UNIVERSITATEA TEHNICĂ A MOLDOVEI

ÎNDRUMAR METODIC
PENTRU LUCRĂRILE DE LABORATOR

PARTEA II
ARHITECTURA REȚELELOR DE CALCULATOARE

Chișinău
2025

UNIVERSITATEA TEHNICĂ A MOLDOVEI

FACULTATEA CALCULATOARE, INFORMATICĂ ŞI MICROELECTRONICĂ

ÎNDRUMAR METODIC
PENTRU LUCRĂRILE DE LABORATOR

PARTEA II
ARHITECTURA REȚELELOR DE CALCULATOARE

Chişinău
Editura „Tehnica-UTM”
2024

CZU

Lucrarea a fost discutată și aprobată pentru editare la ședința Consiliului Facultății Calculatoare, Informatică şi Microelectronică,

Lucrarea este destinată studenților Facultatății Calculatoare, Informatică și Microelectronică, care studiază cursul *Arhitectura sistemelor de calcul*, însă poate fi consultată și de studenții altor facultăți în cadrul cursurilor de rețele de calculatoare. Ciclul conține patru lucrări de laborator destinate simulării rețelelor de calculatoare în mediul de simulare **Cisco Packet Tracer** studiat în cadrul cursului *Arhitectura sistemelor de calcul.* Fiecare lucrare de laborator include materialul teoretic necesar pentru înțelegerea principiilor de funcționare a instrucțiunilor utilizate, ordinea de efectuare a programelor și exercițiilor propuse, precum și cerințele pentru perfectarea raportului.

Autori: conf. univ., dr. Vasilii CREȚU
lect. univ., dr. Nicolae MAGARIU

Recenzenți: conf. univ., dr. Nicolae ABABII
conf. univ., dr. Victor ABABII

DESCRIEREA CIP A CAMEREI NAŢIONALE A CĂRŢII

ISBN

INSTRUCȚIUNI GENERALE

Lucrările de laborator la disciplina *Arhitectura sistemelor de calcul* sunt destinate aprofundării cunoștințelor teoretice și obținerii abilităților practice de lucru cu rețelele de calculatoare. Pentru a participa la lucrările de laborator, studenții trebuie să parcurgă partea teoretică a cursului. Ei sunt instruiți prealabil privind tehnica securității muncii în laboratoarele cu calculatoare, cu semnarea fișei de instructaj. Cunoașterea materialului teoretic este esențială. Studenții trebuie să fie familiarizați cu materialele teoretice aferente temei respective și să înțeleagă modul de desfășurare a laboratorului. Prezența profesorului sau a asistentului este obligatorie pe tot parcursul laboratorului. Aceștia vor oferi asistență și îndrumare pe durata desfășurării lucrării. Echipamentul de laborator, inclusiv calculatoarele și orice echipamente specifice (de exemplu emulatorul de microprocesor), trebuie utilizate în conformitate cu instrucțiunile de rigoare. Fiecărui student i se dă o sarcina individual. La sfârșitul lucrării de laborator, studentul comunică profesorului sau asistentului codul programului și rezultatele obținute.

Elementele de bază pentru darea de seamă cuprind: denumirea și scopul lucrării, codul programului, rezultatele îndeplinirii programului. Termenul de predare a lucrării de laborator constituie data următoarei lucrări. Toate lucrările de laborator din ciclul prezent se vor îndeplini în mediul de simulare **Cisco Packet Tracer 6.0.1** versiunea **student**.

INTRODUCERE ÎN PROGRAMUL CISCO PACKET TRACER 6.0.1

Cisco Packet Tracer este un instrument de modelare și vizualizare a rețelei care permite utilizatorilor să configureze diverse echipamente de telecomunicații Cisco, inclusiv comutatoarele, routerele, telefoanele IP, gateway-urile, serverele și ecranele de rețea. Interfața sa ușor de utilizat permite crearea și configurarea lejeră a rețelei, indiferent de cunoștințele privind tehnologiile de rețea sau hardware Cisco. Software-ul este folosit pentru proiectarea rețelei, instruire, pregătirea pentru examenele de certificare CCNA/CCNP și dobândirea de abilități practice în instruirea administratorilor de rețea și rezolvarea problemelor pe dispozitivele Cisco.

În ciuda faptului că Cisco Packet Tracer nu este disponibil pentru descărcare gratuită (disponibil numai pentru membrii Academiei de Rețea Cisco), se poate găsi cu ușurință o distribuție pe rețea. Pentru lucrările de laborator, în continuare, se va utiliza Cisco Pscket Tracer versiunea 6.0.2 for students. Când se utilizează Cisco Packet Tracer, trebuie specificat că se dorește utilizarea accesului pentru oaspeți. În plus, există versiuni gratuite ale Cisco Packet Tracer pentru Android și iOS.

Cisco Packet Tracer este o aplicație versatilă utilizată în diverse domenii, inclusiv în educația în domeniul tehnologiei rețelelor, certificările Cisco, dezvoltarea de aplicații, proiectarea rețelelor, predarea la distanță, testarea dispozitivelor și a protocoalelor, simularea securității rețelelor, instruirea în situații de urgență și pregătirea pentru carieră. Aceasta oferă un mediu sigur pentru învățarea și exersarea conceptelor de rețea, permițând profesioniștilor IT să testeze și să valideze setările, să dezvolte aplicații și servicii într-un mediu de rețea simulat, să proiecteze și să planifice rețele de calculatoare. De asemenea, ajută la pregătirea pentru situații de

urgență și la recuperarea în caz de dezastru în telecomunicații și rețele. În general, Cisco Packet Tracer este un instrument valoros pentru profesioniștii din diverse domenii.

Cisco Packet Tracer este un software care oferă numeroase avantaje în educația și dezvoltarea rețelelor de calculatoare. Acesta oferă un mediu de laborator virtual pentru configurarea și testarea rețelelor fără hardware fizic, reducând costurile și facilitând accesul la resurse. De asemenea, oferă învățarea interactivă, permițând studenților să creeze, să modifice și să experimenteze topologii de rețea într-un mediu securizat. Software-ul este disponibil gratuit, permițând instituțiilor de învățământ să dezvolte competențe de rețea. Acesta oferă o simulare realistă a comportamentului dispozitivelor de rețea, economisește timp la configurare, suportă diverse dispozitive, dezvoltă abilități practice, facilitează colaborarea, permite experimentarea cu protocoale avansate și permite monitorizarea și rezolvarea problemelor.

Mediul de laborator virtual Cisco Packet Tracer permite utilizatorilor să creeze, să configureze și să experimenteze rețele de calculatoare. Acesta oferă mai multe caracteristici, inclusiv crearea de topologii de rețea, permițând configurarea și testarea dispozitivelor și protocoalelor de rețea, oferind învățare prin experiență și prezentând dispozitive Cisco. Mediul virtual facilitează, de asemenea, testarea protocoalelor de rețea, inclusiv TCP/IP, OSPF, EIGRP și VLAN. De asemenea, acesta oferă simulări de securitate și instruire pentru gestionarea incidentelor de securitate. Packet Tracer este valoros pentru instituțiile de învățământ și instructori, oferind o modalitate interactivă și sigură de predare a rețelelor de calculatoare. De asemenea, oferă flexibilitate și economie de timp fără hardware fizic.

Lucrarea de laborator nr.1
PROIECTAREA SUBREȚELELOR PE BAZA UNUI SWITCH

1. Scopul lucrării: a înțelege conceptul de proiectare a subrețelelor, a oferi exerciții practice de proiectare și configurare a subrețelelor și a dezvolta competențe practice în utilizarea echipamentelor de rețea.

2. Noțiuni teoretice generale

Fereastra principală de lucru din Cisco Packet Tracer este interfața centrală unde se realizează proiectarea, configurarea și simularea rețelelor. Această fereastră se deschide automat la pornirea programului și servește ca punct de plecare pentru toate operațiunile ulterioare.

După pornirea Cisco Packet Tracer, utilizatorul va interacționa constant cu fereastra principală de lucru pentru a crea, configura și analiza diverse elemente de rețea. Această fereastră oferă acces la o gamă largă de instrumente și resurse necesare pentru simularea rețelelor complexe și a scenariilor specifice.

1) Fereastra principală de lucru Packet Tracer

1. **Logical/Physical Workspace Tabs**. Spațiu de lucru logic/fizic, sunt utilizate pentru a comuta între spațiile de lucru logice sau fizice.
2. **Workspace.** Spațiu de lucru - acesta este spațiul de lucru principal în Packet Tracer unde se creează topologia necesară (configurația rețelei) și se afișează simularea procesului de comunicare în rețea.
3. **Common Tools Bar.** Bara de instrumente commune - oferă posibilitatea de a selecta instrumente de manipulare a diagramei rețelei, cum ar fi selectarea și modificarea locației

dispozitivelor și evidențierea și repoziționarea dispozitivelor, plasarea etichetelor și notelor, ștergerea, redimensionarea și selectarea unui bloc de date simplu (Simple PDU) sau complex (Complex PDU) definit de utilizator.

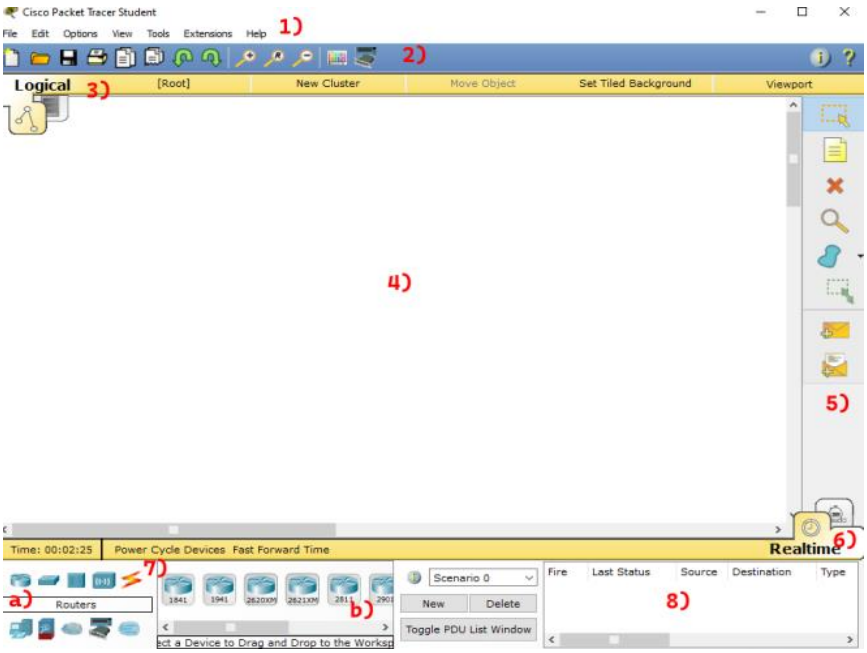

Figura 1.1. Fereastra principală de lucru

4. **Realtime/Simulation Tabs.** Comutatorul de selectare a modului - asigură comutarea între modul de funcționare Realtime/Simulation. Acest comutator oferă, de asemenea, posibilitatea de a controla sincronizarea și capturarea pachetelor de pe rețea.
5. **Network Component Box.** Caseta Componente de rețea conține echipamente de rețea și puncte finale disponibile în Packet Tracer. Este împărțită în două zone:

a) **Device-type Selection Box.** Caseta de selectare a tipului de dispozitiv conține categoriile de dispozitive de bază (routere, switch-uri, hub-uri, dispozitive fără fir, cabluri de rețea, puncte finale și diverse);

b) **Device-specific Selection Box.** Caseta de selecție specifică dispozitivelor. După selectarea unei categorii, aici devin disponibile diverse modele de dispozitive.

6. **User-created Packet Box.** Caseta de pachete create de utilizator este concepută pentru ca utilizatorii să creeze teste detaliate de topologie a rețelei și să afișeze rezultatele acestora.

2) Crearea unei diagrame de rețea simplă

În fereastra Network Component Selection, în categoria End Devices (Dispozitive finale) se selectează Genetic PC și Generic Laptop. Ambele dispozitive se trag în spațiul de lucru Packet Tracer. În continuare se face clic pe Connections (Conexiuni), apoi se selectează Copper Cross-Over (Cupru încrucișat). Clic mai întâi pe imaginea PC-ului și se selectează interfața FastEthernet a dispozitivului în lista care se deschide. În continuare, se face clic pe imaginea laptopului și se selectează interfața FastEthernet. Când sunt conectate corect, indicatorii de stare ai dispozitivului ar trebui să fie verzi, ceea ce indică faptul că interfețele dispozitivului sunt activate.

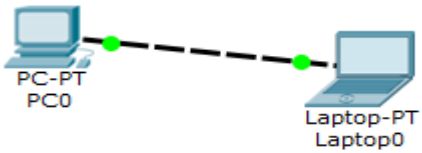

Figura 1.2. O simplă topologie de subrețea

Pentru a seta un dispozitiv, cum ar fi un PC, se face clic pe imaginea acestuia, apoi se selectează fila Desktop (figura 1.3.). Se selectează instrumentul IP Configuration (Configurare IP) și se introduce IP Address (Adresă IP) și Subnet Mask (Mască de subrețea) ale dispozitivului.

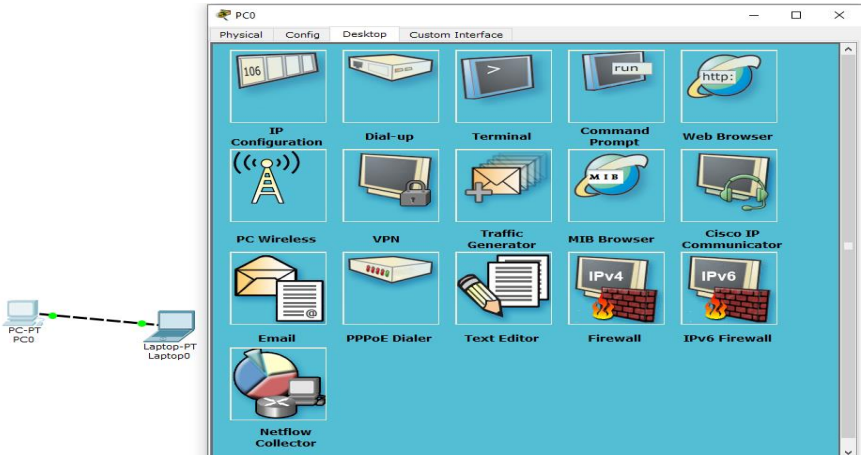

Figura 1.3. PC desktop

Pentru schemă, se poate renunța la adresele IP ale gateway implicit și ale serverului DNS, deoarece nu sunt necesare (schema constă doar din pasarela implicită și serverul DNS). Serverul DNS nu este necesar (schema constă doar din două calculatoare și nu implică accesul la internet sau conectarea la alte rețele, precum și utilizarea de nume simbolice).

Se închide fereastra PC Setup. Clic pe imaginea notebook-ului și se configură notebook-ul în același mod. Se verifică dacă adresele IP specificate se află în aceeași subrețea. Se închide fereastra de configurare a adreselor IP, apoi se deschide instrumentul Command Prompt (Prompt de comandă). Utilizând instrumentul ping, se execută un test de conectivitate (figura 1.5).

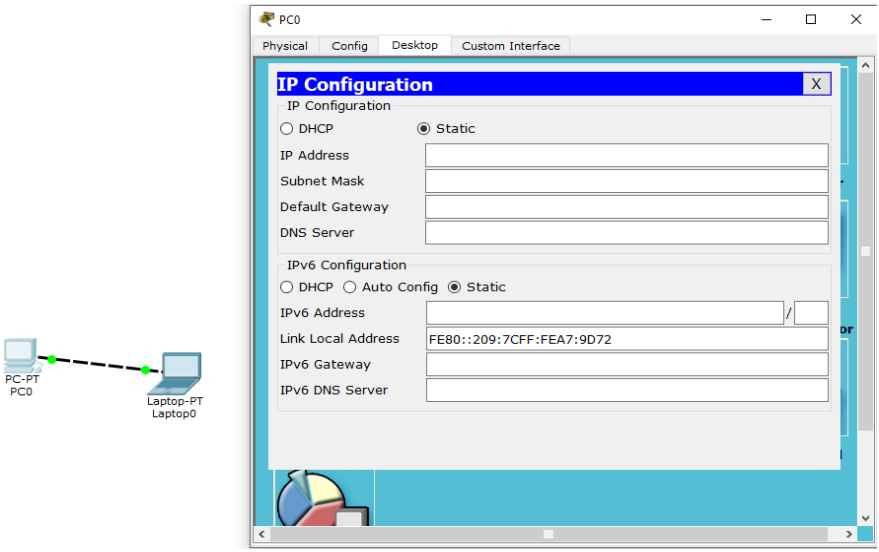

Figura 1.4. Configurarea adresei și a măștii IP a PC-ului

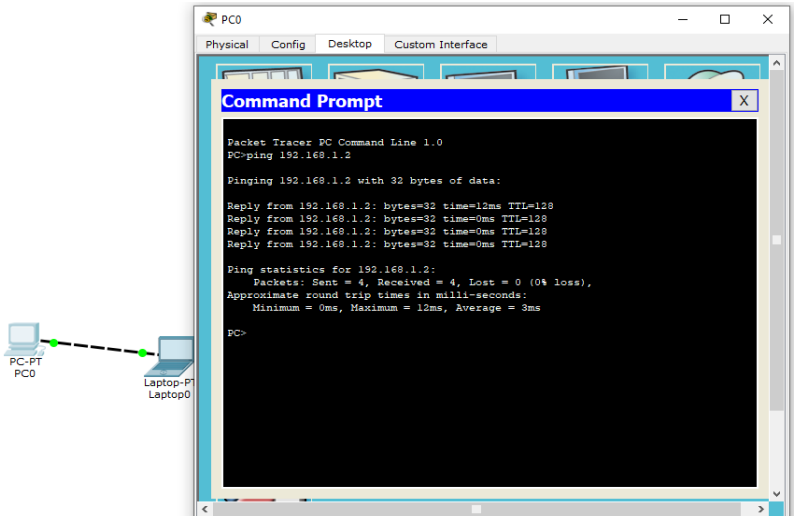

Figura 1.5. Test de conectare între dispositive

Configurația rețelei luate în considerare este relativ simplă. În realitate, o rețea modernă necesită echipamente de rețea. Se complica topologia prin adăugarea unui comutator Ethernet.

Pentru aceasta, din categoria de dispozitive Switches (Comutatoare) se selectează și se trage în spațiul de lucru orice tip de comutator (cu excepția Switch-PT-Empty) din fereastra de selectare a tipului de dispozitiv. Se șterge cablul dintre PC și laptop cu ajutorul instrumentului Delete (Ștergere) din bara de instrumente generală. Clic pe categoria Connections (Conexiuni), apoi se selectează Cooper Straight-Through (Cooper direct-prin trecere) și se conectează PC-ul și laptopul la Switch (Comutator). Când este conectat, luminile comutatorului vor deveni portocalii, deoarece porturile comutatorului sunt în modurile de ascultare și de setare pentru protocolul Spanning Tree Protocol (STP).

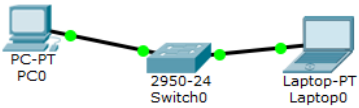

Figura 1.6. Schema retelei cu comutator

Îndată ce LED-urile își schimbă culoarea (ceea ce indică faptul că porturile switch-ului funcționează corect), se va efectua un test de conectivitate între PC și laptop cu ajutorul utilitarului ping. Se va salva topologia modificată sub un alt nume (meniul File> Save As). Schema este salvată într-un fișier cu extensia .pkt. Starea și setările curente ale dispozitivelor sunt memorate.

3) Linia de comandă (Command Prompt)

Acest utilitar imită linia de comandă a sistemului de operare al Microsoft Windows. Cu toate acestea, este acceptat un set limitat de comenzi, care este suficient pentru testarea rețelei.

