**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.

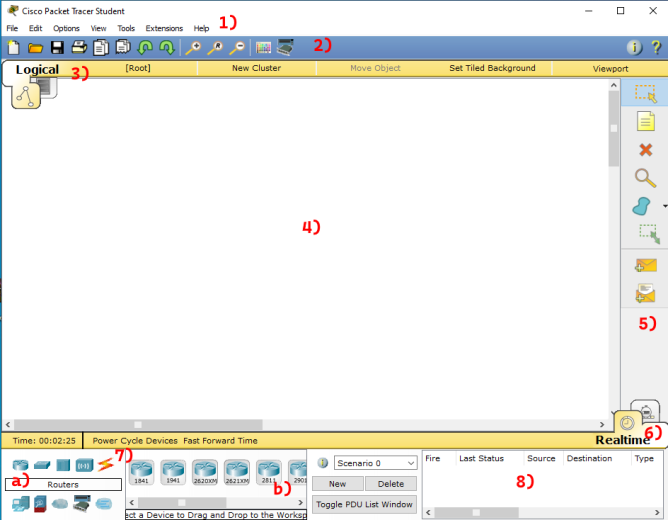
**Lucrarea de laborator nr.1  
PROIECTAREA SUBREȚELELOR PE BAZA UNUI SWITCH**

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. **Noţiuni 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.

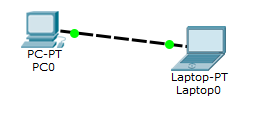
1. ***Fereastra principală de lucru Packet Tracer***
2. **Logical/Physical Workspace Tabs**. Spațiu de lucru logic/fizic, sunt utilizate pentru a comuta între spațiile de lucru logice sau fizice.
3. **Workspace.** Spațiu de lucru - acesta este spațiul de lucru principal în Packet Tracer unde se creează topologia necesară (configurația rețelei) și se afișează simularea procesului de comunicare în rețea.
4. **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***

1. **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.
2. **Network Component Box.** Caseta Componente de rețea conține echipamente de rețea și puncte finale disponibile în Packet Tracer. Este împărțită în două zone:
   1. **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);
   2. **Device-specific Selection Box.** Caseta de selecție specifică dispozitivelor. După selectarea unei categorii, aici devin disponibile diverse modele de dispozitive.
3. **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.
4. ***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***

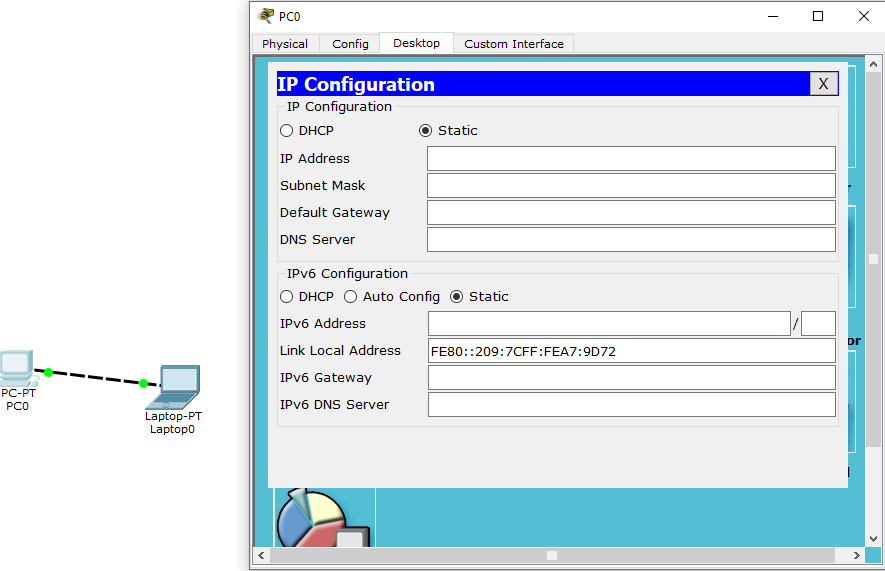
Pentru a seta un dispozitiv, cum ar fi un PC, se face clic pe imaginea acestuia, apoi se selectează fila Desktop (figura 1.3.). Se selectează instrumentul IP Configuration (Configurare IP) și se introduce IP Address (Adresă IP) și Subnet Mask (Mască de subrețea) ale dispozitivului.



