1             -   0001.6417.4502  ARPA
FastEthernet0/1
Internet  172.20.20.25            0   000B.BE0C.A682  ARPA
FastEthernet0/1
Internet  192.168.0.1             -   0001.6417.4501  ARPA
FastEthernet0/0
Internet  192.168.0.2             0   0030.A3B1.8A2D  ARPA
FastEthernet0/0
Router#
```

Folosind comanda tracert, putem sstabili ruta de la host-ul sursă la host-ul destinaţie (toate routerele intermediare, dacă nu există mai mult de 30). Dacă în Command Prompt pentru PC0 executăm comanda tracert 172.20.20.25, atunci vom obţine rezultatul prezentat în Figura 13.

```
C:\>tracert 172.20.20.25

Tracing route to 172.20.20.25 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.0.1
  2    0 ms      1 ms      0 ms      172.20.20.25

Trace complete.
```

Figura 13

Concluzii despre router:

- Routerul realizează transferul pachetelor IP dintr-un domeniu broadcast în altul.
- Routerele sunt utilizate pentru a limita dimensiunea domeniului broadcast şi pentru a reduce încărcarea în reţea.
- Dacă host-ul sursă nu poate stabili legătură cu host-ul destinaţie prin adresa MAC, atunci host-ul sursă apelează la serviciile routerului implicit (default gateway).

Cerinţe pentru realizarea lucrării de laborator №1

1. Construiţi topologia logică de reţea din Figura 12, utilizând Cisco Packet Tracer.
2. Utilizând adresele prezentate în Tabelul 2, configuraţi toate dispozitivele (host-uri, switch-uri şi routere) astfel încât să fie asigurată conexiunea dintre acestea, iar host-urile să poată face schimb de date. Salvaţi reţeaua creată cu numele Nume_Prenume_Grupa_Network1.pkt.
3. Verificaţi conexiunea între dispozitivele de reţea, folosind comanda ping**.** În raportul cu privire la lucrul efectuat includeţi capturi de ecran cu comenzile date şi rezultatele obţinute.
4. Stabiliţi traseul parcurs cu ajutorul comenzii tracert. În raportul cu privire la lucrul efectuat includeţi capturi de ecran cu comenzile date şi rezultatele obţinute.

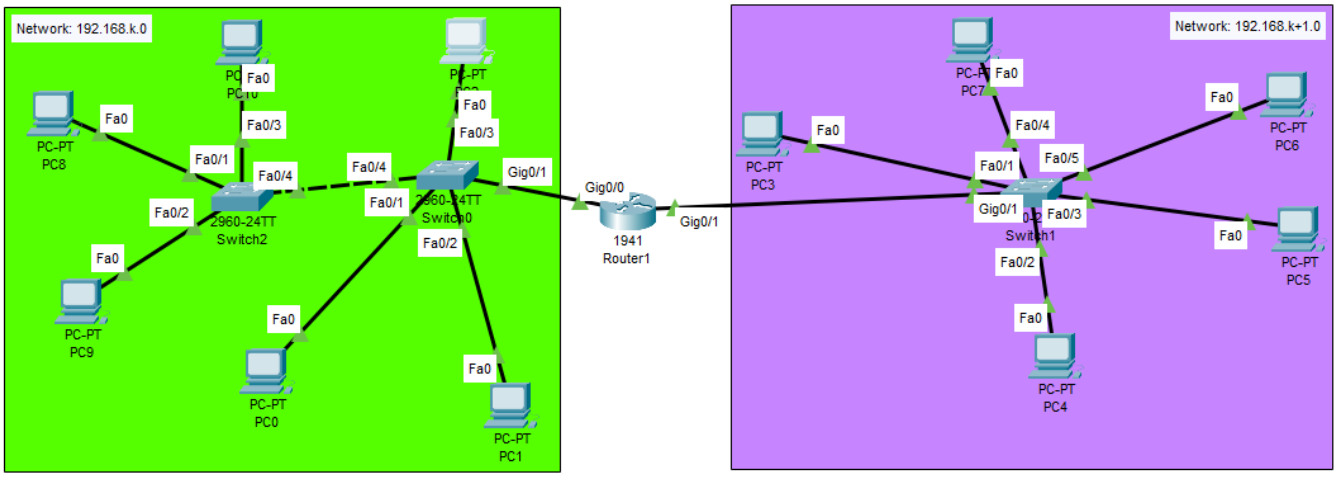

Figura 12

Tabelul de adrese

Tabelul 2

IP Reţea	Device	Interface	IP Address	Subnet Mask	Default Gateway
192.168.k.0	PC0	FastEthernet0	192.168.k.k+1	255.255.255.0	192.168.k.1
	PC1	FastEthernet0	192.168.k.k+2	255.255.255.0	192.168.k.1
	PC2	FastEthernet0	192.168.k.k+3	255.255.255.0	192.168.k.1
	PC8	FastEthernet0	192.168.k.k+4	255.255.255.0	192.168.k.1
	PC9	FastEthernet0	192.168.k.k+5	255.255.255.0	192.168.k.1
	PC10	FastEthernet0	192.168.k.k+6	255.255.255.0	192.168.k.1
192.168.k+1.0	PC3	FastEthernet0	192.168.k+1.k+1	255.255.255.0	192.168.k+1.1
	PC4	FastEthernet0	192.168.k+1.k+2	255.255.255.0	192.168.k+1.1
	PC5	FastEthernet0	192.168. k+1.k+3	255.255.255.0	192.168.k+1.1
	PC6	FastEthernet0	192.168. k+1.k+4	255.255.255.0	192.168.k+1.1
	PC7	FastEthernet0	192.168. k+1.k+5	255.255.255.0	192.168.k+1.1
192.168.k.0	Router 1941	GigabitEthernet0/0	192.168.k.1	255.255.255.0	-
192.168.k+1.0		GigabitEthernet0/1	192.168.k+1.1	255.255.255.0	-

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

5. Activaţi modul de simulare. Treceţi în modul CLI (Command Line Interface) de control al comutatorului Switch0. Folosind comanda ping, ilustraţi procesul de completare a tabelului MAC al Switch0. Descrieţi modul în care este aplicat tabelul MAC al switch-ului în dirijarea traficului din cadrul link-ului. Faceţi o captură de ecran a liniei de comandă cu tabelul MAC completat.
6. Activaţi modul de simulare. Treceţi în modul CLI (Command Line Interface) de control al host-ului PC1. Folosind comanda ping, ilustraţi procesul de completare a tabelului ARP al PC1. Descrieţi modul în care este aplicat tabelul ARP al host-ului în dirijarea traficului din cadrul link-ului. Faceţi o captură de ecran a liniei de comandă cu tabelul ARP completat.
7. Treceţi în modul CLI (Command Line Interface) al routerului. Utilizaţi comanda ping pentru a ilustra procesul de completare a tabelului ARP al routerului. Descrieţi modul în care este aplicat tabelul ARP al routerului în dirijarea traficului între subreţele. Faceţi o captură de ecran a liniei de comandă cu tabelul ARP completat.

Realizaţi o dare de seamă asupra lucrului efectuat, care să conţină răspunsuri explicite la fiecare punct formulat în cerinţe.

Încărcaţi fişierul cu darea de seamă şi fişierele .pkt în mapa corespunzătoare *Lucrarea de laborator N1* din pagina dedicată cursului de Reţele de Calculatoare a platformei educaţionale moodle.usm.md.