Sunt disponibile următoarele comenzi:

? - este folosită pentru a obține ajutor contextual, se va afișa o listă a opțiunilor disponibile sau a comenzilor care pot fi introduse în continuare. Se va obține o listă a comenzilor disponibile la nivelul respectiv. Acest lucru ajută la navigarea prin comenzile disponibile, la amintirea sintaxei corecte sau aflarea opțiunilor disponibile în cadrul acelei comenzi specific;

arp – este utilizată pentru a afișa sau manipula tabelul ARP (Address Resolution Protocol). Tabelul ARP asociază adresele IP cu adresele MAC (Media Access Control) în rețelele de tip Ethernet. Comanda *arp* poate fi folosită cu diferite opțiuni pentru a realiza diverse acțiuni. *Router> arp* – această comandă va afișa tabelul ARP curentă cu asocierile dintre adresele IP și adresele MAC. *Router> arp <adresa_IP>,* înlocuiți *<adresa_IP>* cu adresa IP pentru care doriți să aflați asocierea cu adresa MAC. *Router> clear arp <adresa_IP>* – această comandă șterge intrarea corespunzătoare adresei IP specificate din tabelul ARP. *Router> clear arp* – această comandă șterge toate intrările din tabelul ARP. E de menționat că comportamentul exact al comenzii *arp* poate varia în funcție de platforma și versiunea Cisco Packet Tracer utilizată. De obicei, aceste comenzi sunt utilizate mai frecvent în mediile reale de rețea;

delete – este folosită pentru ștergerea unui fișier sau director. Structura acestei comenzi: *delete <nume_fișier>,* unde *<nume_fișier>* reprezintă numele fișierului sau directorului care este necesar a fi șters. Într-un mediu real, această comandă poate fi utilizată pentru a șterge fișiere de configurare sau alte date;

dir – este folosită pentru a afișa lista de fișiere și directoare din directorul curent. Aceasta este o comandă specifică pentru vizualizarea conținutului unui director. E de menționat că Cisco Packet Tracer, fiind un simulator pentru dispozitive de rețea Cisco, nu simulează toate aspectele unui sistem de operare complet. Comanda *dir* este specifică unui sistem de fișiere și director, iar în acest context se referă la vizualizarea fișierelor și directoarelor în directorul curent al dispozitivului;

ftp – este utilizată pentru a iniția o conexiune FTP (File Transfer Protocol) către un server FTP. Aceasta permite transferul de fișiere între dispozitivul Cisco Packet Tracer și un server FTP extern. Structura generală a comenzii *ftp* este: *ftp <adresa_server_ftp>* – această comandă deschide o sesiune FTP și permite introducerea numelui de utilizator și parolei pentru a se conecta la serverul FTP specificat. După stabilirea conexiunii, se pot efectua operațiuni precum descărcarea și încărcarea de fișiere între dispozitivul Cisco Packet Tracer și serverul FTP;

Help – este folosită pentru a afișa o listă a comenzilor disponibile și pentru a furniza informații scurte despre modul în care acestea sunt utilizate. Aceasta oferă un sumar al comenzilor și opțiunilor disponibile, permițând utilizatorului să exploreze și să înțeleagă funcționalitățile oferite de simulator;

ipconfig – este specifică sistemelor de operare Windows și este folosită pentru a afișa informații despre configurația rețelei, adresele IP, gateway-urile, masca de subrețea și alte detalii legate de interfața de rețea a unui dispozitiv;

netstat – funcționează împreună cu comanda *ifconfig* pentru a afișa starea unei interfețe de rețea TCP/IP. De exemplu, cu ajutorul comenzii *netstat -in* și a indicatorului *-i* se pot vizualiza informații despre interfețele de rețea, în timp ce indicatorul *-n* este utilizat

pentru a imprima adresele IP în loc de numele gazdelor. Această comandă se poate utiliza pentru a verifica interfețele, adresele și numele de gazdă SLIP;

Ping – este utilizată pentru a testa conectivitatea între dispozitivele de rețea. Când se utilizează comanda ping, aceasta trimite pachete ICMP (Internet Control Message Protocol) către o adresă IP specificată sau un nume de domeniu și așteaptă un răspuns. *Router> ping 192.168.1.1,* sau pentru a testa un nume de domeniu *Router> ping www.google.com.* Aceasta va trimite pachete de test către adresa IP asociată dispozitivului sau numărului de domeniu specificat și va afișa informații despre reușita sau nereușita comunicării;

Snmpget – se referă la utilizarea protocolului SNMP (Simple Network Management Protocol) pentru a interoga o entitate gestionată și pentru a obține informații despre starea sau configurația dispozitivului. Într-un mediu real, comanda *snmpget* ar fi folosită pentru a interoga dispozitivele de rețea pentru a obține informații despre starea lor, cum ar fi numărul de pachete transmise, starea interfețelor etc. *Router> snmpget -v2c -c public 192.168.1.1 sysDescr.0:*

-v2c: Specifică versiunea SNMP;

-c public: Comunitatea SNMP (parolă, adesea "public" în medii de testare);

192.168.1.1: Adresa IP a dispozitivului;

sysDescr.0: Identificatorul de obiect SNMP (OID) care specifică informații despre dispozitiv;

snmpgetbulk este utilizată în principal pentru a minimiza numărul de cereri SNMP necesare pentru a obține o cantitate mai mare de date, permițând astfel o comunicare mai eficientă între managerul SNMP și dispozitivul gestionat. Este folosită în special în

situații în care trebuie recuperate un număr mare de variabile SNMP într-o singură solicitare. *Router> snmpgetbulk -v2c -c public -Cn0 -Cr10 192.168.1.1 sysDescr:*

-v2c: Specifică versiunea SNMP;

-c public: Comunitatea SNMP (parolă, adesea "public" în medii de testare);

-Cn0: Numărul minim de variabile returnate într-o cerere;

-Cr10: Numărul maxim de iterații ale variabilelor returnate într-o cerere;

192.168.1.1: Adresa IP a dispozitivului;

sysDescr: Identificatorul de obiect SNMP (OID) care specifică informații despre descrierea sistemului;

snmpset - este folosită pentru a seta valorile unor obiecte de gestionare. Comanda *snmpset* este parte a suitei SNMP și este folosită pentru a modifica valorile variabilelor stocate pe un dispozitiv gestionat. O comandă *snmpset* poate fi structurată astfel: *snmpset -v:[versiune] -c:[comunitate] -r:[adresa_ip_dispozitiv] [OID] [tip_date] [valoare];*

-v:[versiune]: Specifică versiunea SNMP (de exemplu, -v:2c pentru SNMPv2c);

-c:[comunitate]: Comunitatea SNMP (parola);

-r:[adresa_ip_dispozitiv]: Adresa IP a dispozitivului gestionat;

[OID]: Identificatorul de obiect SNMP (OID) care indică obiectul de gestionat pe care dorim să îl modificăm;

[tip_date]: Tipul de date al obiectului SNMP;

[valoare]: Noua valoare pe care dorim să o atribuim obiectului SNMP identificat prin OID.

Comanda *snmpset* poate afecta funcționarea dispozitivului și trebuie utilizată cu grijă, având în vedere drepturile de securitate și accesul la dispozitivul gestionat. De asemenea, este important ca dispozitivul să suporte operațiunea de setare SNMP, iar comunitatea

SNMP să fie configurată corespunzător pentru a permite modificările.

Ssh - este adesea folosită în medii reale pentru a stabili o conexiune sigură la distanță la un dispozitiv sau un server care acceptă protocolul SSH (Secure Shell). Într-un mediu real, utilizatorul poate utiliza comanda *ssh* într-un terminal pentru a se conecta printr-un canal securizat la un dispozitiv sau server. *ssh [utilizator]@[adresa_ip_dispozitiv]:*

[utilizator]: Numele utilizatorului cu care doriți să vă conectați la dispozitiv;

[adresa_ip_dispozitiv]: Adresa IP a dispozitivului la care doriți să vă conectați;

telnet - poate fi utilizată pentru simularea conexiunilor Telnet către dispozitivele din rețea. Această comandă este folosită pentru a stabili o conexiune text-based (bazată pe caractere) cu un dispozitiv care acceptă conexiuni Telnet. *telnet [adresa_ip_dispozitiv]*. *[adresa_ip_dispozitiv]* adresa IP a dispozitivului la care doriți să vă conectați. Dacă conexiunea Telnet este configurată cu o parolă, se va solicita introducerea informațiilor de autentificare, cum ar fi numele de utilizator și parola. E de menționat că utilizarea Telnet într-un mediu de producție poate avea riscuri de securitate, deoarece informațiile sunt transmise în format text, fără criptare. În medii reale, este recomandată utilizarea SSH (Secure Shell) în locul Telnet pentru conexiuni securizate;

Tracert / traceroute - este utilizată pentru a urmări traseul unui pachet în rețea, afișând toate nodurile intermediare prin care pachetul trece pentru a ajunge la destinație. *traceroute [adresa_destinație]*. *[adresa_destinație]* – adresa IP a destinației către care se urmărește traseul. Această comandă va furniza o listă a tuturor nodurilor intermediare prin care trece un pachet pe drumul către destinație. Va arăta și timpii de răspuns de la fiecare nod. Numele exact al comenzii și sintaxa pot varia în funcție de versiunea Cisco Packet Tracer sau de imaginea platformei pe care se utilizează.

Fiecare comandă suportă parametri care pot fi descifrați prin introducerea comenzii fără nicio opțiune, așa cum se arată în fig.1.7.

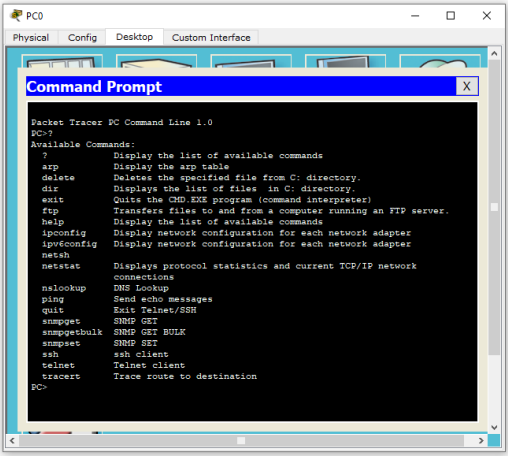

Figura 1.7. Linia de comandă și comenzile de bază de nivel superior

4) Echipamente de rețea Cisco și dispozitive Packet Tracer

Majoritatea dispozitivelor prezentate în Packet Tracer corespund mai mult sau mai puțin echipamentelor Cisco reale. Cu toate acestea, există dispozitive care sunt unice pentru Packet Tracer. Aceste dispozitive se află în subsecțiuni ale categoriilor Switches and Routers (Comutatoare și routere) și au cuvântul Generic în denumire. Inițial, sloturile lor sunt goale și permit instalarea diferitelor tipuri de module.

a) Routerele

Routerele asigură comunicarea dintre subrețele (segmente logice). Orice router din Packet Tracer poate fi pornit și oprit prin comutarea comutatorului "Power" (Alimentare), situat în vederea externă a dispozitivului ("Physical Device View") (figura 1.8).

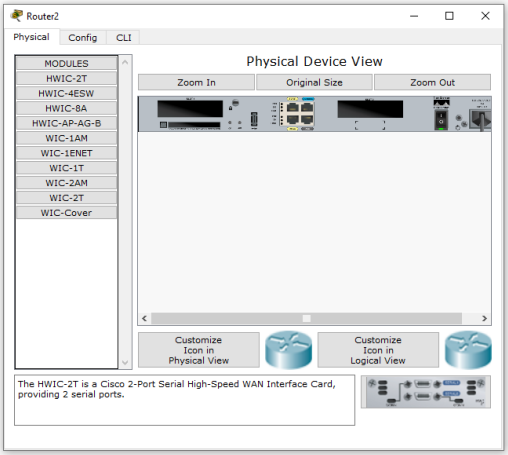

Figura 1.8. Fila "Vedere fizică a dispozitivului" (este indicat comutatorul de comutare "Power" al routerului)

Capacitatea de a porni/opri puterea routerelor în Packet Tracer simulează funcționarea unor dispozitive reale. Un modul de dispozitiv poate fi adăugat și eliminat numai după ce se oprește alimentarea cu energie a dispozitivului. Dacă nu este salvată configurația curentă, oprirea dispozitivului va duce la pierderea setărilor efectuate.

În Packet Tracer sunt disponibile următoarele routere:

1. Cisco 1841. Router de servicii integrate (Integrated Service Router (ISR), are două porturi Fast Ethernet și două sloturi libere pentru conectarea plăcilor de circuite integrate, pentru circuite de mare viteză conexiune WAN de mare viteză.
2. Cisco 1941 (Cisco 1941). Acest model este asemănător cu cel precedent, cu singura diferență că funcționează sub controlul Cisco IOS versiunea 15. De asemenea, dispune de două porturi Gigabit Ethernet.

3. Cisco 2620XM. Acest router multiserviciu are un port Fast Ethernet, două sloturi pentru instalarea interfeței WAN carduri WAN și un slot pentru AIM.
4. Cisco 2621XM. Acest router este similar cu cel precedent, cu excepția faptului că are două porturi Fast Ethernet.
5. Cisco 2811. Un router cu servicii integrate, are două porturi Fast Ethernet, patru sloturi WIC și două sloturi AIM.
6. Cisco 2901. Acest router are două porturi Gigabit Ethernet, patru sloturi WIC și două sloturi DSP.
7. Cisco 2911. Acest router are trei porturi Gigabit Ethernet Ethernet, în rest, are aceleași caracteristici ca și ale dispozitivului anterior. Funcționează sub versiunea 15 a Cisco IOS.
8. Genetic Router-PT. Un router cu personalizare. Are 10 sloturi și mai multe module speciale al căror nume începe cu literele PT.

b) Comutatoarele

Un comutator (denumit anterior punte multiport) conectează mai multe puncte terminale într-o rețea. Fiecare port al unui comutator este un domeniu de coliziune. În Packet Tracer sunt disponibile următoarele comutatoare:

1. Cisco 2950-24. Un comutator gestionat care acceptă 24 de porturi Fast Ethernet.
2. Cisco 2950T-24. Acest switch aparține familiei de switch-uri inteligente Catalyst 2950 și are 24 de porturi Fast Ethernet și două porturi Gigabit Ethernet cu suport pentru module GBIC (Gigabit Interface Converter).
3. Cisco 2960-24TT. Un alt switch cu 24 de porturi. Spre deosebire de modelul anterior, are porturi Gigabit Ethernet cu suport pentru module SFP (Small Form-factor Pluggable). Cu

toate acestea, această diferență este esențială pentru switch-urile reale și nu are nicio influență când se lucrează în Packet Tracer.

4. Cisco 3560-24PS. Spre deosebire de alte switch-uri, acest dispozitiv este un comutator de nivelul 3 și, pe lângă funcția standard de comutare, este capabil să efectueze rutarea. Ultimele două litere PS înseamnă suport pentru Power over Ethernet PoE, care este utilizat pentru a alimenta telefoanele IP fără o sursă de alimentare separată.
5. Bridge PT. Acest dispozitiv este utilizat pentru segmentarea rețelei și are doar două porturi.
6. Comutator generic PT. Acest dispozitiv există numai în Packet Tracer și este un comutator configurabil de către utilizator. Are 10 sloturi și mai multe module specializate.

La fel ca și Router-PT Genetic discutat anterior, Generic Switch PT poate fi dezactivat, ceea ce este necesar pentru a schimba modulele. Toate celelalte comutatoare au o structură fixă și nu implică personalizare. Prin urmare, nu este necesară oprirea sursei de alimentare.

c) Alte dispozitive

După cum se observă, Packet Tracer nu acceptă doar switch-uri și routere, ci și alte dispozitive. Aceste dispozitive sunt configurate și funcționează în felul următor:

1. Hub PT. Construirea rețelelor bazate pe hub-uri este domeniul istoriei. Cu toate acestea, cu acest dispozitiv se examinează problema de difuzare și coliziuni. Are 10 sloturi.
2. Repeater (Repetitor). Utilizat pentru a îmbunătăți și a restabili nivelul și forma unui semnal electric. Are două sloturi.

3. Splitter coaxial PT. Conceput pentru a diviza o conexiune coaxială. Are trei porturi pentru conexiunea coaxială și nu poate fi personalizat.

5) Conectarea modulelor de dispozitive de rețea

Modulele de dispozitive de rețea sunt implementări hardware ale unor interfețe comune. De exemplu, modulul HWIC-4ESW conține 4 porturi Ethernet (10 Mbps). Ca și în cazul dispozitivului real, precum și în cazul dispozitivului reprezentat în Packet Tracer, este necesară oprirea alimentării pentru schimbarea modulului.

Pentru a opri alimentarea, se efectuază un singur clic pe comutatorul de alimentare din partea dreaptă a dispozitivului. Pentru a instala un modul, se trage și se fixează oricare dintre modulele disponibile în lista de module, instalându-se în orice slot liber. În cazul în care un modul nu poate fi instalat într-un anumit slot, acesta va fi readus automat în listă.

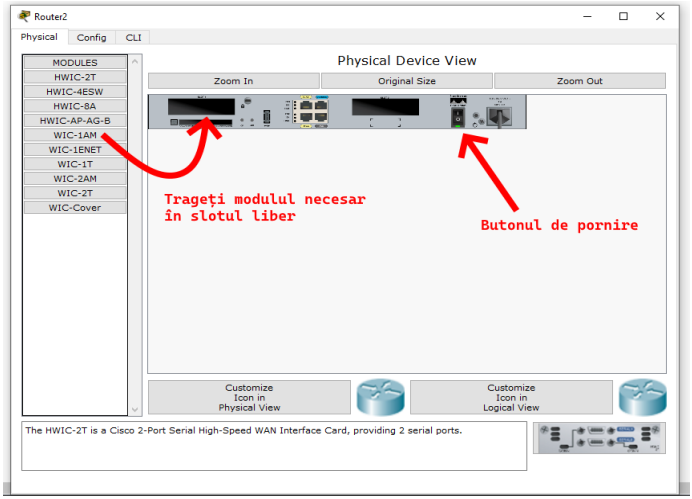

Figura 1.9. Adăugarea unui modul de router

Pentru a elimina un modul, trebuie, de asemenea, oprit și tras din slot înapoi în listă. După schimbarea modulului dispozitivul este pornit din nou.

6) Sistemul de denumire a modulelor

Fiecare router are mai mult de o duzină de module care pot fi identificate după numele lor. Mai jos sunt enumerate modulele grupate în funcție de tipul de conexiune prin cablu.

a) Interfață Ethernet de cupru

Reprezintă interfețele LAN standard la care se conectează un cablu de cupru cu perechi torsadate cu un conector RJ-45. Denumirea acestor interfețe se bazează pe indicarea vitezei: Etnernet (10 Mbps),

FastEtnernet (100 Mbit/s), GigabitEtnernet (1000 Mbit/s). În consecință, denumirile modulelor au trimitere prescurtată la viteza interfeței: E, FE, GE, CFE sau CGE. Modulele denumite SW sunt concepute pentru routere și asigură funcții de comutare:

1. HWIC-4ESW - 4 porturi Ethernet comutate;
2. WIC-1ENET - un singur port Ethernet;
3. NM-1E - un singur port Ethernet;
4. NM-1FE-TX - un singur port Fast Ethernet;
5. NM-4E - 4 porturi Ethernet;
6. NM-ESW-161 - 16 porturi Ethernet comutate;
7. PT-ROUTER-NM-1CE, PT-ROUTER-NM-lCFE, PT-ROUTER-NM-1CGE - module de utilizator Packet Tracer.

b) Modul Ethernet optic

Acest tip de modul este similar cu cel precedent, cu excepția faptului că utilizează cablu optic în loc de cablu de cupru. Aceste module pot fi identificate prin prezența literei F:

1. NM-1FE-FX - un singur port Ethernet pentru mediul de transmisie optic;

2. PT-ROUTER-NM-1FFE, PT-ROUTER-NM-1FGE – personalizat, module Packet Tracer.

c) Interfață serială

Numele acestor module conțin litera T sau o pereche de simboluri A/S. Modulele cu litera T sunt sincrone, iar modulele cu caracterele simbolice A/S sunt asincrone. Diferența în funcționarea lor este evidentă pentru hardware-ul real, în Packet Tracer nu există nicio diferență între ele:

1. WIC-1T, WIC-2T – port serial sincron simplu sau dublu;
2. NM-4A/S, NM-8A/S – patru sau opt porturi seriale asincrone-sincrone;
3. PT-ROUTER-NM-1S, PT-ROUTER-NM-1SS – module de utilizator Packet Tracer.

d) Interfață modem

Acest tip de modul are o interfață RJ-11 pentru conectarea cablurilor telefonice. Astfel de module pot fi identificate prin literele AM, prezente în denumire după numărul care indică numărul de porturi

1. WIC-1AM – port dublu RJ-11 pentru conectarea de telefoane și modem;
2. WIC-2AM, WIC-8AM – două sau opt porturi RJ-11;
3. PT-ROUTER-NM-1AM – modul de utilizator Packet Tracer.

e) Module WIC

Modulele de rețea WIC nu ocupă întregul slot, module (WIC în cadrul modulelor de rețea(NM)) care au sloturi suplimentare pentru a suporta module mai mici. Aceste module pot fi recunoscute prin litera W la sfârșitul denumirii:

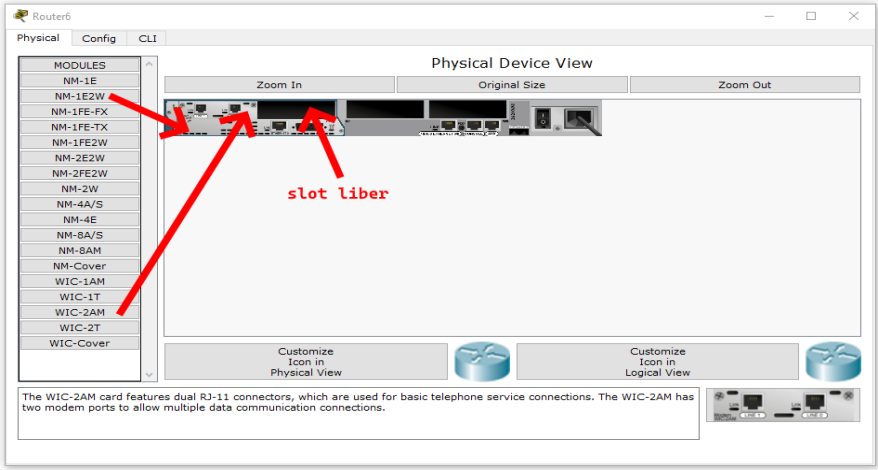

Figura 1.10. Module cu suport pentru modulele WIC

1. NM-1E2W, NM-1FE2W – un port Ethernet/două porturi Fast Ethernet cu suport pentru două sloturi WIC; un port Ethernet/două porturi Fast Ethernet cu suport pentru două sloturi WIC.
2. NM-2E2W, NM-2FE2W – două porturi Ethernet/ Fast Ethernet cu două sloturi WIC;
3. NM-2W – nu are porturi, conceput pentru a suporta două sloturi WIC.

3. Ordinea efectuării lucrării de laborator

1. Să se proiecteze o subrețea pe baza unui switch conform figurii 1.11).
2. Să se atribuie adrese IP și masca subrețelei în regim static (figura 1.12).
3. Să se verifice conexiunea dintre hosturile conectate în subrețea, folosind comanda ping în meniul consolei (figura 1.14).
4. Să se adauge încă un switch și un număr de hosturi (5-7) și să se seteze adresele IP și masca subrețelei pentru hosturile date.

5. Folosind un cablu de conexiune, să se conecteze switchiurile între ele (figura 1.15).
6. Să se verifice conexiunea dintre hosturile subrețelelor nr.1 și nr.2, folosind comanda ping (figura 1.17).
7. Să se noteze și să se facă concluziile în urma efectuării punctelor de mai sus.
8. Să se conecteze un router la subrețeaua proiectată și să se înscrie comenzile în (CLI) pentru configurarea routerului privind atribuierea adreselor IP și masca subrețelei în regim dinamic.
9. Folosind comanda ping, să se verifice conexiunile.