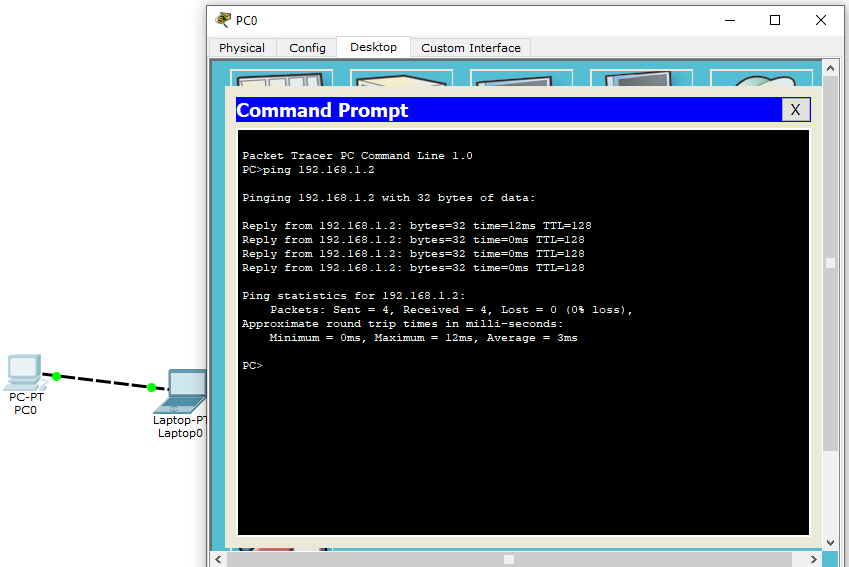
***Figura 1.3. PC desktop***

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).



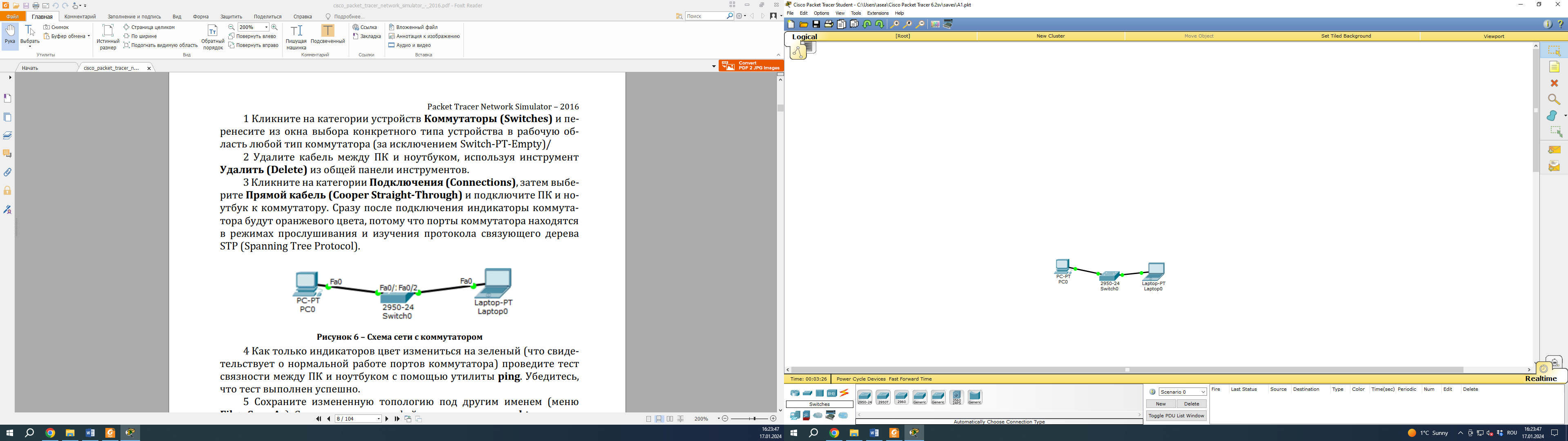
***Figura 1.4. Configurarea adresei și a măștii IP a PC-ului***



***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.

1. ***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*](http://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]:*

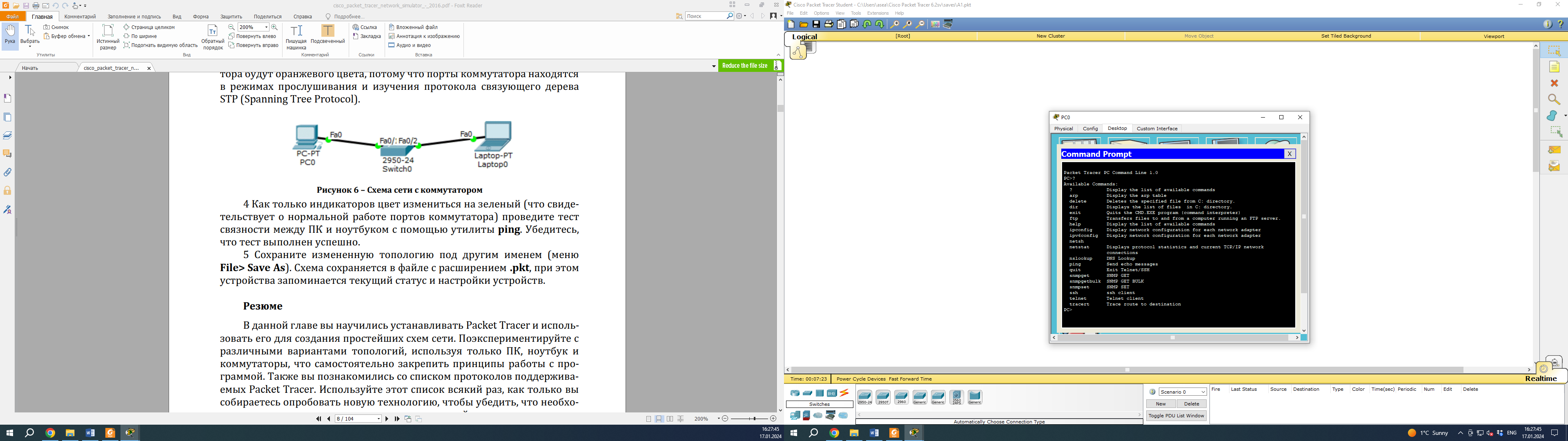
[utilizator]: Numele utilizatorului cu care doriți să vă conectați la dispozitiv;

[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.