4. Efectuarea lucrării de laborator

Se cere proiectarea unei subrețele bazate pe switch, având la bază topologia prezentată în figura 1.11. Topologia din figură servește drept fundament pentru proiectarea unei subrețele, unde switch-urile joacă un rol central în gestionarea conectivității dintre diferitele segmente ale rețelei:

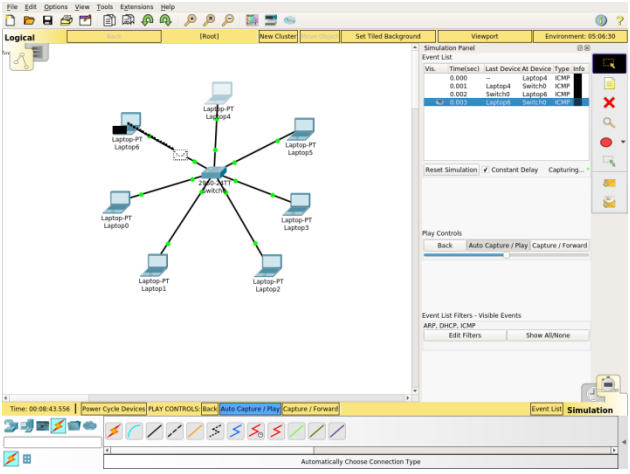

Figura 1.11. Simularea CISCO a subrețelei pe bază de switch

Este necesar să se configureze adresa IP pentru a permite comunicația între două dispozitive dintr-o subrețea. Adresa IP și mască trebuie să fie setate corect pentru a asigura conectivitatea și comunicarea eficientă dintre cele două dispozitive din subrețeaua respectivă.

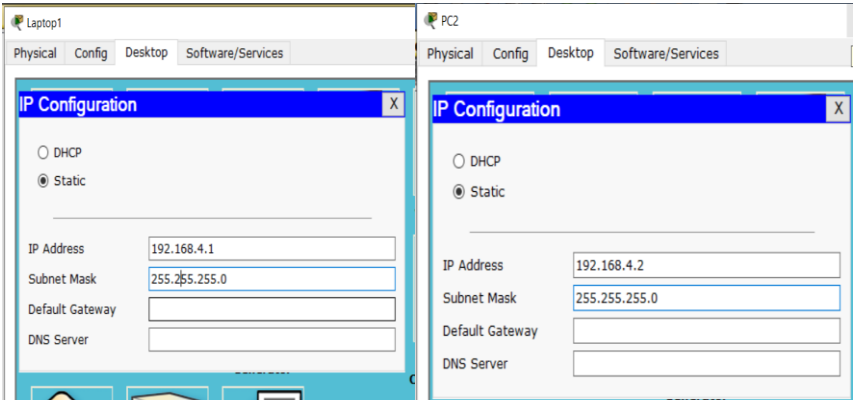

Figura 1.12. Configurarea adreselor IP și a măștilor de subrețea

Pentru a verifica corectitudinea adresei, se utilizează comanda *ipconfig*. Comanda *ipconfig* oferă informații detaliate despre configurația rețelei, inclusiv adresele IP atribuite. Prin analizarea rezultatelor furnizate de comanda *ipconfig,* se poate asigura că adresele IP sunt configurate în mod corespunzător și că dispozitivele din rețea pot comunica eficient.

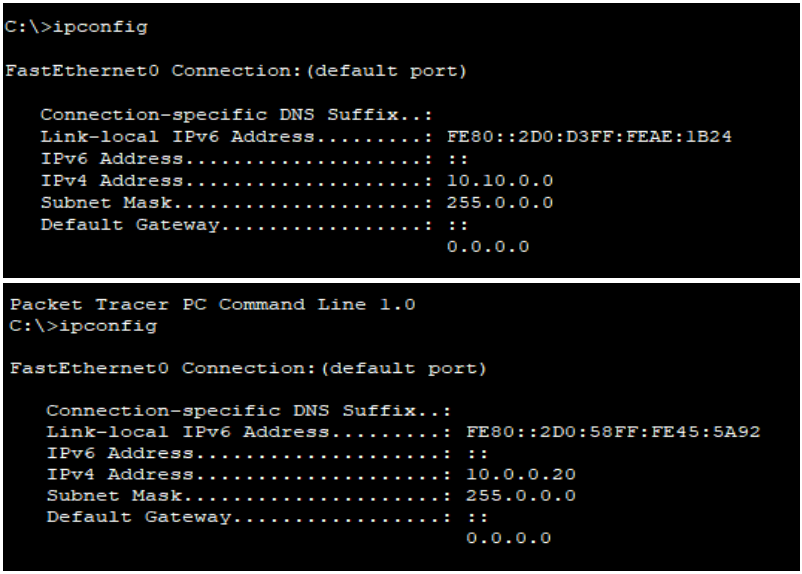

Figura 1.13. Îndeplinirea comenzii ipconfig

După configurarea adresei IP și măștii de subrețea între cele două dispozitive, este necesar să verificați conexiunea dintre ele. Pentru a asigura corectitudinea adresei, utilizați comanda *ipconfig* în linia de comandă a sistemului. Utilizați comanda *ping* pentru a testa dacă există o conexiune funcțională între cele două dispozitive.

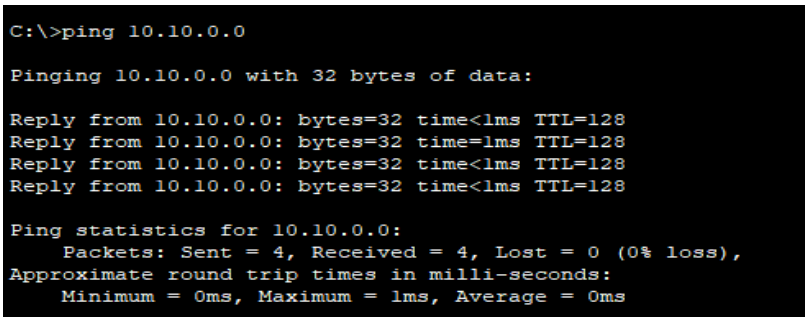

Figura 1.14. Îndeplinirea comenzii ping

În Cisco Packet Tracer s-a creat o nouă subrețea și s-a conectat la rețeaua existentă. Pentru aceasta, s-a adăugat un alt switch în topologie și s-au configurat adresele IP și măștile de subrețea pentru toate cele 5-7 gazde. Hosturile din noua subrețea au fost conectate la noul switch, utilizând cabluri de rețea adecvate. Ulterior, s-a interconectat switch-urile folosind un cablu de rețea. Această configurație a permis unei noi rețele să comunice cu rețeaua originală și să utilizeze dispozitivele interconectate pentru a efectua operațiuni de rețea.

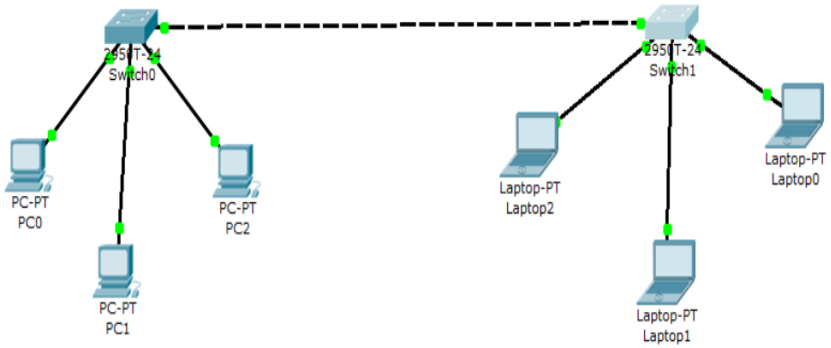

Figura 1.15. Subrețea cu 2 switch-uri

Pentru unul dintre dispozitivele din noua subrețea se va configura o adresă IP și o mască de subrețea corespunzătoare (figura 1.16). Utilizând comanda *ping* din interfața de comandă, se verifică conectivitatea între două hosturi din subrețeaua originală și noua subrețea (figura 1.17). Această verificare se efectuează pentru a asigura că hosturile din cele două subrețele sunt capabile să comunice între ele. Dacă răspunsurile la comenzile *ping* au fost prompte și fără pierderi, acest lucru indica faptul că conexiunea dintre subrețele funcționează corect.

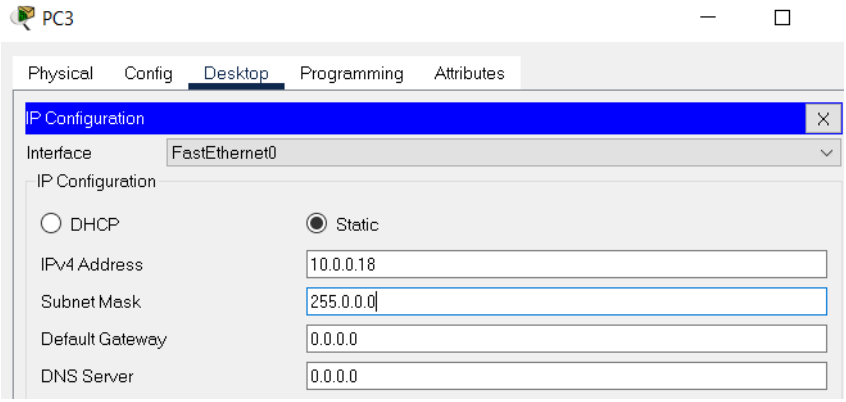

Figura 1.16. Setarea Ip și Masca pentru dispozitivul terminal

```
C:\>ping 10.10.0.0

Pinging 10.10.0.0 with 32 bytes of data:

Reply from 10.10.0.0: bytes=32 time<1ms TTL=128
Reply from 10.10.0.0: bytes=32 time<1ms TTL=128
Reply from 10.10.0.0: bytes=32 time<1ms TTL=128
Reply from 10.10.0.0: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.0.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 1.17. Rezultatul verificarii conexiunii subrețelelor

În cadrul infrastructurii de rețea proiectată s-a integrat un router pentru a îndeplini funcția unui server DHCP. Acest router a fost conectat la subrețeaua proiectată, oferind astfel funcții de routing și atribuire de adrese IP prin intermediul serviciului DHCP. În interfața de comandă a routerului s-au introdus comenzile corespunzătoare pentru configurarea sa în regim dinamic, inclusiv pentru a specifica gama de adrese IP disponibile și a defini parametrii de leasing pentru adresele IP alocate de DHCP. Această configurație a routerului

asigură că dispozitivele conectate la rețea primesc automat o adresă IP și o mască de subrețea de la serverul DHCP al routerului. Serviciul DHCP al routerului simplifică administrarea adresei IP a dispozitivelor în rețea, facilitând adăugarea, modificarea și eliminarea dispozitivelor fără a fi nevoie de configurarea manuală a adreselor IP.

Codul de configurare al router-ului:

```
Router>enable
Router#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface g 0/1
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
exit
Router(config)#ip dhcp pool tibrigan
Router(dhcp-config)#network 192.168.4.2 255.255.255.0
Router(dhcp-config)#default-router 192.168.4.1
Router(dhcp-config)#exit
Router(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
```

Pentru a oferi servicii DHCP în cadrul subrețelei proiectate, pentru a simplifica procesul de alocare și gestionare a adreselor IP pentru dispozitivele conectate, se finalizază configurarea routerului. După finalizarea acestei configurări, s-a setat fiecare dispozitiv

conectat la subrețele să utilizeze DHCP pentru a primi automat o adresă IP și o mască de subrețea.

Această abordare de configurare automată, bazată pe DHCP, elimină necesitatea de a stabili manual adrese IP și oferă o soluție scalabilă și flexibilă pentru creșterea sau modificarea rețelei, facilitând astfel administrarea rețelei.

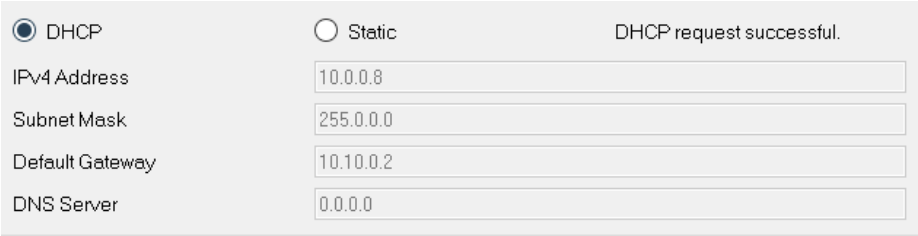

Figura 1.18. Setarea configurării DHCP

5. Conținutul raportului

1. Introducere:
    a. Prezentarea scopului lucrării: obiectivul acestei lucrări constă în proiectarea unei subrețele, utilizând dispozitive de tip switch pentru a asigura o comunicare eficientă între echipamentele conectate.
2. Configurarea Switch-urilor:
    a. Detalii privind setarea parametrilor switch-urilor, cum ar fi adresa IP, masca de subrețea și gateway-ul.
    b. Descrierea topologiei subrețelei, inclusiv numărul de switch-uri și echipamente conectate.
3. Conectarea dispozitivelor la Switch:
    a. Pași detaliați pentru conectarea echipamentelor la switch-uri.
    b. Verificarea fizică a conexiunilor și asigurarea unei infrastructuri fizice corespunzătoare.

4. Configurarea adreselor IP:
    a. Instrucțiuni privind configurarea adreselor IP pentru dispozitivele conectate la switch-uri.
    b. Utilizarea comenzilor specifice pentru setarea parametrilor de rețea.
5. Verificarea conexiunilor și testarea comunicării:
    a. Utilizarea comenzilor precum ping pentru a verifica conectivitatea dintre echipamente.
    b. Testarea comunicației dintre diferitele dispozitive pentru a asigura o funcționalitate corespunzătoare.
6. Probleme întâmpinate și soluții:
    a. Identificarea potențialelor probleme și descrierea modului în care acestea au fost rezolvate.
    b. Sugestii pentru optimizarea performanței subrețelei.
7. Concluzii:
    a. Sumar al rezultatelor obținute în cadrul lucrării.
    b. Observații și concluzii generale privind proiectarea și implementarea subrețelei.
8. Referințe:
    a. Menționarea tuturor resurselor și documentației utilizate în procesul de proiectare și configurare a subrețelei.
9. Anexe:
    a. Detalii suplimentare, capturi de ecran sau diagrame care completează informațiile din cadrul raportului.

Întrebări de control

1. Ce pași ați urmat pentru configurarea switch-urilor din subrețea?
2. Cum ați setat adresele IP și măștile de subrețea pentru switch?

3. Care sunt pașii de bază pentru conectarea echipamentelor la switch-uri?
4. Ce comenzi specifice ați utilizat pentru configurarea adreselor IP ale dispozitivelor?
5. Cum ați asigurat unicitatea adreselor IP în subrețea?
6. Ce comenzi specifice ați utilizat pentru configurarea adreselor IP ale dispozitivelor?
7. Cum ați asigurat unicitatea adreselor IP în subrețea?
8. Cum ați documentat adresele IP și configurațiile switch-urilor?
9. Cum se configurează adresa IP pe un switch într-o subrețea specifică?
10. Care sunt pașii pentru atribuirea unei măști de subrețea unui switch?
11. Ce comenzi sunt necesare pentru a configura adresa IP pe un dispozitiv conectat la switch?

Bibliografie

1. Tanenbaum, Andrew S., and David J. Wetherall. "Computer Networks." Pearson, 2010.
2. Cisco. "CCNA Routing and Switching Portable Command Guide." Cisco Press, 2013.
3. Doyle, Jeff. "Routing TCP/IP, Volume 1." Cisco Press, 2017.
4. Lammle, Todd. "CCNA Routing and Switching Complete Study Guide." Wiley, 2016.
5. Odom, Wendell. "CCNA Routing and Switching ICND2 200-105 Official Cert Guide." Cisco Press, 2018.
6. Spurgeon, Charles E. "Ethernet: The Definitive Guide." O'Reilly Media, 2014.

7. Garg, Dinesh C., and Rick McDonald. "Switching Basics and Intermediate Routing CCNA 3 Companion Guide." Cisco Press, 2007.
8. Halabi, Sam. "Internet Routing Architectures." Cisco Press, 1997.
9. Albitz, Paul, and Cricket Liu. "DNS and BIND." O'Reilly Media, 2017.
10. Tanenbaum, Andrew S. "Computer Networks." Pearson, 2010.

Lucrarea de laborator nr.2
PROIECTAREA SUBREŢELELOR ROUTING ÎNTRE DIFERITE SUBREŢELE

1. Scopul lucrării: a înțelege conceptul de subrețea, a oferi instrucțiuni practice pentru configurarea dispozitivelor de rutare și optimizarea fluxului de date în rețele.

2. Noţiuni teoretice generale

1) Configurarea rutelor utilizând Command Line Interface (CLI)

Rutarea permite comunicarea între mai multe subrețele logice. Configurarea rutării cu ajutorul interfeței de linie de comandă (CLI) Packet Tracer Interfața de linie de comandă (CLI) a Packet Tracer nu este diferită de configurarea hardware-ului propriu-zis. De asemenea, se poate utiliza interfața grafică a Packet Tracer, concepută pentru configurarea rutării statice și a rutării dinamice RIP. Pe lângă aceasta, se observă și echilibrarea sarcinii, ceea ce va permite înțelegerea mai bună a principiilor de rutare

2) Rutarea statică

Rutarea statică este o metodă simplă utilizată în diverse forme și se găsește în majoritatea rețelelor. În cadrul Packet Tracer se poate configura rutarea statică, folosind interfața grafică. În acest mod de configurare, se introduce adresa rețelei de destinație și gateway-ul necesar pentru a ajunge la acea rețea specifică. Fiecare router din rețea trebuie să cunoscă cum să ajungă la toate destinațiile din rețea. Rutarea statică implică un efort manual considerabil. Prin urmare, când se adaugă sau se elimină un router din rețea, toate celelalte routere trebuie să actualizeze aceste modificări.

3) Configurarea rutării statice utilizând funcția interfața grafică (GUI)

Pentru exercițiu, folosim topologia din figura 2.1.

Patru routere sunt conectate într-o topologie în inel în această rețea, fără a utiliza interfețe loopback sau a conecta calculatoare. Deci, se va utiliza GUI și această configurație va avea doar câteva instrucțiuni.

Următorul pas:

1) Clic pe imaginea routerului, apoi se trece la fila *Configurație*. După aceea, se selectează interfața dorită și se stabilește adresa IP. Apoi se bifează căsuța de selectare pentru a selecta opțiunea On (Activat). În acest exemplu, se folosesc adresele IP care sunt inserate în tabelul 2.1.

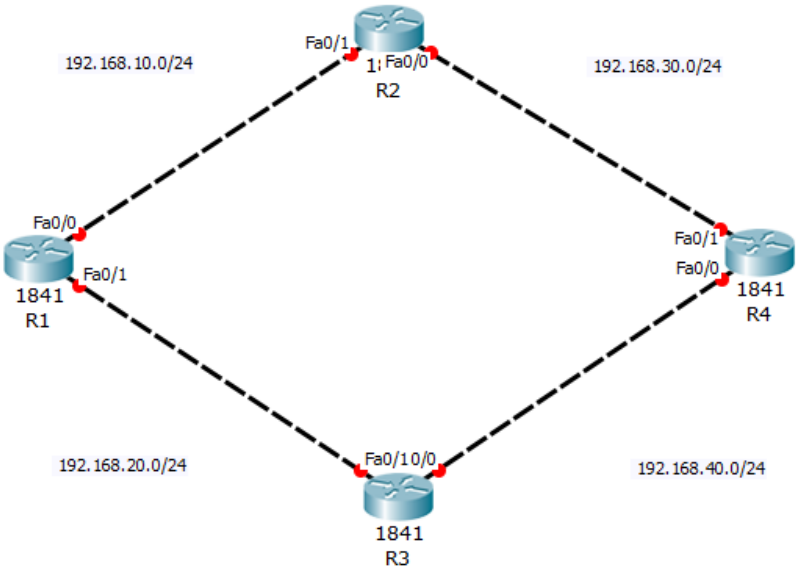

Figura 2.1. Exemplu de retea pentru setarea rutării statice

Tabelul 2.1. Atribuirea de adrese IP la routere

Router	*Interface*	*IP-Address*
R1	FastEthernet0/0	192.168.10.1
	FastEthernet0/1	192.168.20.1
R2	FastEthernet0/0	192.168.10.2
	FastEthernet0/1	192.168.30.1
R3	FastEthernet0/0	192.168.20.2
	FastEthernet0/1	192.168.40.1
R4	FastEthernet0/0	192.168.30.2
	FastEthernet0/1	192.168.40.2

2) În conformitate cu figura 2.2, se selectează Routing Static (Rutare statică) în aceeași filă.

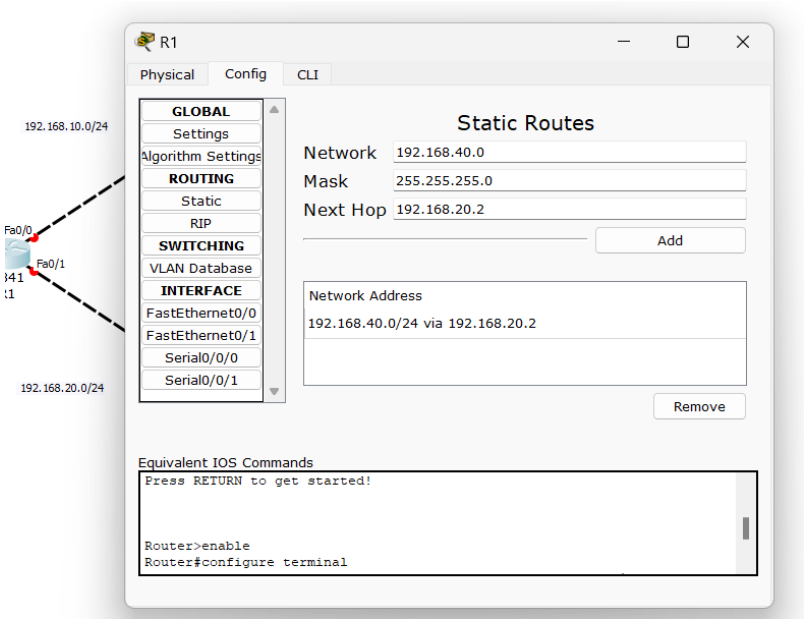

Figura 2.2. Rutarea statică

3) Configurarea rutelor statice necesită inserarea manuală a tuturor rutelor care nu sunt conectate direct în tabelul de rutare. Interfața grafică va fi utilizată pentru a configura rutele statice, folosind setările următoare.

Tabelul 2.2. Rute statice

Router	*Interface*	*IP-Address*
R1	192.168.30.0/255.255.255.0	192.168.10.2
	192.168.40.0/255.255.255.0	192.168.20.2
R2	192.168.20.0/255.255.255.0	192.168.10.1
	192.168.40.0/255.255.255.0	192.168.30.2
R3	192.168.10.0/255.255.255.0	192.168.20.1
	192.168.30.0/255.255.255.0	192.168.40.2
R4	192.168.10.0/255.255.255.0	192.168.30.1
	192.168.20.0/255.255.255.0	192.168.40.1

4) Acum se verifică comunicarea dintre toate routere, folosind instrumentul Simple PDU. Pentru a monitoriza traseul de propagare a pachetelor, se recomandă utilizarea modului de simulare.
5) Cum arată tabelul de rutare? În acest scop, există și un instrument grafic numit „Inspect” (Inspectare), care se află în bara de instrumente generală. Se va face clic pe imaginea lupă, apoi se va efectua clic pe un router. Fiecare router are un tabel de rutare care conține patru rute (figura 2.3).

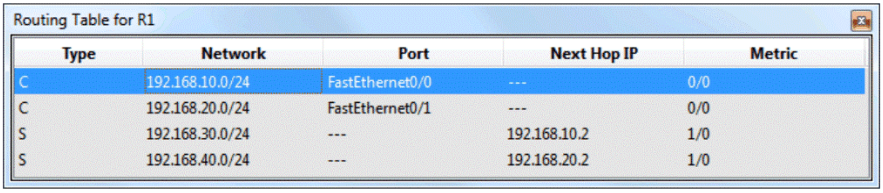

Figura 2.3. Tabelul de rutare (interfata grafică)

În timp ce au fost configurate doar două rute statice, de unde se pot obține alte două rute în tabelul de rutare? Aceste două rute sunt conectate direct la rețele.

Deoarece s-au configurat rutele statice în această topologie, există doar o singură rută specifică care poate ajunge la orice rețea, chiar dacă există rute alternative către fiecare rețea.

Configurarea rutării statice utilizând funcția interfața de linie de comandă CLI. Vom folosi același exemplu din patru routere, pentru a configura o rută statică, folosind CLI. Vom examina procesul de introducere a comenzilor pe un router R1. Pentru aceasta, trebuie aplicate următoarele comenzi:

1) Se va atribui o adresă IP pe interfața fiecărui router, folosind următoarele comenzi:

```
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.10.1
255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 192.168.20.1
255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

2) O rută statică este configurată prin comanda ip route cu următoarea sintaxă:

```
R1(config)#ip route <Destination Prefix>
<Destination prefix mask> <Gateway IP>
```

3) Următoarele comenzi sunt utilizate pentru routerul R1:

```
R1(config)#ip route 192.168.30.0 255.255.255.0
192.168.10.2
R1(config)#ip route 192.168.40.0 255.255.255.0
192.168.20.2
```

Pentru a efectua un test de conectivitate, se utilizează instrumentul PDU simplu.

Dacă apre un mesaj de eroare, se trece în modul de simulare pentru a afla care router a fost configurat incorect.

Setarea algoritmelor de routing pentru subrețelele locale depinde de infrastructura și nevoile rețelei specifice. Există mai multe algoritme de routing disponibile pentru gestionarea traficului într-o rețea locală, iar alegerea algoritmului potrivit depinde de diverse factori, cum ar fi dimensiunea rețelei, topologia, cerințele de performanță și nivelul de securitate dorit.

Iată câteva dintre cele mai comune algoritme de routing utilizate în rețelele locale:

1) Routing Information Protocol (RIP): este un algoritm de routing de tip distanță-vector care utilizează metrica hop count (numărul de salturi) pentru a determina calea optimă. Este potrivit pentru rețelele mici și medii, dar poate prezenta limitări în privința scalabilității și timpului de convergență.
2) Open Shortest Path First (OSPF): este un protocol de routing de tip link-state care atribuie o valoare metrică fiecărei legături din rețea și determină calea cea mai scurtă folosind algoritmul Dijkstra. OSPF este adecvat pentru rețelele de dimensiuni mari și oferă o scalabilitate mai bună decât RIP.
3) Enhanced Interior Gateway Routing Protocol (EIGRP): este un protocol de routing de tip hibrid care combină caracteristicile algoritmului de distanță-vector și ale celui

link-state. EIGRP este dezvoltat de Cisco și este potrivit pentru rețelele complexe care utilizează echipamente Cisco.

4) Border Gateway Protocol (BGP): este un protocol de routing folosit în principal pentru interconectarea rețelelor autonome (AS) la nivelul internetului. BGP utilizează politici de rutare și atribute pentru a determina calea optimă între rețelele autonome.

3. Ordinea efectuării lucrării de laborator

1. Să se proiecteze subrețele reprezentate în figura 2.4.
2. Să se atribuie IP și masca subrețelei pentru fiecare subrețea în parte.
3. Să se verifice conexiunile dintre hosturi, folosind comanda *ping*.
4. Folosind algoritmii de routing, să se seteze comenzile necesare.
5. Să se verifice conexiunea dintre subrețele, folosind comanda *ping.*

4. Efectuarea lucrării de laborator

În cadrul proiectului, se prevăd trei subrețele distincte, care sunt interconectate prin routere și switch-uri, permițând astfel comunicarea dintre calculatoarele din fiecare subrețea.

Subrețeaua cuprinde trei routere care direcționează traficul în funcție de destinație, utilizând setările de rutare statice sau dinamice, iar switch-urile facilitează comunicația la nivel local dintre calculatoarele conectate.

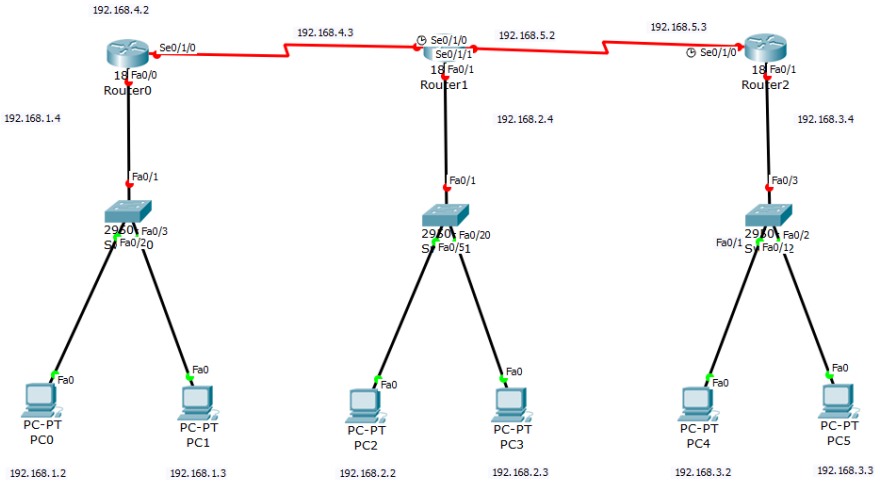

Figura 2.4. Rețeaua locală alcătuită din 3 routere, 3 switch-uri și 6 calculatoare

Proiectarea unei astfel de rețele implică configurarea adecvată a fiecărui router și switch, precum și a setărilor de rețea pentru calculatoarele implicate, pentru a asigura conectivitatea și securitatea rețelei locale. În cadrul programului Cisco Packet Tracer, am configurat rutarea statică pentru a asigura conectivitatea între subrețelele reprezentate în figura 2.4.

S-a introdus adresa rețelei de destinație și gateway-ul asociat pentru fiecare subrețea, asigurându-se astfel că traficul este direcționat corect.

Această abordare de configurare statică a rutei permite să se gestioneze manual direcționarea traficului în cadrul rețelei, controlând astfel fluxul de date și resursele accesibile de la un router la altul.

Configurarea rutării statice pe interfețele routerelor și a gateway-urilor pentru fiecare subrețea asigură comunicarea eficientă dintre diferitele dispozitive și rețele.

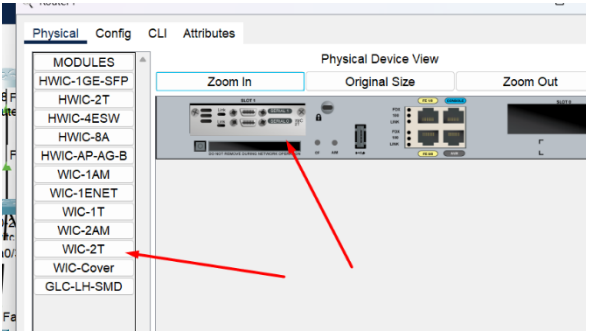

Figura 2.5. Adăugarea extensiei WC-2T pentru a putea conecta cablul serial

Adăugarea extensiei WC-2T este necesară pentru a permite conectarea cablului serial între switch-uri și routere, oferind o interfață de conexiune serială. Acest lucru permite switch-urilor să comunice cu routerele prin porturile de consolă, ceea ce facilitează configurarea și gestionarea dispozitivelor în rețea. În plus, această extensie extinde posibilitățile de conectare și configurare a echipamentelor în cadrul rețelei locale proiectate, contribuind la funcționalitatea generală a rețelei.

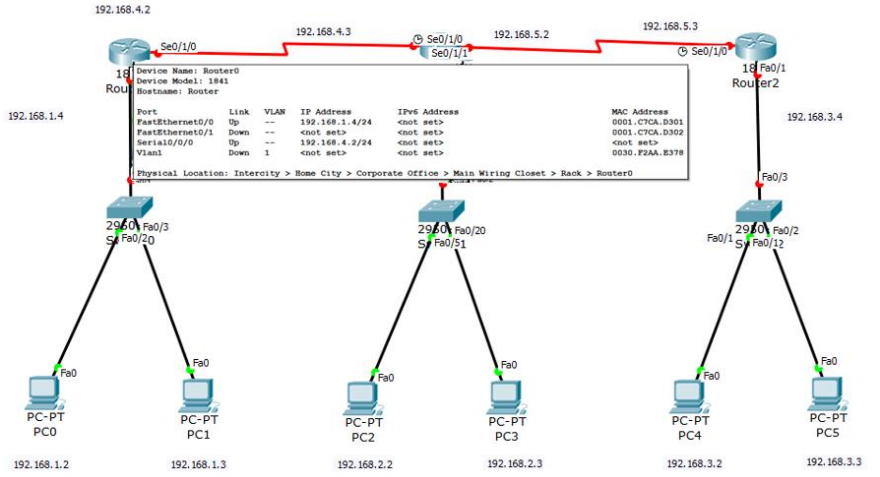

Figura 2.6. Adresele routerului nr.1

Routerul nr.1 trebuie configurat cu adrese IP și măști de subrețea pentru fiecare subrețea din rețeaua locală. Acest lucru implică atribuirea unei adrese IP distincte și a unei măști de subrețea pentru fiecare interfață a routerului, care este asociată cu o anumită subrețea din rețea.

Această configurație este esențială pentru a asigura conectivitatea și rutarea corectă dintre subrețelele locale și externe din cadrul rețelei.

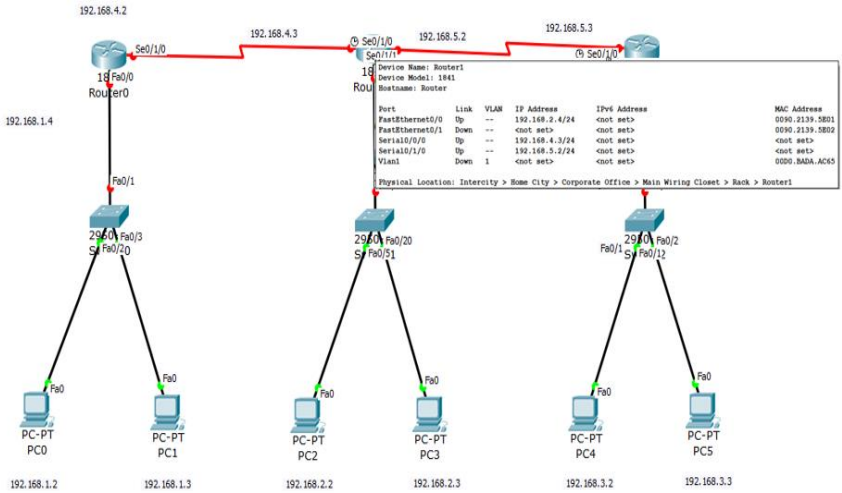

Figura 2.7. Adresele routerului nr.2

De asemenea, și routerul nr.2 trebuie să fie configurat cu adrese IP și măști de subrețea pentru fiecare subrețea din rețeaua locală. Pentru fiecare interfață a routerului nr.2 se va atribui o adresă IP și o mască de subrețea distinctă care sunt asociate cu fiecare subrețea în parte.

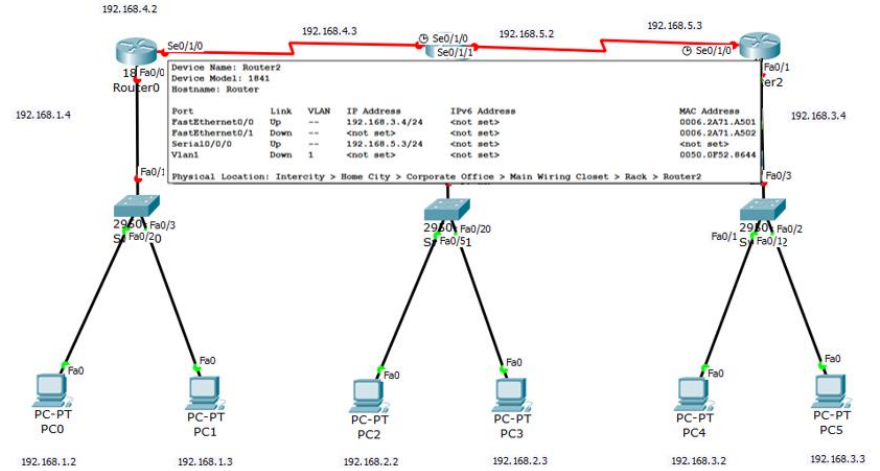

Figura 2.8. Adresele routerului nr.3

Pentru fiecare interfață a routerului nr.3 se va atribui o adresă IP și o mască de subrețea distinctă asociate cu fiecare subrețea în parte.

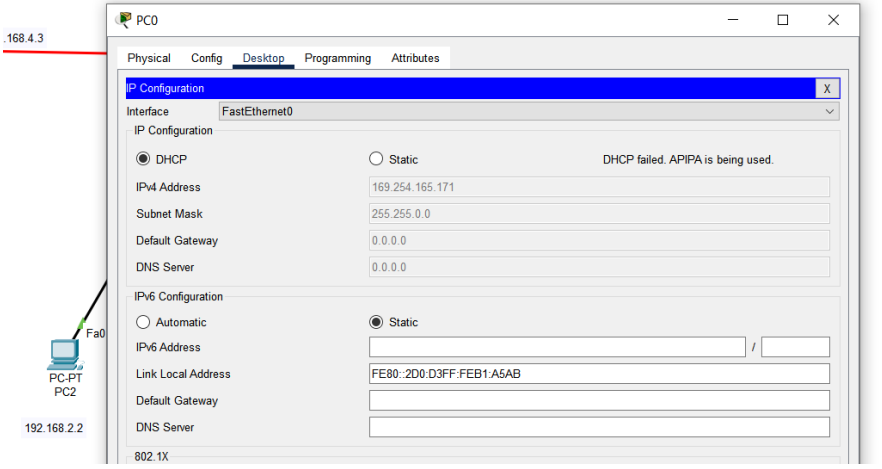

Figura 2.9. Adresa primită în mod dinamic pentru calculatorul PC-0

Întrucât o adresă IP dinamică nu este stabilită prin configurarea manuală a calculatorului, este esențial să se permită obținerea acesteia printr-o procedură cunoscută sub numele de "obținere automată a adresei IP" (DHCP). Această procedură este implementată în general prin intermediul unui server DHCP care poate fi, de exemplu, un router configurat pentru această funcție. Când acest calculator este conectat la rețea, acesta solicită o adresă IP de la serverul DHCP, care ulterior îi este alocată. Este important de remarcat că, în cazul conexiunii calculatorului la un switch, serverul DHCP ar trebui să fie poziționat pe aceeași rețea locală cu calculatorul pentru a permite obținerea cu succes a adresei IP.

5. Conținutul raportului

1. Introducere:
    a. Scopul și obiectivele lucrării de laborator.
    b. Descrierea generală a rețelei proiectate.
2. Descrierea rețelei proiectate:
    a. Prezentarea topologiei rețelei: switch-uri, routere, calculatoare etc.
    b. Configurarea fiecărui dispozitiv în cadrul rețelei: setarea adreselor IP, configurația gateway-ului etc.
3. Proiectarea și setarea subrețelelor:
    a. Descrierea proiectării și configurării subrețelelor, inclusiv a maselor și a adresei IP.
4. Proiectarea și setarea rutării între diferite subrețele:
    a. Configurarea statică a rutării între subrețele.
    b. Explicația modului de funcționare a rutării statice în rețeaua proiectată.
5. Verificarea conexiunii dintre subrețele:

a. Utilizarea comenzii *ping* pentru a verifica conectivitatea dintre diferitele subrețele.

6. Concluzie:
    a. Rezultatele obținute în cadrul lucrării de laborator.
    b. Observațiile și concluziile finale.
7. Bibliografie:
    a. Sursele bibliografice utilizate în cadrul lucrării.
8. Anexe:
    a. Capturi de ecran cu configurările și interacțiunile din cadrul laboratorului, dacă este necesar.

Întrebări de control

1. Care este scopul principal al subrețelelor?
2. Explicați diferența dintre o adresă IP și o mască de subrețea.
3. Cum se calculează numărul maxim de hosturi dintr-o subrețea?
4. Ce este un router și care este rolul lui în rețea?
5. Explicați conceptul de tabel de rutare.
6. Cum se configurează manual o rută statică pe un router?
7. Cum se calculează adresa de rețea și adresa de broadcast pentru o subrețea specifică?
8. Ce este un protocol de rutare și care sunt funcțiile sale principale?
9. Cum se configurează un router pentru a utiliza un protocol de rutare statică?
10. Cum se pot verifica rutele active pe un router?
11. Descrieți câteva instrumente și comenzi utilizate pentru depanarea problemelor de rutare.

Bibliografie

1. Hunt, Craig. TCP/IP Network Administration. 4th ed., O'Reilly Media, 2014.
2. Odom, Wendell. CCNA Routing and Switching: Official Cert Guide. 2nd ed., Cisco Press, 2019.
3. Barnhart, Glynn. Subnetting Made Easy. 3rd ed., Sybex, 2013.
4. Lammle, Todd. Routing Protocols and Concepts. CCIE Routing & Switching Certification Guide, 2nd ed., John Wiley & Sons, 2016.
5. **Cisco Networking Academy**. https://www.netacad.com/
6. **Microsoft Learn**. https://docs.microsoft.com/en-us/learn/
7. **Tutorials Point**. https://www.tutorialspoint.com/

Lucrarea de laborator nr.3
SETAREA ALGORITMELOR DE ROUTING LA SUBREȚELE LOCALE

1. Scopul lucrării: a permite selectarea și configurarea algoritmilor de rutare statică și dinamică, a optimiza traficul de rețea prin configurarea rutelor eficiente și a verifica corectitudinea transmiterii datelor din diferite subrețele.

2. Noţiuni teoretice generale

1) Rutarea dinamică

Partea negativă a rutării statice constă în necesitatea unui volum mare de lucru manual. În plus, schimbările în topologia rețelei necesită ajustări manuale ale setărilor. Utilizarea protocoalelor de rutare dinamică permite ca fiecare router să fie ajustat automat în funcție de rutele actuale.

Pentru a crea relații de vecinătate între routere, protocoalele de rutare permit schimbul de rute direct conectate și alte rute (acceptate). Prin urmare, toate routerele comunică actualizări între ele. În plus, routerele transmit actualizări când se produc modificări de topologie, ceea ce permite detectarea pierderilor de rute.

2) Configurarea protocolului de rutare RIP utilizând protocolul RIP

Packet Tracer oferă o interfață grafică care permite configurarea unui protocol de rutare dinamic cunoscut sub numele de Protocol de informații de rutare (RIP). Configurarea rutării statice este similară cu această opțiune. În plus, există o singură casetă de text care poate fi utilizată pentru a introduce adresa de rețea a rețelei conectate direct.

Deși se poate presupune că această setare este asemănătoare cu configurarea rutelor statice, dar nu în acest caz. Configurarea rutei statice necesită introducerea rutei către alte rețele, dar pentru RIP trebuie introduse adresele IP ale propriei interfețe de rețea. Introducem adresele IP ale interfețelor propuse. În consecință, se îndeplinesc două funcții: se introduce protocolul de rutare pe interfața specificată și se permite răspândirea datelor despre rețea.

Pașii pentru configurarea rutării dinamice RIP sunt:

1. Se creează o topologie identică cu cea din exemplul anterior. Folosind fila Configuration (Configurație), se atribuie adrese IP identice interfețelor routerului.
2. Se accesează secțiunea RIP din aceeași filă. Configurarea rutării dinamice este foarte simplă. Fiecare router trebuie doar să introducă adresa IP a interfeței sale de rețea (figura 3.1.).

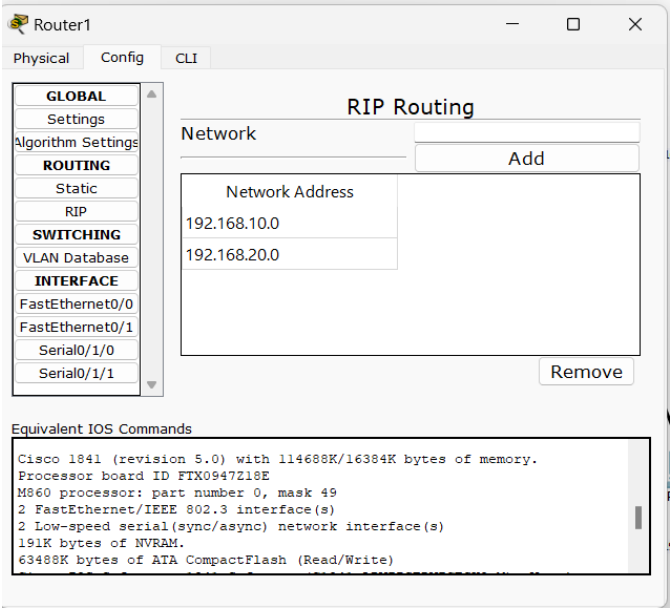

Figura 3.1. Configurarea rutării dinamice utilizând GUI

3. Pentru fiecare router se introduc următoarele adrese IP de rețea:

Tabelul 3.1. Adresele IP de rețea ale interfețelor routerului

Router	***RIP Network***
R1	192.168.10.0
	192.168.20.0
R2	192.168.10.0
	192.168.30.0
R3	192.168.20.0
	192.168.40.0
R4	192.168.30.0
	192.168.40.0

4. După configurarea topologiei, se efectuează un test de conectivitate, folosind instrumentul PDU convențional. Se testează două routere fără legătură directă, de exemplu, R1 și R4 sau R2 și R3. O trecere cu succes indică faptul că fiecare router are rutarea dinamică configurată corect.
5. În pasul următor se verifică modul în care protocoalele de rutare dinamică se comportă când se produc schimbări de topologie. Pentru aceasta se selectează instrumentul „Șterge” din bara de instrumente generală și se șterge legătura dintre routerele R1 și R2, sau R1 și R3. Pentru a efectua un test de conectivitate, se utilizează modul de simulare și instrumentul Simple PDU. Pachetele vor călători pe o rută diferită, ceea ce va indica succesul testului. Pachetele vor parcurge o cale mai lungă.

Dacă s-a efectuat pasul 5 din rutarea statică, se va observa apariția unei erori, deoarece nu s-au introdus manual rute alternative

pentru fiecare rețea în fiecare router pentru a preveni pierderea conectivității dintre routere. Aceasta este o caracteristică semnificativă a rutelor dinamice.

3) Configurarea protocolului de rutare RIP utilizând CLI

Se va configura aceeași topologie, folosind CLI. Comenzile de configurare sunt foarte simple, după cum se observă când se utilizează GUI, în fereastra Comenzi IOS echivalente. Se va accesa fila CLI pentru a configura rutarea dinamică și se vor efectua următorii pași:

1. Se utilizează aceleași comenzi ca și în exemplul de configurare a rutării statice cu linia de comandă pentru a atribui adresele IP ale interfeței routerului.
2. Apoi se revine la modul de configurare globală și se utilizează următoarea comandă pentru a trece la modul router RIP:
   ```
   R1(config)#router rip
   ```
3. Pentru a afla adresa IP a rețelei, se utilizează comanda *network.* Urmeaza următoarele comenzi pentru Router R1:
   ```
   R1(config-router)#network 192.168.10.0
   R1(config-router)#network 192.168.20.0
   ```
4. Se configurează toate routerele în mod identic. Apoi, pentru a efectua un test de conectivitate, se utilizează instrumentul PDU convențional.

În continuare, se poate examina tabelul de rutare în detaliu.

4) Tabelul de rutare

Tabelul de rutare include o listă a tuturor rutelor preferate pe care routerele le cunosc. Tabelul de rutare poate fi vizualizat în două moduri. Pentru unul dintre ele se utilizează butonul Inspect Instrument, iar pentru celălalt se utilizează comanda Cisco IOS *show*

ip route. Apare un tabel format din mai multe coloane și informații în ele. În continuare se va afișa ce anume este inclus în tabel:

```
R1#show ip route
C 192.168.10.0/24 is directly connected,
FastEthernet0/0
C 192.168.20.0/24 is directly connected,
FastEthernet0/1
R 192.168.30.0/24 [120/1] via 192.168.10.2,
00:00:13,
FastEthernet0/0
R 192.168.40.0/24 [120/1] via 192.168.20.2,
00:00:22,
FastEthernet0/1
```

Prima coloană descrie motivul pentru care a fost introdusă în tabelul de rutare C - rețea conectată direct, R - protocol de rutare dinamică RIP.

A doua coloană indică rețeaua de destinație.

Între parantezele pătrate, prima valoare indică distanța administrativă (administrative distance), arătând prioritatea protocolului de rutare, iar a doua valoare reprezintă valoarea metrică a protocolului de rutare dinamic. Valoarea metrică a protocolului de rutare dinamic este reprezentată de numărul de salturi și de numărul de routere care se îndreaptă către rețeaua de destinație pentru protocolul RIP. În acest caz, distanța administrativă pentru protocolul RIP este de 120, iar distanța pentru o rută statică – de 1.

Dacă un router are două rute către aceeași rețea, fie statică, fie RIP, va fi utilizată ruta statică, deoarece distanța administrativă este mai mică.

Adresa gateway-ului, care este următorul router ce se îndreaptă către rețeaua de destinație, este adresa IP scrisă după cuvântul „via”. Un cronometru de reținere sau holddown timer este marca temporală scrisă la sfârșitul unei rute dinamice. În plus, orice protocol de rutare

trimite mesajele la un interval specific, cum ar fi „Hello timer”. Când vine vorba de protocolul RIP, acesta este de 30 de secunde. Dacă routerul nu primește mesaje despre o rută în timpul a trei intervale Hello (180 s sau Holddown timer), această rută este eliminată din tabelul de rutare și se caută o rută alternativă.

Interfața de ieșire a routerului pe care gateway-ul o poate accesa se află în ultima coloană.

5) Distribuția sarcinii

În topologia care va fi examinată în continuare este posibil ca fiecare router să aibă două modalități diferite de a ajunge la fiecare rețea de destinație. Când traficul trece de-a lungul routerelor, ar fi util să examinăm modul în care acestea utilizează căile alternative și efectuează echilibrarea sarcinii.

a) Echilibrarea sarcinii în protocolul RIP

Deoarece în acest caz nu trebuie nimic de modificat, vom lua în considerare mai întâi protocolul RIP. Nu este necesar să luăm măsuri. RIP echilibrează automat sarcinile dacă căile alternative pentru a ajunge la rețelele de destinație au aceeași metrică. În acest exemplu, vom folosi tipul de interfață loopback ca rețea de destinație. O interfață virtuală loopback folosește o adresă IP și se comportă ca o interfață reală. Se adaugă această interfață routerului R4, folosind următorii pași în aceeași topologie:

1) Din păcate, GUI nu poate face acest lucru, așa că se va utiliza CLI pentru a adăuga această interfață la router (CLI) și se introduc comenzile care urmează:

```
R4(config)#interface loopback 0
R4(config-if)#ip address 192.168.100.1
255.255.255.0
```

2) Procesul de rutare trebuie început pe interfața loopback pe același router. Se introduce adresa IP de rețea a interfeței loopback după ce se trece la modul de configurare globală. Informațiile referitoare la rutare vor fi trimise automat:

```
R4(config)#router rip
R4(router-if)#network 192.168.100.0
```

3) Se utilizează „Complex” pentru testare, PDU, aranjați un interval de timp de 2 s.

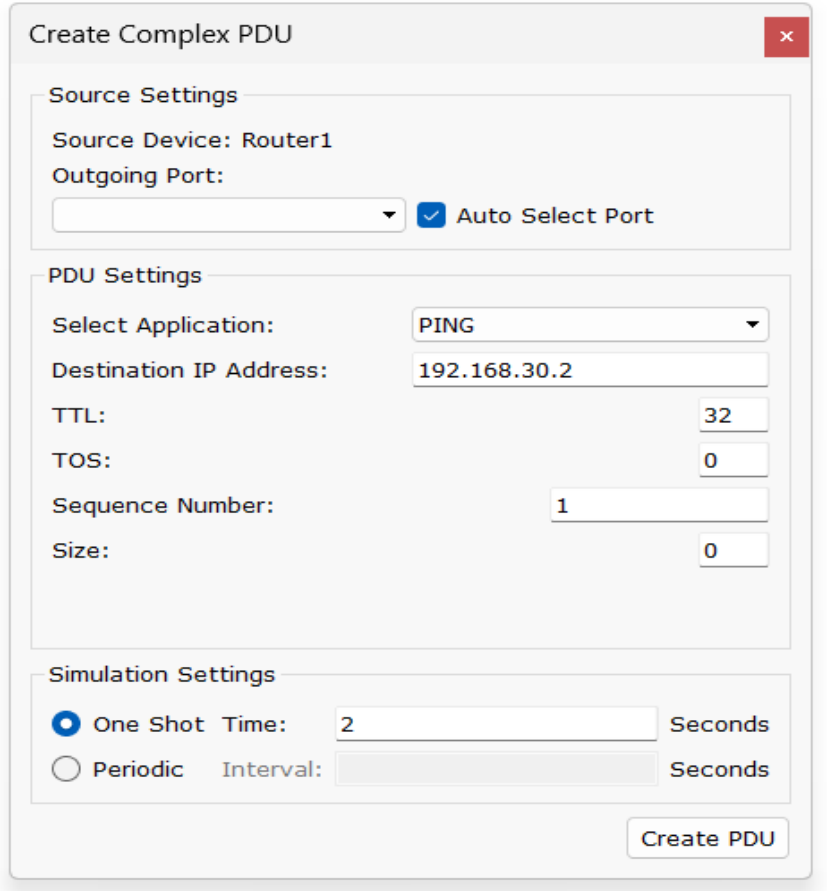

Figura 3.2. Utilizarea instrumentului Complex PDU

4) În modul de simulare se determină că primul pachet va urma traseul R1-R2-R4, iar cel de-al doilea pachet va urma traseul R1-R3-R4.

În plus, examinând tabelul de rutare, se verifică dacă mecanismul de distribuție a traficului funcționează corect:

```
Router>show ip route
R 192.168.30.0/24 [120/1] via 192.168.10.2,
00:00:12,
FastEthernet0/0
R 192.168.40.0/24 [120/1] via 192.168.20.2,
00:00:14,
FastEthernet0/1
R 192.168.100.0/24
[120/2] via 192.168.20.2, 00:00:08,
FastEthernet0/1
[120/2] via 192.168.10.2, 00:00:08,
FastEthernet0/0
```

Pentru o înțelegere mai bună, tabelul de rutare afișat conține doar rutele RIP. Deoarece 192.168.100.0/24 are două porturi de intrare, traficul va fi distribuit între ele.

b) Echilibrarea sarcinii pentru rutele statice

Rutarea statică necesită ajustări suplimentare pentru a echilibra încărcarea. Alocarea adreselor IP ale tuturor interfețelor fizice, precum și ale interfețelor loopback are loc așa cum a fost menționat anterior. Pentru a configura echilibrarea sarcinii, se îndeplinesc următorii pași:

1) Se configurează o rută pentru routerele R2 și R3 pentru a ajunge la interfața orbaskin a routerului R4:

```
R2(config)#ip route 192.168.100.0
255.255.255.0 192.168.30.2
R3(config)#ip route 192.168.100.0
255.255.255.0 192.168.40.2
```

2) Se configurează două rute către 192.168.100.0/24 pe routerul R1. Routerului trebuie să i se explice că există două moduri

pentru a ajunge la interfața loopback a routerului R4. Pentru a realiza acest lucru, se utilizează comenzile următoare:

```
R1(config)#ip route 192.168.100.0
255.255.255.0 192.168.10.2
R1(config)#ip route 192.168.100.0
255.255.255.0 192.168.20.2
```

3) Se activează „Complex PDU" ca în rutarea statică și „Complex PDU" ca în secțiunea anterioară pentru a testa eficiența mecanismului de distribuție pentru rutarea statică.

După ce s-a realizat această configurație, în tabelul de rutare putem observa două rute către 192.168.100.0/24 asemănătoare cu rutele RIP.

6) Protocol gateway extern BGP (Border Gateway Protocol)

Internet este o mare rețea compusă din multe alte rețele. Fiecare rețea folosește protocoale de rutare pentru a determina rutele către alte rețele. Protocoalele precum Enhanced Interior Gateway Routing Protocol (EIGRP), RIP (Routing Information Protocol) și OSPF (Open Shortest Path First) funcționează bine pentru majoritatea rețelelor. Cu toate acestea, din cauza dimensiunii lor reduse nu sunt potrivite pentru o rețea compozită precum internetul, din cauza scalabilității inadecvate și a lipsei de separare administrativă suficientă. Prestatorul de servicii internet (ISP) și întreprinderile mari folosesc protocolul Border Gateway Protocol (BGP) pentru a le informa despre rutele existente între ele.

Protocolul BGP și caracteristicile sale se vor examina în comparație cu alte protocoale. În plus, vom analiza protocolul Cisco IOS comenzi utilizate în configurarea BGP și cum se realizează configurarea pentru ele.

a) Ce este BGP?

Când se utilizează schimbul de informații de rutare între mai multe sisteme autonome (AS), BGP este un protocol de rutare extrem de eficient. Această definiție ridică o altă întrebare: ce înseamnă a fi o zonă autonomă? O zonă autonomă este un set de prefixe IP sau rețele IP, care sunt supravegheate de un singur administrator. Companiile sau ISP pot fi operator de rețea care supraveghează zona autonomă.

Fiecare zonă autonomă are un număr numit ASN (Autonomous System Number). Numerele publice ale zonelor autonome sunt atribuite de către registrele regionale de internet RIR (Regional Internet Registries), cărora le este delegat acest drept de către Autoritatea pentru numere atribuite pe internet IANA (Internet Assigned Numbers Authority).

Configurația BGP se bazează în mare parte pe modul în care o organizație se conectează la un furnizor de servicii de internet. Există patru tipuri posibile de conexiuni:

1. Cu o singură conectare – cea mai simplă opțiune de proiectare, care oferă o singură legătură către un singur prestator de servicii internet (ISP) (figura 3.3). Nu există garanție că această conexiune oferă redundanță sau toleranță la erori.
2. Conexiune dual-homed sau două repere. În plus, această schemă de conectare utilizează un singur furnizor, dar permite utilizarea a două sau mai multor canale pentru aceasta (figura 3.4). Aceasta îmbunătățește credibilitatea în cazul problemelor cu un canal.

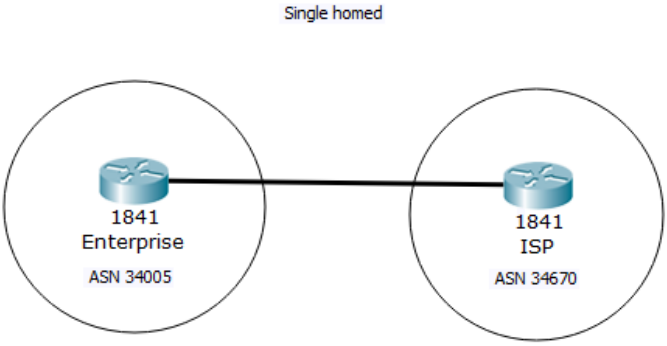

Figura 3.3. Conexiune cu o singură localizare (Single homed)

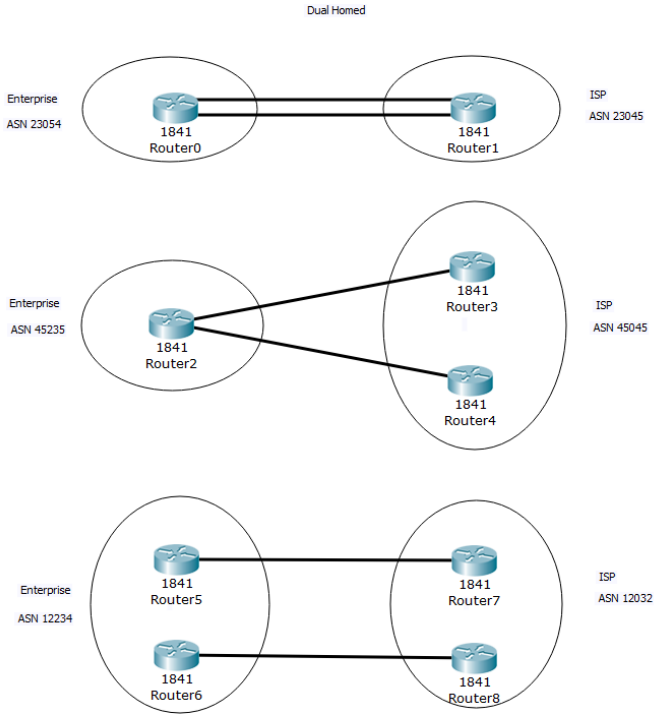

Figura 3.4. Opțiuni cu dublă localizare (Dual homed)

3. O conexiune multihomed unică (Single multihomed). În acest caz, există mai mulți furnizori de servicii de internet, iar fiecare dintre ei are o legătură conectată (figura 3.5).
4. Conexiune multihomed dublă (Dual mutihomed). Schemele de conexiune oferă cel mai înalt nivel de disponibilitate și fiabilitate. În acest caz, există doi sau mai mulți furnizori, iar la fiecare dintre aceștia sunt conectate două sau mai multe canale de comunicare (figura 3.6).

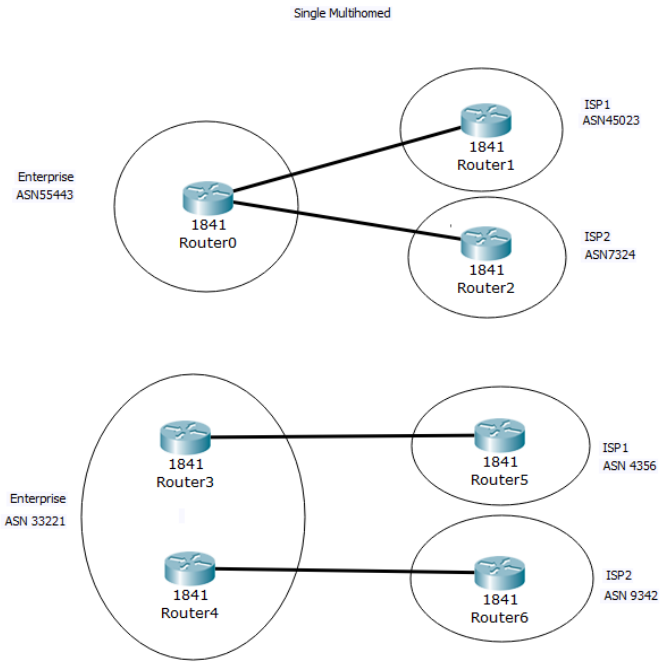

Figura 3.5. Opțiuni de conexiune multihomed unică (Single multihomed)

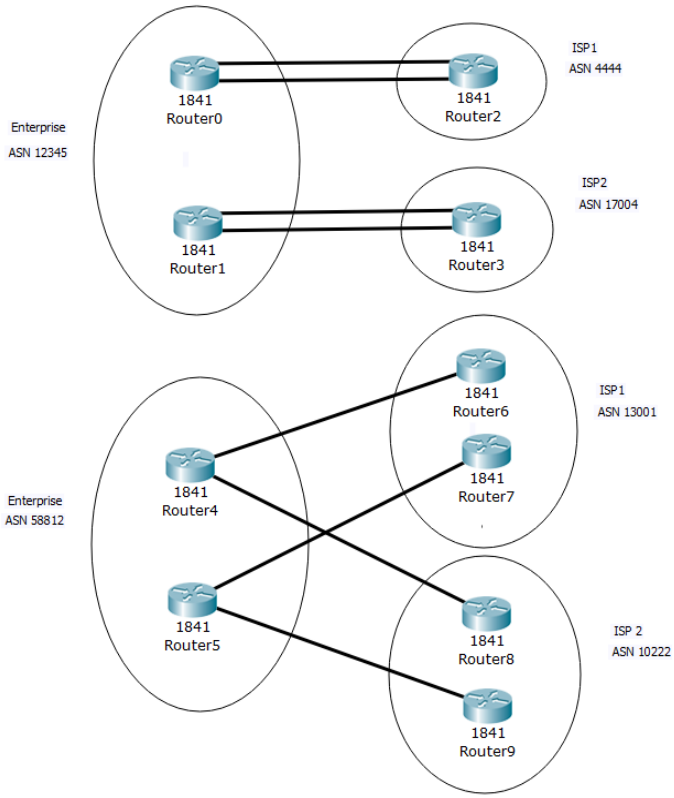

Figura 3.6. Opțiuni dual multihomed (Dual multihomed)

Este posibil ca BGP să nu respecte opțiunile de topologie sugerate. În unele cazuri de conexiune unică, este mai bine să existe o singură rută statică implicită către ISP și o altă rută statică de la ISP către rețeaua companiei. Dar implementarea BGP în varianta de conectivitate multirețele asigură o rutare mai eficientă.

Există două tipuri de BGP:

1. BGP extern (External BGP, eBGP);
2. BGP intern (iBGP).

b) BGP extern

Pentru a face schimb de rute între zonele autonome, se utilizează tipul de protocol BGP. eBGP care are o distanță administrativă de 20. În mod implicit, TTL (Time-to-Live) este setat la 1, când se trimit pachete de actualizare către eBGP. Acest lucru înseamnă că doar routerul BGP conectat direct va primi pachetele. Prin comanda potrivită, acest comportament poate fi schimbat. Routerul eBGP notifică toate rutele acceptate atât de routerele eBGP, cât și de cele iBGP. Un vecin eBGP indică o rută în câmpul routerului următor al rutei anunțate.

c) BGP intern

Pentru a face schimb de rute în cadrul unei zone autonome, se utilizează tipul de protocol BGP. iBGP care are o distanță administrativă de 200. Actualizările iBGP nu limitează valoarea TTL. Rutele iBGP nu comunică rutele care au fost învățate de alte routere iBGP. Acest mecanism împiedică formarea de rute bucle de rute în interiorul unei zone separate. Routerul iBGP lasă adresa routerului următor neschimbată în câmpul adresei din anunțurile de rute. Cu ajutorul comenzilor adecvate, acest comportament poate fi, de asemenea, modificat. Cisco Packet Tracer nu acceptă iBGP.

7) BGP ca protocol de rutare dinamic

Deși BGP și alte protocoale de rutare dinamice funcționează la fel, există câteva diferențe între protocoalele de rutare dinamice. Protocoalele de gateway interior IGP (Interior Gateway Protocols) precum RIP, OSPF și EIGRP au protocoale de rutare avansate. Adresa IP a rețelei este determinată de anunțul de rețea care este creat prin configurarea protocolului de rutare. Procesul de anunțare a rutării implică interfețe ale căror adrese IP se încadrează în intervalul rețelei anunțate. Anunțurile de rutare sunt difuzate sau distribuite prin

intermediul acestor interfețe. Pentru ca acest lucru să funcționeze, două routere vecine trebuie să aibă o conexiune directă unul cu celălalt și trebuie să aibă procese de protocol gateway interior (IGP) care să funcționeze pe ele. Numărul de salturi, lățimea de bandă, timpul de întârziere și alți parametri sunt utilizați de protocoalele interfeței interne de protocol (IGP) pentru a alege calea optimă.

În schimb, BGP nu folosește ideea de interfețe. Întregul router funcționează într-o zonă autonomă. Vecinii BGP trebuie atribuiți manual cu ajutorul comenzii de vecinătate, deoarece nu sunt detectați automat. În continuare, mesajele BGP sunt transmise într-un set de pachete unidirecționale. BGP se bazează pe protocolul TCP și ascultă portul 179. Vecinii pot fi găsiți la mai multe salturi distanță și nu trebuie neapărat să fie aproape. Valoarea duratei de viață implicită TTL pentru un mesaj GP este 1. Această valoare trebuie ajustată în sus în cazul în care punctul de schimb nu este conectat direct. Principiile care guvernează alegerea celei mai bune rute BGP diferă de cele ale protocoalelor de gateway interior (IGP). Atributele PA sau atributele căii includ accesibilitatea următorului hop, greutatea rutei și calea către zona autonomă (AS_PATH este numărul de zone autonome care fac parte din calea către rețeaua de destinație).

În plus, când se execută prin protocoalele de gateway în interior (IGP), BGP este proiectat pentru a gestiona sute de mii de rute IP, ceea ce necesită o cantitate mare de resurse.

8) Configurarea BGP în Packet Tracer

În primul rând, se examinează comenzile utilizate în BGP:

```
router bgp <asn>
```

De exemplu:

```
R1(config)# router bgp 120
```

Această comandă pornește procesul BGP al routerului și îl pune în modul de configurare a rutelor. Numărul zonei autonome ASN poate fi de la 1 până la 65535.

Procesul BGP cere atribuirea unui ID de router. Metodele de selectare a ID de router sunt implicit utilizate de BGP în următoarea ordine de prioritate:

1. A fost setat manual. În modul de configurare a rutelor se utilizează funcția bgp router-id pentru a configura ID-ul.
2. Valoarea interfeței loopback cea mai mare. Când procesul BGP este inițiat în acest scenariu, identificatorul routerului devine cea mai mare adresă IP a oricărei interfețe loopback disponibile. Interfață loopback este disponibilă când procesul BGP a început.
3. Valoarea cea mai mare a celeilalte interfețe. Când începe procesul BGP, identificatorul routerului este selectat pentru a fi cea mai mare adresă IP configurată pe orice interfață disponibilă, în afară de interfața loopback.

ID al routerului se poate seta în mod explicit prin următoarea comandă:

```
bgp router-id X.X.X.X
```

Drept exemplu se utilizează următoarea comandă pentru a atribui ID-ul routerului:

```
R1(config-router)#bgp router-id 1.1.1.1
```

Pentru a configura un BGP alăturat, se utilizează următoarea comandă:

```
R1(config-router)#neighbor X.X.X.X remote-as
<asn>
```

De exemplu:

```
R1(config-router)#neighbor 10.0.0.2 remote-as 130
```

Aici valoarea numărului de zonă autonomă introdus după opțiunea `remote-as` trebuie să corespundă unei zone autonome conectate la un router vecin. Deci, există o distincție între protocolul extern (eBGP) și cel intern (iBGP).

Pentru protocolul BGP extern se vor utiliza următoarele comenzi:

```
R1(config)#router bgp 120
R1(config-router)#neighbor 10.0.0.2 remote-as 130
```

Pentru protocolul BGP intern se va utiliza următoarea formă:

```
R1(config)#router bgp 120
R1(config-router)#neighbor 192.168.1.20 remote-as 120
```

După cum a fost menționat, protocolul BGP intern nu modifică câmpul routerului următor când se schimbă informațiile de rutare în cadrul unei zone autonome. Aceasta poate fi o problemă, deoarece este posibil ca redistribuirea să nu fie disponibilă prin protocoale IGP. Acest lucru se întâmplă, deoarece protocoalele IGP resping astfel de rute din cauza adresei incorecte a routerului următor. Adresa IP a routerului următor este stabilită prin comanda:

```
R1(config-router)#neighbor X.X.X.X next-hop-self
```

Protocolul BGP are, de asemenea, o comandă `network`. Aceasta este utilizată pentru a specifica o anumită rută care să fie anunțată prin intermediul protocolului BGP, iar o astfel de rută trebuie să existe în tabelul de rutare:

```
R1(config-router)#network 10.20.20.0 mask 255.255.255.0
```

Când se selectaează doar o rută de clasă, se poate omite opțiunea de mască.

Packet Tracer nu poate accepta toate comenzile protocolului BGP. Astfel, în exemplele ulterioare se vor folosi doar comenzile menționate anterior.

Se va utiliza o singură topologie multinetwork pentru exemplul din figura 3.7, deoarece Packet Tracer nu este compatibil cu iBGP.

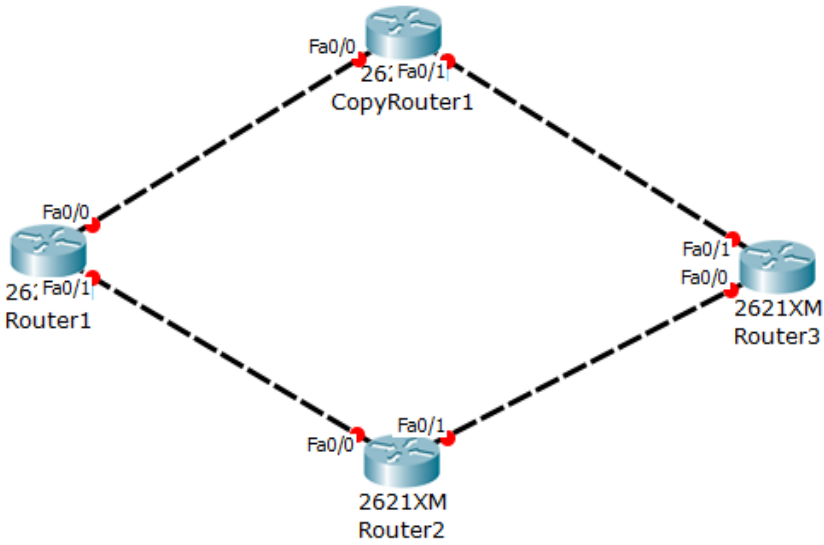

Figura 3.7. Exemplu de configurare BGP în Packet Tracer

În această rețea există patru routere, dintre care două sunt proprietatea unei companii distincte, iar celelalte două sunt proprietatea unor furnizori diferiți de servicii Internet. Routerele companiei au interfețe loopback configurate cu adrese IP. Acest lucru va ilustra modul în care tabelul de rutare include rutele învățate prin protocolul BGP (tabelul 3.2).

Tabelul 3.2. Adresele IP ale interfețelor routerului

Dispozitivul	*Interfața*	*IP-adresa*	*Masca*
Enterprise 1	Loopback0	20.30.0.1	255.255.0.0
	FastEthernet0/0	10.0.0.1	255.255.255.255
	FastEthernet1/0	10.0.0.9	255.255.255.255
Enterprise 2	Loopback0	40.30.0.1	255.255.0.0
	FastEthernet0/0	10.0.0.5	255.255.255.255
	FastEthernet1/0	10.0.0.13	255.255.255.255
ISP1	FastEthernet0/0	10.0.0.2	255.255.255.255
	FastEthernet1/0	10.0.0.6	255.255.255.255
ISP2	FastEthernet0/0	10.0.0.10	255.255.255.255
	FastEthernet1/0	10.0.0.14	255.255.255.255

Pentru a configura protocolul BGP în această topologie, trebuie efectuați următorii pași:

1) Configurarea începe de la routerele de producție:

```
Enterprise1(config)#router bgp 10200
Enterprise1(config-router)#bgp router-id
0.0.0.1
Enterprise1(config-router)#neighbor 10.0.0.2
remote-as 30200
Enterprise1(config-router)#neighbor
10.0.0.10 remote-as 50300
Enterprise1(config-router)#network 20.30.0.0
mask 255.255.0.0

Enterprise2(config)#router bgp 3400
Enterprise2(config-router)#bgp router-id
0.0.0.2
Enterprise2(config-router)#neighbor 10.0.0.6
remote-as 30200
```

```
Enterprise2(config-router)#neighbor
10.0.0.14 remote-as 50300
Enterprise2(config-router)#network 40.30.0.0
mask
255.255.0.0
```

2) În continuare, se configurează routerele ISP:

```
ISP1(config)#router bgp 30200
ISP1(config-router)#bgp router-id 1.1.1.1
ISP1(config-router)#neighbor 10.0.0.1
remote-as 10200
ISP1(config-router)#neighbor 10.0.0.5
remote-as 3400
ISP2(config)#router bgp 50300
ISP2(config-router)#bgp router-id 2.2.2.2
ISP2(config-router)#neighbor 10.0.0.9
remote-as 10200
ISP2(config-router)#neighbor 10.0.0.13
remote-as 3400
```

3) Când configurarea este corectă, vor apărea mesaje de consolă despre stabilirea vecinătății:

```
%BGP-5-ADJCHANGE: neighbor 10.0.0.9 Up
%BGP-5-ADJCHANGE: neighbor 10.0.0.13 Up
```

4) Ping la interfața loopback a routerului Enterprise2 de la routerul Enterprise1:

```
Enterprise1>ping 40.30.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.30.0.1,
timeout is 2
seconds:
.....
```

```
Success rate is 0 percent (0/5)
```

5) Se observă că încercarea de testare a conectivității a eșuat.

Aceasta se datorează faptului că pachetul de solicitare ICMP utilizează adresa 10.0.0.1 ca expeditor, astfel încât, atunci când pachetul este primit de către routerul Enterprise2, acesta nu poate trimite un răspuns ICMP, deoarece nu are o adresă, o rută către rețeaua 10.0.0.0.0.0/30. Pentru a ajunge la rețeaua specificată pe Enterprise1, se va utiliza o versiune extinsă a utilitarului ping, în care se poate specifica în mod explicit interfața de ieșire:

```
Enterprise1#ping
Protocol [ip]:
Target IP address: 40.30.0.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 20.30.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp,
Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.30.0.1,
timeout is 2 seconds:
Packet sent with a source address of
20.30.0.1
!!!!!
Success rate is 100 percent (5/5), round-
trip min/avg/max = 0/0/1 ms
```

6) Astfel, s-a configurat cu succes eBGP. În continuare se examinează rutele BGP în tabelul de rutare.

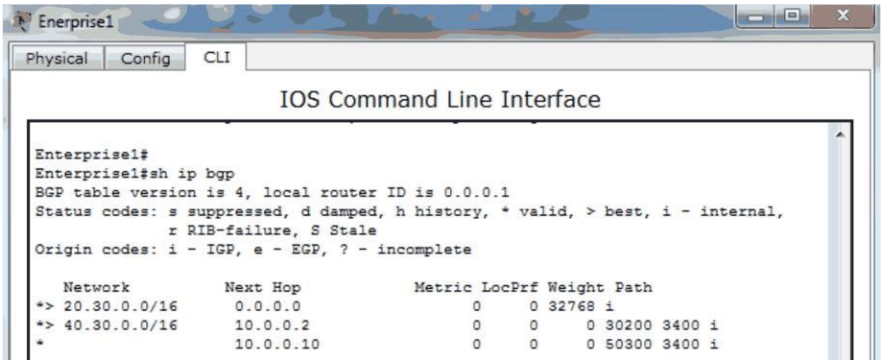

Figura 3.8. Rezultatul utilizării comenzii sh ip bgp

3. Ordinea efectuării lucrării de laborator

1. Să se proiecteze subrețele reprezentate în figura 3.9.
2. Să se atribuie IP și masca subrețelei pentru fiecare subrețea în parte.
3. Să se verifice conexiunile dintre hosturi, folosind comanda *ping.*
4. Folosind algoritmii de routing dinamic, să se seteze comenzile necesare.
5. Folosind comanda *show ip route* pentru verificarea rețelelor *ip* atribuite fiecărui port.
6. Să se verifice conexiunea dintre subrețele, folosind comanda *ping*.

4. Efectuarea lucrării de laborator

Se cere proiectarea unei subrețele, având la bază topologia prezentată în figura 3.9. Rețeaua locală va fi segmentată în subrețele

pentru a optimiza traficul și a spori securitatea. Fiecare router va fi responsabil pentru gestionarea subrețelelor specifice din rețea. Switch-urile vor conecta calculatoarele la subrețelele respective, asigurând conectivitatea și comunicarea eficientă. Proiectarea subrețelelor va lua în considerare numărul de calculatoare, tipul de trafic și cerințele de securitate specifice fiecărei subrețele.

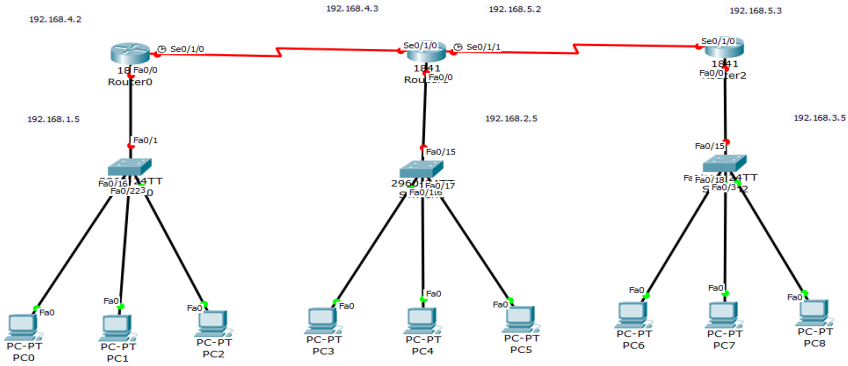

Figura 3.9. Rețeaua locală alcătuită din 3 routere, 3 switch-uri și 9 calculatoare

Rețeaua va fi împărțită în 3 subrețele distincte, având configurații specifice de adresare IP și mască. Subrețeaua 1 va utiliza intervalul 192.168.1.0/24 cu masca 255.255.255.0, Subrețeaua 2 va fi definită de 192.168.2.0/24 și masca 255.255.255.0, iar Subrețeaua 3 va cuprinde adresele din 192.168.3.0/24 cu masca 255.255.255.0.

Pentru a facilita comunicarea între subrețele, se vor configura rute statice pe cele 3 routere. Primul router va deține rute statice către subrețelele 2, 3 și 4, utilizând interfața de ieșire 192.168.4.3. Al doilea router va fi configurat cu rute statice către subrețelele 1 și 3, având ca interfață de ieșire 192.168.4.2. Al treilea router va completa

schema prin configurarea de rute statice către subrețelele 1, 2 și 4, cu interfața de ieșire 192.168.5.2.

Switch-urile vor juca un rol esențial în conectarea calculatoarelor la subrețelele respective, asigurând comunicarea eficientă între dispozitivele din rețea. Segmentarea rețelei în subrețele va optimiza traficul și va spori semnificativ nivelul de securitate prin limitarea accesului la anumite segmente specifice.

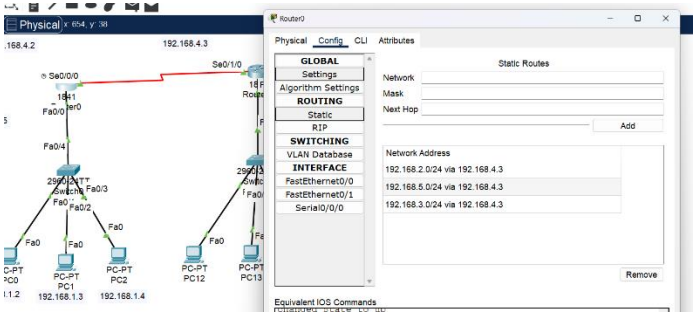

Figura 3.10. Configurarea routingului static la primul router

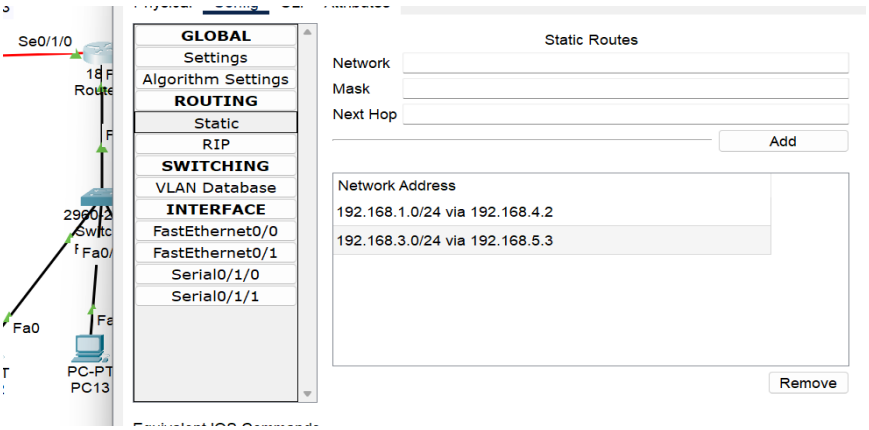

Figura 3.11. Configurarea routingului static la al doilea router

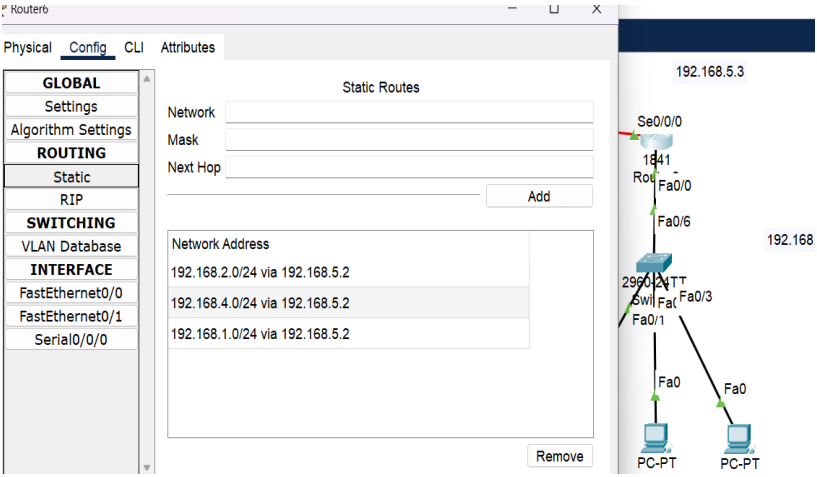

Figura 3.12. Configurarea routingului static la al treilea router

După configurarea rețelei, se utilizează comanda `ping` pentru a verifica dacă există conexiune între dispozitive. Se trimit pachete de date către routere și calculatoare pentru a verifica accesibilitatea lor. Comanda `show ip route` afișează tabelul de rutare a routerului, oferind informații despre rețelele IP cunoscute și rutele către ele. Se verifică rutele statice configurate anterior pentru a se asigura corectitudinea lor.

Se trimit pachete *ping* între calculatoarele din diferite subrețele pentru a verifica dacă pot comunica. Acest lucru confirmă segmentarea corectă a rețelei. Se verifică conexiunea dintre primul calculator (Subrețeaua 1) și ultimul calculator (Subrețeaua 3). Se trimite un *ping* de la primul calculator la adresa IP a ultimului. Succesul *ping-ului* demonstrează funcționarea corectă a rețelei. Utilizarea combinată a metodelor de mai sus oferă o imagine completă a stării rețelei, permițând identificarea și remedierea promptă a problemelor de conectivitate sau rutare.

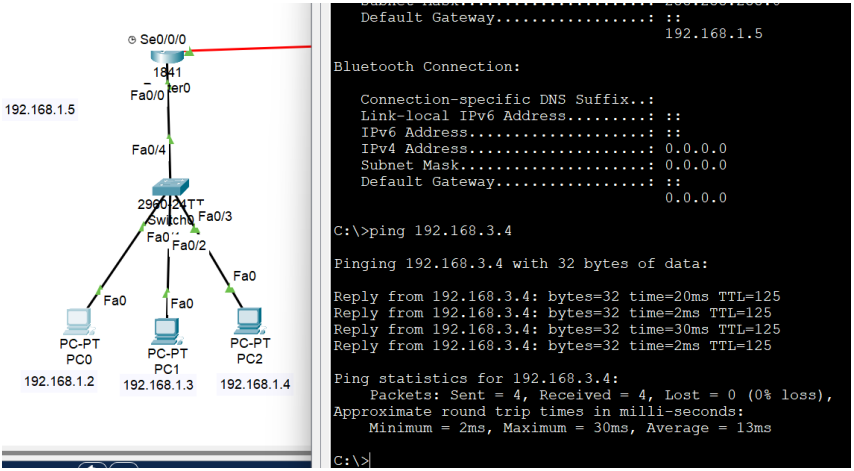

Figura 3.13. Legătura primului calculator cu ultimul prin comanada ping

5. Conținutul raportului

1. Introducere:
    a. Scopul și obiectivele lucrării de laborator.
    b. Descrierea generală a rețelei locale și a necesității utilizării algoritmilor de routing.
2. Descrierea rețelei locale:
    a. Prezentarea topologiei rețelei: routere, switch-uri, calculatoare etc.
    b. Configurarea inițială a dispozitivelor din rețea: setarea adreselor IP, configurarea interfețelor de rețea etc.
3. Algoritmii de routing utilizați:
    a. Explicarea conceptelor și principiilor de bază ale algoritmilor de routing: static, RIP, OSPF etc.

    b. Descrierea modului de funcționare a fiecărui algoritm în cadrul rețelei locale proiectate.
4. Configurarea algoritmilor de routing:
    a. Configurarea și setarea algoritmilor de routing pe dispozitivele din rețea.
    b. Descrierea pașilor specifici necesari pentru fiecare algoritm.
5. Verificarea funcționării algoritmilor de routing:
    a. Utilizarea comenzilor specifice pentru a verifica starea și funcționarea algoritmilor de routing pe dispozitivele din rețea.
    b. Testarea conectivității între diferitele subrețele, utilizând algoritmii de routing configurați.
6. Concluzie:
    a. Rezultatele obținute în cadrul lucrării de laborator.
    b. Observații și concluzii privind eficiența și performanța algoritmilor de routing utilizați.
7. Bibliografie:
    a. Sursele bibliografice utilizate pentru a înțelege conceptele și principiile algoritmilor de routing.
8. Anexe:
    a. Capturi de ecran cu configurările și interacțiunile din cadrul laboratorului, dacă este necesar.

Întrebări de control

1. Definiți conceptul de rutare dinamică și explicați avantajele sale în comparație cu rutarea statică.
2. Prezentați două protocoale de rutare dinamică comune și menționați diferențele majore dintre ele.

3. Exemplificați configurarea RIP prin CLI (Command Line Interface) pe un router real sau virtual, specificând comenzile utilizate și parametrii configurabili.
4. Explicați ce este un tabel de rutare și care sunt elementele-cheie ale sale.
5. Descrieți modul în care un router utilizează tabelul de rutare pentru a direcționa traficul de rețea.
6. Definiți conceptul de echilibrare a sarcinii în contextul protocolului RIP și explicați beneficiile sale.
7. Exemplificați configurarea echilibrării sarcinii cu RIP pe un router virtual, menționând opțiunile disponibile și impactul lor.
8. Definiți protocolul BGP (Border Gateway Protocol) și menționați rolul său în internet.
9. Explicați diferențele dintre BGP extern și BGP intern, dând exemple de aplicabilitate pentru fiecare.
10. Prezentați BGP ca protocol de rutare dinamică și comparați-l cu RIP, evidențiind aspecte precum scalabilitatea și convergența.

Bibliografie

1. Doyle, J., & Carroll, J. (2016). Routing TCP/IP. Cisco Press.
2. Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach. Pearson.
3. Eggert, L., & Fritzsche, U. (2014). BGP: The Definitive Guide. O'Reilly Media.
4. Lammle, Todd. Routing Protocols and Concepts. CCIE Routing & Switching Certification Guide, 2nd ed., John Wiley & Sons, 2016.
5. Cisco Networking Academy. https://www.netacad.com/
6. Microsoft Learn. https://docs.microsoft.com/en-us/learn/
7. Tutorials Point. https://www.tutorialspoint.com/

Lucrarea de laborator nr.4
PROIECTAREA ȘI CONFIGURAREA REȚELELOR VIRTUALE

1. Scopul lucrării: a înțelege și a configura VLAN-urile, a oferi experiență practică în implementarea VLAN-urilor într-un mediu simulat și a dezvolta abilități de proiectare și depanare a rețelelor VLAN.

2. Noţiuni teoretice generale

1) Configurarea VLAN-urilor și a magistralelor

Comutatoarele împart domeniul de coliziune în mai multe domenii mai mici și reprezintă, de asemenea, un singur domeniu de difuzare.

Rețelele locale virtuale (VLAN) fac posibil ca pe un singur comutator să avem un singur domeniu de difuzare. LAN-urile fac posibil ca pe un singur comutator să avem mai multe domenii de difuzare. Cu toate acestea, prin crearea mai multor VLAN-uri pe un singur switch, ne vom confrunta cu problema de a răspândi această configurația pe toate celelalte switch-uri. Astfel, vor apărea multe switch-uri cu distribuții diferite cu setări VLAN diferite. De aceea, intervine VTP (VLAN Trunking Protocol). Corespunzător cu VLAN-urile și protocolul VTP, se simplifică managementul. În continuare vom examina rutarea interVLAN pentru a descrie formarea comunicării dintre VLAN-uri diferite.

2) Crearea unui VLAN și a unui domeniu VTP

VLAN-urile sunt o tehnologie care presupune împărțirea unei rețele simple de nivelul 2 în mai multe domenii de difuzare. Acest lucru restricționează comunicarea în rețea doar la dispozitivele care

se află în același domeniu de difuzare. În același timp, dispozitivele pot comunica în continuare, dar utilizând dispozitive de nivelul 3, cum ar fi routerele sau switch-uri de nivelul 3. În general, acest lucru se aseamănă cu conectarea dispozitivelor utilizatorului la diferite switch-uri, apoi conectarea comutatoarelor prin intermediul unui router ca domenii de difuzare (subrețele) separate.

Cu cât sunt create mai multe VLAN-uri, cu atât devine mai anevoioasă propagarea configurației la toate switch-urile din rețea. Acesta este motivul pentru care a fost creat protocolul VLAN Trunking Protocol (VTP). Inițial vom descrie crearea și atribuirea porturilor VLAN. VLAN de management al rețelei (VLAN 1) este prezent pe toate switch-urile în același timp, iar toate porturile switch-urilor sunt alocate acestui VLAN.

Următoarea comandă este utilizată pentru a crea un VLAN:

```
Sw1(config)#vlan 2
```

Identificatorul (numărul) VLAN poate lua valori cuprinse între 1 și 1001. Numerele de la 1002 la 1005 sunt rezervate. Când se introduce comanda de mai sus, se intră în modul de configurare VLAN. Aici se poate atribui un nume al VLAN:

```
Sw1(config-vlan)#name finance
```

Atribuirea unui nume este opțională. Dacă nu se atribuie manual un nume, sistemul va genera un nume pe baza numărului de rețea, în cazul dat (VLAN2). Acesta va fi VLAN0002.

În continuare, trebuie se adauge mai multe porturi la acest VLAN. Pentru a atribui mai multe porturi odată unui VLAN, se poate utiliza opțiunea range, urmată de intervalul de porturi:

```
Sw1(config)#interface range f0/10-20
```

Următoarea comandă se va utiliza pentru a atribui aceste porturi la VLAN2:

```
Sw1(config-if-range)#switchport access vlan 2
```

În cele din urmă, este necesar de asigurat că porturile sunt alocate efectiv la VLAN-ul corect:

```
Sw1#show vlan
```

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 4.1. Rezultatul comenzii show vlan

Unele dintre liniile tipărite la executarea acestei comenzi au fost omise din motive de concizie.

Se va crea o nouă topologie cu trei switch-uri pentru a demonstra principiile protocolului VTP. Protocolul VLAN backbone are trei moduri de funcționare: server, client și transparent.

1. Modul server este activat implicit. În acest mod, comutatoarele au permisiunea de a-și modifica VLAN-urile și de a trimite anunțuri VTR.
2. În modul client, comutatoarele ascultă anunțurile VTP de la alte comutatoare care funcționează în modul server. Comutatoarele care funcționează în modul client VTP nu-și pot modifica local propria bază de date; acest lucru este posibil numai pe baza anunțurilor VTP primite.
3. Modul de funcționare transparent implică independența față de alte comutatoare. În acest mod, comutatorul promovează doar anunțurile VTP pe care le-a acceptat, dar nu generează

niciun anunț și nici nu își modifică propria bază de date VLAN pe baza anunțurilor VTP.

Următoarea topologie (figura 4.2) va servi la demonstrarea principiilor protocolului VTP.

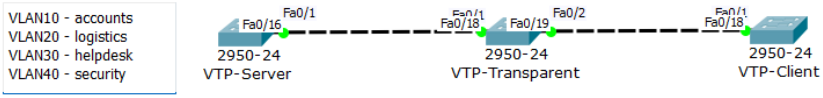

Figura 4.2. Exemplu de demonstrare a modurilor de funcționare a protocolului VTP

1) Pe primul switch (VTP-Server) se creează 4 VLAN-uri cu nume diferite, așa cum se arată în figura 4.2. Apoi se formează o legătură trunchi între switch-uri prin setarea porturilor dintre switch-uri în modul trunchi:

```
VTP-Server(config)#interface Fa0/1
VTP-Server(config-if)#switchport mode trunk
VTP-Transparent(config)#interface range Fa0/1-2
VTP-Transparent(config-if-range)#switchport mode trunk
VTP-Client(config)#interface Fa0/1
VTP-Client(config-if)#switchport mode trunk
```

2) Se utilizează modul server VTP implicit; este necesar a modifica numele domeniului VTP și a seta parola:

```
VTP-Server(config)#vtp domain My-Office
Changing VTP domain name from NULL to My-Office
VTP-Server(config)#vtp password s3cRet
Setting device VLAN database password to s3cRet
```

3) Se trece la cel de-al doilea switch (VTP-Transparent) și se instalează în modul transparent:

```
VTP-Transparent(config)#vtp mode transparent
```

4) În cele din urmă, cel de-al treilea switch (VTP-Client) se trece în modul client:

```
VTP-Client(config)#vtp mode client
```

5) Nu trebuie să se modifice numele domeniului VTP pe acest comutator. Acest comutator se va alătura domeniului VTP sub influența serverului VTP (VTP-Server). Parola trebuie să fie setată la aceeași parolă cu cea a serverului:

```
VTP-Client(config)#vtp password s3cRet
```

Configurarea rețelei este completă. Acum, utilizând funcția show vlan pe switch-ul VTP-Client, putem vizualiza noul VLAN. Acest exemplu demonstrează principiile VTP. Această topologie nu are sens, deoarece nu există o comunicare normală între switch-ul VTP-Server și switch-ul VTP-Client.

Între ele se află comutatorul VTP-Transparent, care funcționează în modul transparent și nu are niciunul dintre VLAN-urile care au fost configurate.

3) Configurarea rutării între VLAN-uri (inter-VLAN)

Deși VLAN-urile sunt create pentru a împărți un domeniu de bandă largă în domenii mai mici, acestea au nevoie de un strat de rețea cu rutare IP pentru a comunica între ele. Acesta este denumit inter-VLAN (rutare inter-VLAN) și se poate realiza utilizând atât routere, cât și comutatoare de nivelul 3. Rutarea inter-VLAN necesită o subrețea separată pentru fiecare subrețea.

Se va configura rutarea inter-VLAN prin conectarea routerului la switch cu o singură legătură. Tot traficul din diferite VLAN-uri trece prin această legătură. Această metodă de configurare se

numește router-on-a-stick, deoarece utilizează un singur canal de router pentru a transporta tot traficul.

4) Configurarea inter-VLAN pe router

Pentru a configura rutarea între rețelele virtuale se utilizează topologia ca în figura 4.3.

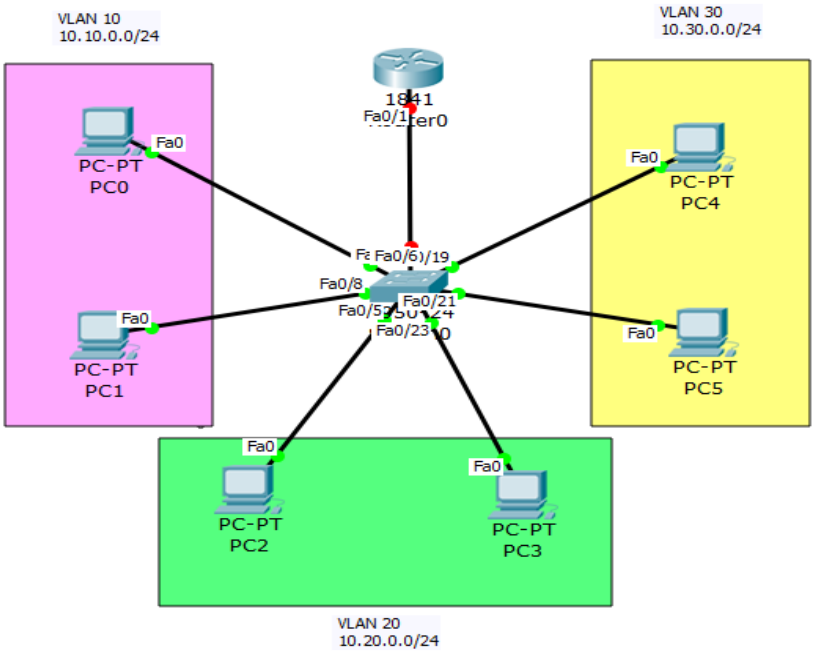

Figura 4.3. Rutarea inter-VLAN

Reamintim că fiecare VLAN va avea o singură subrețea IP, iar routerul trebuie să aibă trei adrese IP corespunzătoare fiecărui VLAN:

1) După atribuirea adreselor IP tuturor calculatoarelor (adresele IP ale subrețelelor sunt reprezentate în figura 4.3, ca porți de acces implicite se vor utiliza rețelele virtuale necesare pe

switch și se vor atribui porturile acestuia la VLAN-uri specifice:

```
Sw1(config)#int range f0/2-3
Sw1(config-if-range)#switchport access vlan 10
Sw1(config-if-range)#int range f0/4-5
Sw1(config-if-range)#switchport access vlan 20
Sw1(config-if-range)#int range f0/6-7
Sw1(config-if-range)#switchport access vlan 30
```

2) Se configurează portul switch-ului conectat la router ca un port trunchi:

```
Sw1(config)#int f0/1
Sw1(config-if)#switchport mode trunk
```

3) În continuare, se selectează routerul și se activează portul conectat la switch:

```
R1(config)#int f0/0
R1(config-if)#no shutdown
```

4) Se vor forma subinterfețe pe interfața fa0/0. Fiecare dintre subinterfețe va avea propria sa adresă IP corespunzătoare unui VLAN specific:

```
R1(config-subif)#int f0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 10.10.0.1
255.255.255.0
R1(config-subif)#int f0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.20.0.1
255.255.255.0
R1(config-subif)#int f0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 10.30.0.1
255.255.255.0
```

5) Se va atrage atenția la comanda de încapsulare. Aceasta definește numărul rețelei virtuale în care va fi localizată subinterfața.
6) Configurarea este finalizată, singurul lucru care mai trebuie făcut este testarea conectivității între calculatoarele din diferite VLAN-uri cu ajutorul instrumentului "Simple PDU" sau utilitarului ping. Este posibil ca primul pachet să se piardă din cauza unei anumite întârzieri asociate cu solicitarea ARP. Pentru a vedea traseul pachetelor, folosim utilitarul tracert.

5) Configurarea inter-VLAN pe comutatorul de nivelul 3

Packet Tracer are doar un singur comutator de nivelul 3. 3560-24PS. Drept exemplu vom folosi aceeași topologie, înlocuind routerul cu un comutator de nivelul 3 (figura 4.4).

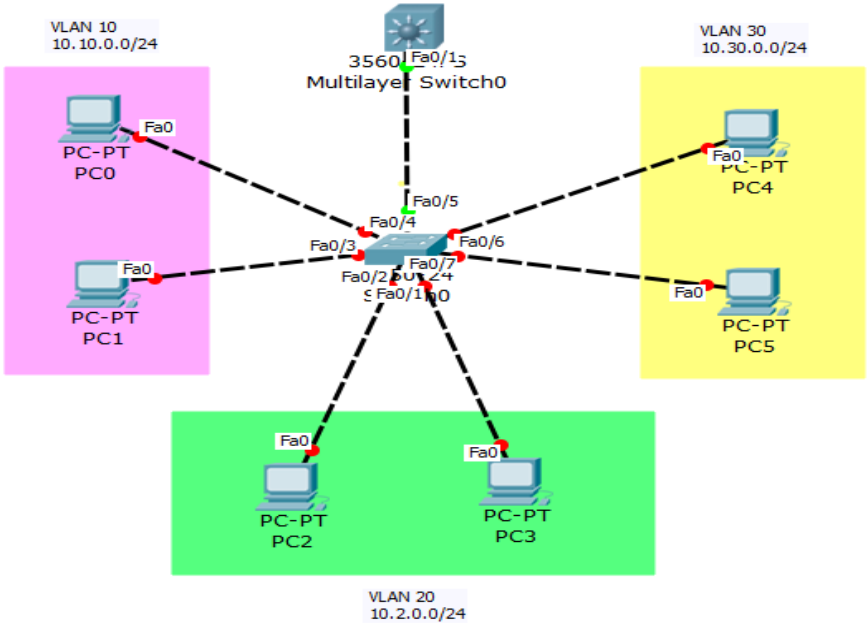

Figura 4.4. Rutarea inter-VLAN pe un comutator de nivelul 3

Deoarece în acest exemplu crearea VLAN-urilor și a VLAN-urilor aferente pe switch-ul de nivelul 2 este aceeași ca și în exemplul anterior, omitem această parte a configurării și trecem la configurarea switch-ului de nivelul 3. Se va indica că interfața fa0/1 a acestui comutator va fi în modul port trunchi, după cum se poate verifica prin următoarea comandă:

```
MSw1#show interface trunk
```

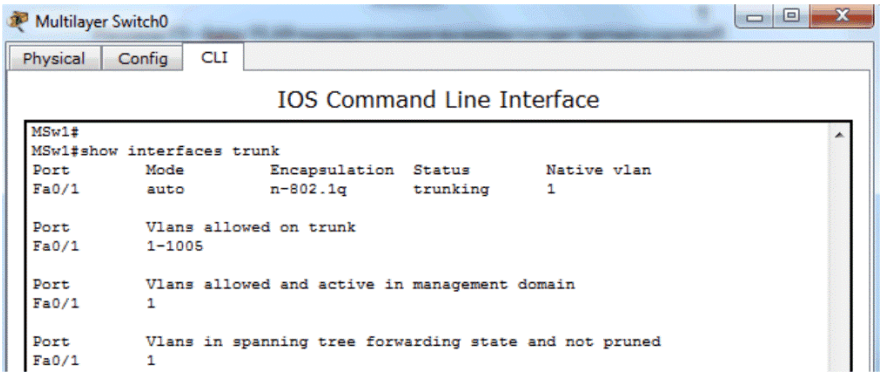

Figura 4.5. Rezultatul rulării show interface trunk

Valoarea câmpului de stare trunking indică modul de funcționare trunking al acestui port:

1) Trebuie configurată o așa-numită SVI (Switch Virtual Interface) pentru switch-ul de nivelul 3, care permite utilizarea interfeței de nivelul 3 pentru fiecare VLAN:

```
MSw1(config)#int vlan 10
MSw1(config-if)#ip add 10.10.0.1
255.255.255.0
MSw1(config-if)#int vlan 20
MSw1(config-if)#ip add 10.20.0.1
255.255.255.0
MSw1(config-if)#int vlan 30
```

```
MSw1(config-if)#ip add 10.30.0.1
255.255.255.0
```

2) Aceste interfețe vor fi în starea off, deoarece switch-ul nu are VLAN 10, VLAN 20. Comutatorul nu are VLAN 10, VLAN 20, VLAN 30. Ele pot fi create folosind următoarele comenzi:

```
MSw1(config)#vlan 10
MSw1(config-vlan)#vlan 20
MSw1(config-vlan)#vlan 30
```

3) După introducerea fiecăreia dintre comenzi, interfețele SVI corespunzătoare vor deveni active. De asemenea, trebuie să fie activată rutarea IP pe comutatorul de nivelul 3:

```
MSw1(config)#ip routing
```

4) În cele din urmă, se utilizează instrumentul "Simple PDU" pentru a efectua un test de conectivitate.

Se va fixa că primul pachet va fi, de asemenea, pierdut din cauza întârzierii asociate cu solicitarea ARP.

6) Canale magistrale (backbone) ale comutatoarelor

Când două switch-uri sunt conectate între ele, trebuie să existe un mecanism care să identifice dacă cadrele aparțin unui anumit VLAN. Acest lucru nu are nimic de-a face cu stratul fizic, ci mai degrabă se află în întregime în stratul de legătură de date. Când două switch-uri sunt conectate între ele, fiecare switch trebuie să știe cărui VLAN este destinat traficul transmis. Pentru aceasta se folosește marcarea cadrelor. Când cadrele sunt transmise pe o legătură între switch-uri, switch-ul de ieșire inserează în cadru câmpuri suplimentare asociate cu ID-ul VLAN. Canalul dintre switch-uri se numește trunchi (trunk).

În figura 4.6 sunt reprezentate detaliile cadrelor de intrare și de ieșire capturate în modul de simulare când un PC din VLAN 10 face

ping la un PC din VLAN 30, iar din VLAN 10 face ping la un PC din VLAN 30.

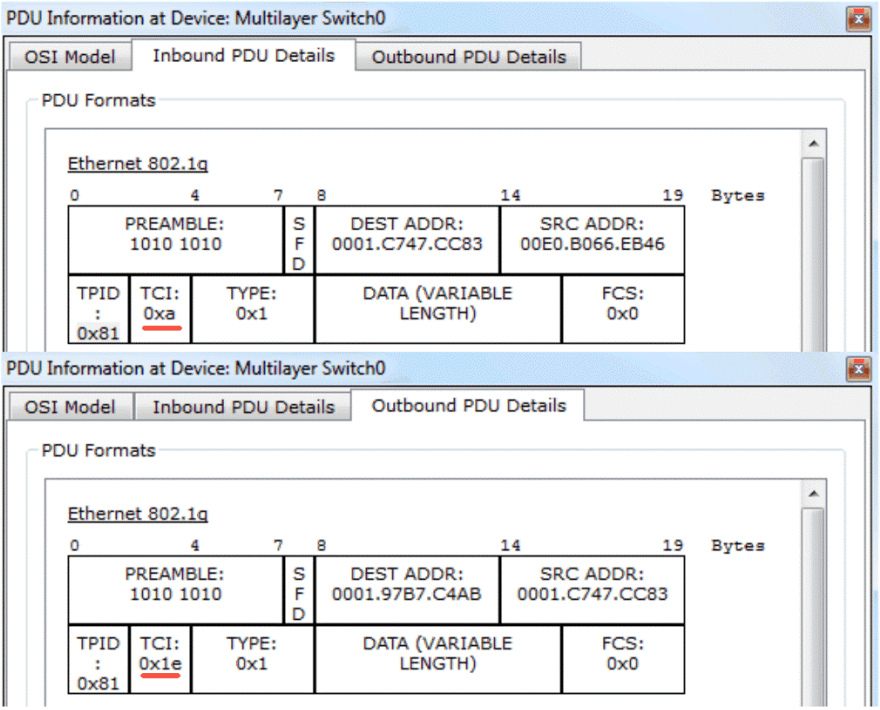

Figura 4.6. Cadre etichetate cu ID-uri VLAN diferite

Se va fixa că câmpul TCI (Tag Control Information) conține valoarea hexazecimală a ID-ului VLAN. Pentru un cadru de intrare, aceasta este 0xA, ce corespunde VLAN 10; pentru un cadru de ieșire este 0x1E, care la rândul său corespunde VLAN 20.

7) Analiza funcționării VLAN în modul de simulare

Conceptul de VLAN implică împărțirea unui domeniu de difuzare. Se va examina în mod simulat modul în care sunt gestionate cadrele de difuzare aparținând unor VLAN-uri diferite. Se va utiliza topologia anterioară. Cu ajutorul instrumentului Complex PDU se

creează un pachet ICMP de la PC către întreaga rețea, specificând 255.255.255.255. ca adresă IP de destinație. Astfel, se stabilește adresa de difuzare la nivelul de legătură (FFFF.FFFF.FFFF). La trecerea în modul de simulare se observă ce se va întâmpla. Comutatorul primește un pachet ICMP de la PC0 și trimite doar două copii ale acestui pachet: una către comutatorul de nivelul 3 (sau router) și către PC1, care se află pe același VLAN 10.

Dacă nu ar exista partiționarea VLAN, un astfel de pachet ar trebui să fie livrat tuturor PC conectate la switch.

3. Ordinea efectuării lucrării de laborator

1. Se cere proiectarea unei subrețele bazate pe switch, având la bază topologia reprezentată în figura 4.7.
2. Să se atribuie IP și masca subrețelei pentru fiecare subrețea în parte, corespunzător specificațiilor reprezentate în figura 4.7.
3. Crearea VLAN-urilor necesare. Atribuirea interfețelor corespunzătoare. Setarea porturilor.
4. Să se verifice conexiunile dintre hosturi, folosind comanda ping (figurile 4.8, 4.9).
5. Să se seteze porturile care unesc switch-urile într-un trunk mode.
6. Verificarea finală a conexiunii cu ajutorul comenzii show interfaces trunc și comenzii ping (figura 4.10).

4. Efectuarea lucrării de laborator

Se cere proiectarea unei subrețele bazate pe switch, având la bază topologia reprezentată în figura 4.7. Calculatoare conectate la switch-uri fac parte din diferite subrețele. Atribuiți fiecărui calculator adresele IP specificate pe topologia din figura 4.7.

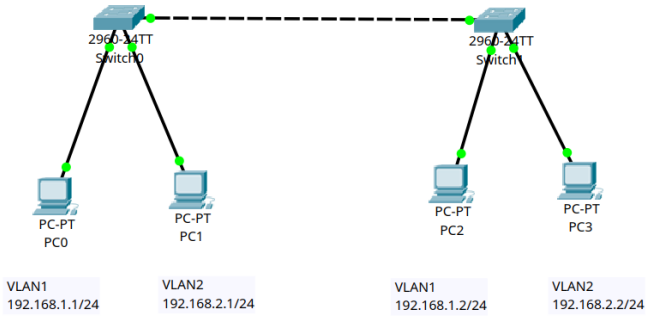

Figura 4.7. Topologia din două subrețele propusă pentru proiectare

Pentru a configura VLAN-uri este necesaă:

1. **Crearea VLAN-urilor** necesare, identificând grupurile logice de dispozitive din rețea.
2. **Atribuirea interfețelor:** atribuirea interfețelor fizice (porturi) la VLAN-urile create anterior.
3. **Configurarea trunk mode:** pentru a permite comunicarea între VLAN-uri pe un singur cablu, este necesară configurarea porturilor care unesc două switch-uri în modul trunk.
4. **Specificarea VLAN ID:** pe porturile trunk este necesară configurarea permiselor pentru a permite traficul între VLAN-urile conectate.
5. **Testarea configurației:** după finalizarea configurării este esențial să se testeze funcționarea VLAN-urilor și conectivitatea dintre dispozitivele din rețea.

Lucrarea de laborator va începe cu configurarea switch-urilor, stabilind setările fundamentale pentru funcționarea rețelei. Când este finalizată configurarea switch-urilor, vom fi gata pentru etapa următoare: crearea și configurarea VLAN-urilor.

1) Pentru setarea Switch-urilor se propun următoarele comenzi**:**

```
Switch>en
Switch#config t
Enter configuration commands, one per line. End
with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname SW1
SW1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/24, changed state to up

SW1(config)#do show vlan

VLAN Name Status Ports
---- -------------------------------- ---------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Gig0/1
Gig0/2
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp
BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------
1 enet 100001 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
```

```
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
Remote SPAN VLANs
------------------------------------------------
-----------Primary Secondary Type Ports
------- --------- -----------------
SW1(config)#vlan 2
SW1(config-vlan)#name STUDENTS
SW1(config-vlan)#do show vlan

VLAN Name Status Ports
---- -------------------------------- ---------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Gig0/1
Gig0/2
2 STUDENTS active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

VLAN Type SAID MTU Parent RingNo BridgeNo Stp
BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------
1 enet 100001 1500 - - - - - 0 0
2 enet 100002 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
```

```
Remote SPAN VLANs
------------------------------------------------
Primary Secondary Type Ports
------- --------- -----------------
SW1(config-vlan)#
```

După configurarea cu succes a primului switch, procesul va fi repetat pentru al doilea switch, asigurând o configurație uniformă a dispozitivelor din rețea. Când va finaliza configurarea celui de-al doilea switch, se va verifica sincronizarea setărilor pentru a garanta funcționarea corectă a ambelor dispozitive.

2) Următorul pas este identificarea interfețelor fizice (porturi) disponibile pe switch-uri. Fiecare port va fi alocat unui VLAN specific, respectând segmentarea logică definită anterior:

```
SW1(config-if)#exit
SW1(config)#int f0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
SW1(config-if)#do show vlan


VLAN Name Status Ports
---- -------------------------------- --------- -
1 default active Fa0/1, Fa0/3, Fa0/4, Fa0/5
Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/11, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Gig0/1, Gig0/2
2 STUDENTS active Fa0/2
```

```
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp
BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------
1 enet 100001 1500 - - - - - 0 0
2 enet 100002 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs
------------------------------------------------
-----------Primary Secondary Type Ports
------- --------- ----------------- -------------
SW1(config-if)#
```

După configurarea cu succes a primului switch, procesul va fi repetat pentru al doilea switch.

3) Se utilizează comanda ping pentru a verifica dacă există o conexiune activă la un dispozitiv specific din rețea.

În VLAN 2 se observă probleme de conectivitate (figura 4.8). S-a constatat că dispozitivele din VLAN 2 nu pot stabili conexiunea cu alte dispozitive din rețea.

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figura 4.8. Rezultatul comenzii ping pentru VLAN2

Pe de altă parte, s-a confirmat funcționarea corectă a conexiunii în VLAN 1, demonstrată prin succesul comenzii ping (figura 4.9).

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::201:C9FF:FEAD:8DDC
   IP Address......................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.1.254

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 4.9. Rezultatul comenzii ping pentru VLAN1

Configurarea porturilor ca trunk pe switch-uri este necesară pentru a permite comunicarea dintre VLAN-uri și a remedia problemele de conectivitate identificate în VLAN 2. Configurarea trunk pe porturi va crea un canal logic care va permite schimbul de trafic între VLAN-uri. Această configurație va elimina limitările impuse de segmentarea VLAN-urilor și va facilita comunicarea între dispozitivele din VLAN 2 și restul rețelei.

4) Să fie setate porturile care unesc două switch-uri în trunk mode. Pentru a permite comunicarea între VLAN-uri pe un singur cablu, este necesară activarea modului trunk pe porturile care conectează cele două switch-uri. Pe ambele switch-uri, porturile configurate ca trunk trebuie să permită traficul pentru toate VLAN-urile active din rețea:

```
SW1#show interfaces trunk

SW1#show interfaces f0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association:
none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN:
none
```

```
Administrative private-vlan trunk encapsulation:
dot1q
Administrative private-vlan trunk normal VLANs:
none
Administrative private-vlan trunk private VLANs:
none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

SW1#config t
Enter configuration commands, one per line. End
with CNTL/Z.

SW1(config)#interface f0/24

SW1(config-if)#switchport mode trunk

SW1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/24, changed state to up

SW1(config-if)#^Z
SW1#
%SYS-5-CONFIG_I: Configured from console by
console
```

```
SW1#wr
Building configuration...
[OK]
SW1#show int f0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association:
none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN:
none
Administrative private-vlan trunk encapsulation:
dot1q
Administrative private-vlan trunk normal VLANs:
none
Administrative private-vlan trunk private VLANs:
none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

Pentru a verifica configurarea porturilor trunk pe switch-urile SW1 și SW2, se va utiliza comanda `show interfaces trunk`. Rezultatul comenzii va afișa detalii despre configurarea trunk, inclusiv VLAN-urile permise și starea administrativă a porturilor:

```
SW1>show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/24 on 802.1q trunking 1
Port Vlans allowed on trunk
Fa0/24 1-1005
Port Vlans allowed and active in management
domain
Fa0/24 1,2
Port Vlans in spanning tree forwarding state and
not pruned
Fa0/24 1,2
```

După configurarea trunk pe switch-uri, este esențial să se utilizeze comanda ping pentru a verifica restabilirea conexiunii dintre dispozitivele din VLAN 2 și restul rețelei. Se va efectua un ping de la un dispozitiv din VLAN 2 către un dispozitiv din VLAN1 (figura 4.10). Un ping reușit va confirma reabilitarea conexiunii și funcționarea corectă a rețelei.

Pe lângă ping, pot fi utilizate și alte metode pentru a verifica funcționalitatea rețelei, cum ar fi:

1. Traficul de rețea cu alte dispozitive.
2. Accesul la resursele partajate (fișiere, imprimante etc.).
3. Performanța generală a rețelei.

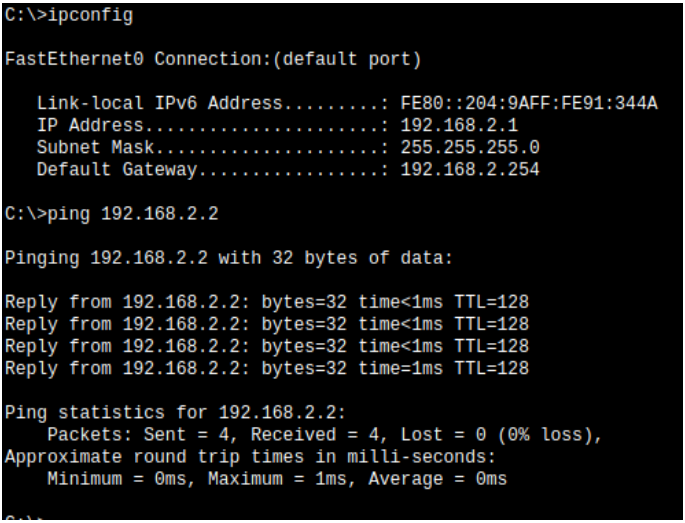

Figura 4.10. Rezultatul verificării finale prin comanda ping

5. Conținutul raportului

1. Introducere:
    a. Scopul și obiectivele lucrării de laborator.
    b. Descrierea generală a rețelei proiectate.
2. Descrierea rețelei proiectate:
    a. Prezentarea topologiei rețelei: switch-uri, routere, calculatoare etc.
    b. Configurarea fiecărui dispozitiv în cadrul rețelei: setarea adreselor IP, configurația gateway-ului etc.
3. Proiectarea și setarea subrețelelor:
    a. Descrierea proiectării și configurării subrețelelor, inclusiv a maselor și a adresei IP.
4. Proiectarea și setarea rutării între diferite subrețele:
    a. Configurarea statică a rutării între subrețele.
    b. Explicarea modului de funcționare a rutării statice în rețeaua proiectată.

5. Verificarea conexiunii dintre subrețele:
    a. Utilizarea comenzii ping pentru a verifica conectivitatea dintre diferite subrețele.
6. Concluzie:
    a. Rezultatele obținute în cadrul lucrării de laborator.
    b. Observațiile și concluziile finale.
7. Bibliografie:
    a. Sursele bibliografice utilizate în cadrul lucrării.
8. Anexe:
    a. Capturi de ecran cu configurările și interacțiunile din cadrul laboratorului, dacă este necesar.

Întrebări de control

1. Descrieți diferența dintre o magistrală de acces și o magistrală de agregare.
2. Ce este VTP (VLAN Trunking Protocol) și care este rolul său?
3. Cum se configurează rutarea statică inter-VLAN pe un router?
4. Cum se configurează inter-VLAN pe un switch de nivelul 3?
5. Care sunt tipurile de canale magistrale și care sunt diferențele dintre ele?
6. Care sunt pașii principali pentru a configura un VLAN într-un simulator de rețea?
7. Care sunt resursele disponibile pentru a depana problemele legate de VLAN?
8. Care sunt riscurile de securitate asociate cu VLAN-urile?
9. Cum se optimizează performanța VLAN pentru a satisface cerințele rețelei?
10. Cum se pot scala rețelele VLAN pentru a se adapta la cerințele viitoare?

Bibliografie

1. Tanenbaum, Andrew S., and David J. Wetherall. "Computer Networks." Pearson, 2010.
2. Cisco Press: CCNA Routing and Switching 200-301 Official Cert Guide, Volume 1:
3. Juniper Networks: Introduction to VLANs: [disponibil online] la data 22.03.24 https://www.juniper.net/documentation/en_US/junos/topics/concept/layer-2-vlan-security-understanding.html
4. NetworkLessons: VLANs, VTP, and Inter-VLAN Routing: [disponibil online] la data 22.03.24 https://networklessons.com/tag/vlan
5. IBM Developer Works: Configuring VLANs on an IBM System z Enterprise Console: [disponibil online] la data 22.03.24 https://cloud.ibm.com/docs/vlans?topic=vlans-getting-started
6. Fortinet: Configuring VLANs on a Fortinet Security Fabric: [disponibil online] la data 22.03.24 https://docs.fortinet.com/document/fortiswitch/7.0.8/devices-managed-by-fortios/546342/configuring-vlans

ANEXĂ

Pregătirea pentru lucrările de laborator
Instalarea programului Cisco Packet Tracer 6.2

Instalarea programului în Windows este simplă. Trebuie găsit fișierul corespunzător (de exemplu, cu numele "Cisco Packet Tracer 6.2 for Windows Student Version.exe"). Este suficient să deschideți acest fișier pentru a porni asistentul de instalare, apoi să acceptați acordul de licență, să alegeți o locație și să începeți instalarea.

a) După copierea versiunii programului în folderul corespunzător, se face dublu clic pe program *deschide fereastra de instalare*. Prin dublul clic cu mouse-ul pe programul copiat se inițiază procesul de instalare prin deschiderea ferestrei dedicate. Deschiderea ferestrei permite utilizatorului să înceapă și să completeze procesul de instalare a programului respectiv.

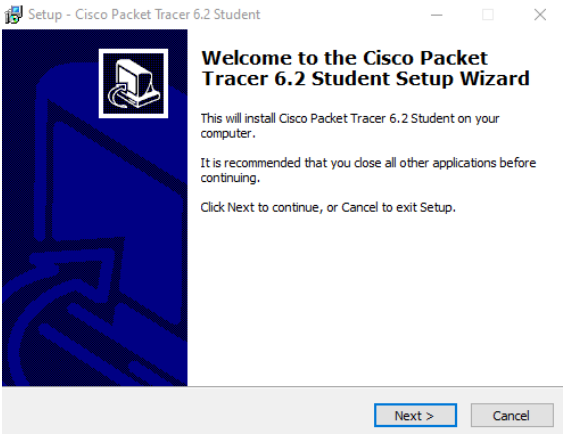

Figura A1.1. Inițierea procesului de instalare a softului CISCO Packet Tracer

b) Este necesară acceptarea condițiilor de licență pentru a continua procesul.

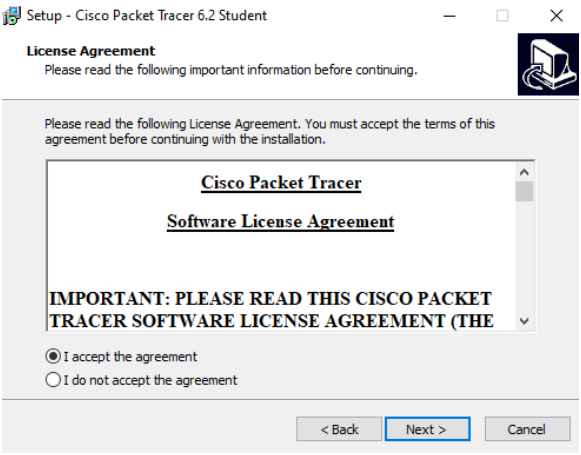

Figura A1.2. Acceptarea condițiilor de licență

c) Utilizatorului i se cere să aleagă folderul destinatar pentru instalarea programului.

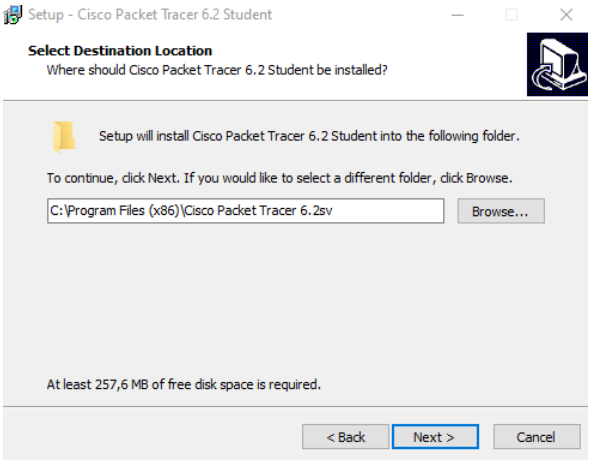

Figura A1.3. Alegerea locației de instalare

d) Utilizatorul trebuie să decidă asupra formării etichetei în procesul de instalare.

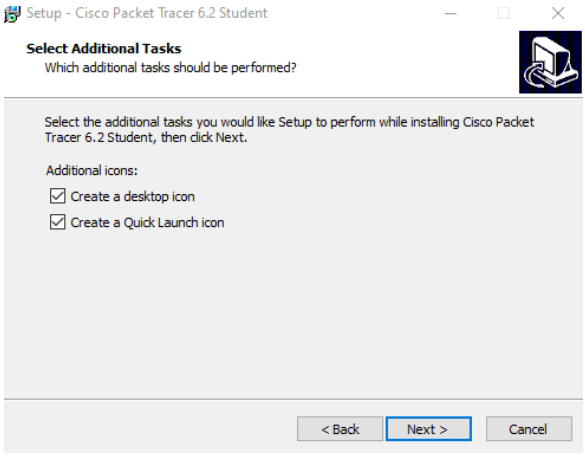

Figura A1.4. Generarea etichetelor

e) Facem clic pentru a începe instalarea programului.

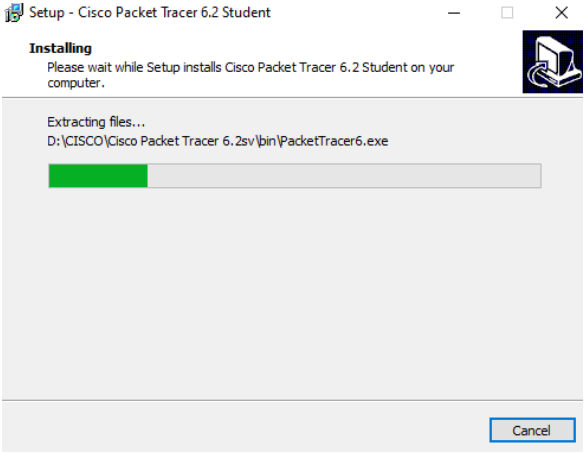

Figura A1.5. Procesul de instalare

f) Ultimul pas constă în alegerea folderului de destinație pentru stocarea fișierelor elaborate în Cisco.

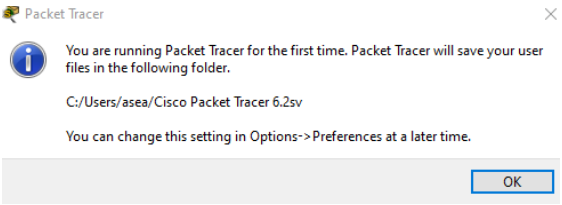

Figura A1.6. Alegerea mapei de salvare a proiectelor elaborate

g) În caz de necesitate, se acceptă utilizarea programului în cadrul sistemului de operare Windows.

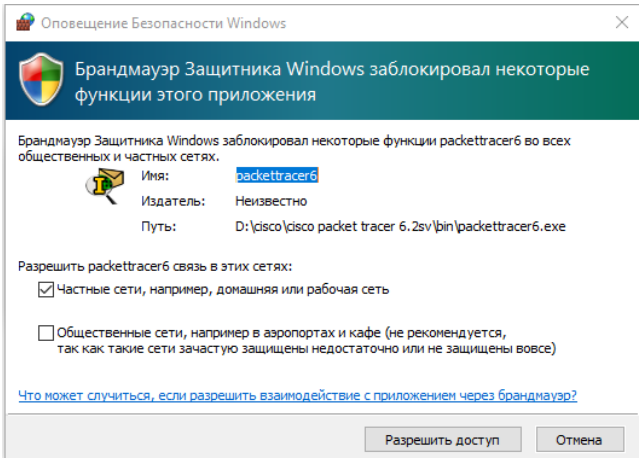

Figura A1.7. Acceptarea programului în sistemul de operare

h) După finalizarea instalării programului, este finisată etapa de pregătire pentru îndeplinirea lucrărilor de laborator.

CUPRINS

Îndrumar metodic
pentru lucrările de laborator

Partea II
Arhitectura rețelelor de calculatoare

Autori: Vasilii Crețu
Nicolae Magariu

Redactor E.Balan

Bun de tipar	Formatul hârtiei 60x84 1/16
Hârtie ofset. Tipar RISO	Tirajul 50 ex.
Coli de tipar 6,75	Comanda

MD-2004, Chișinău, bd. Ștefan cel Mare și Sfânt, 168, UTM
MD-2045, Chișinău, str. Studenților, 9/9, Editura „Tehnica-UTM”