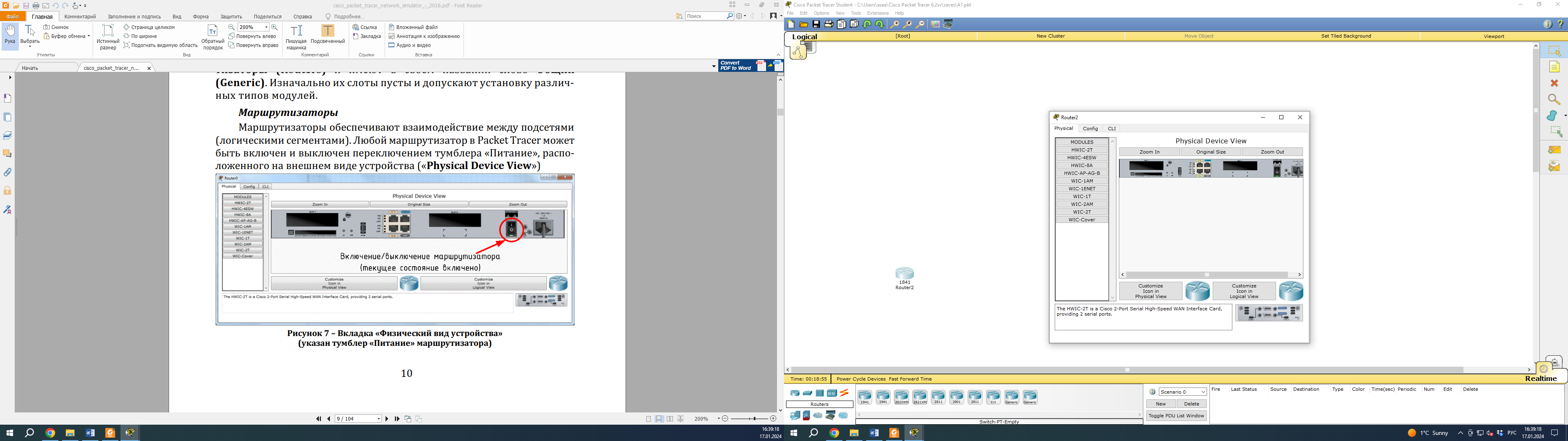
***Figura 1.7. Linia de comandă și comenzile de bază de nivel superior***

1. ***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.

1. **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.
9. **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.

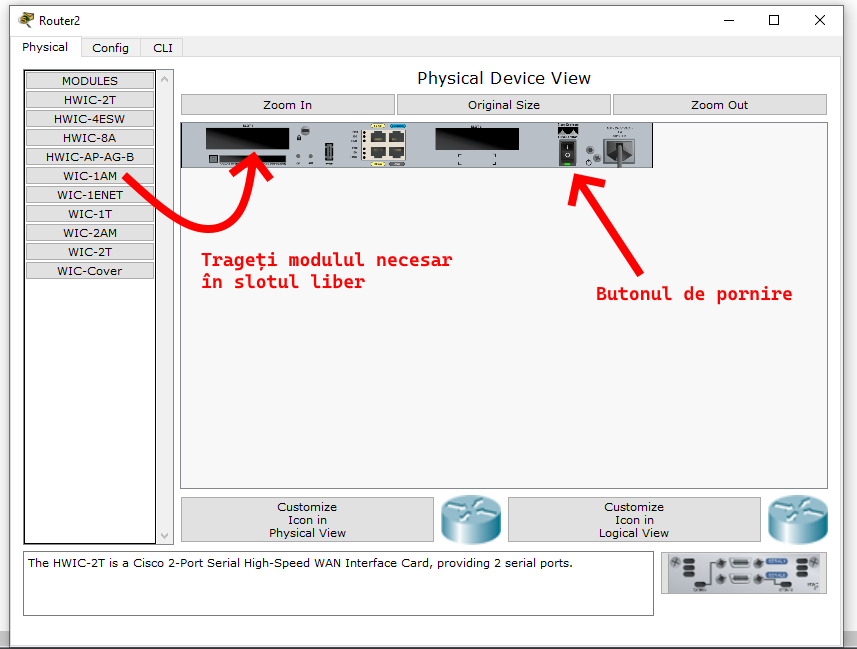
1. **Alte dispozitive**

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.
4. ***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, instalăndu-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.

1. ***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.

1. **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.
8. **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.
3. **Interfață serială**

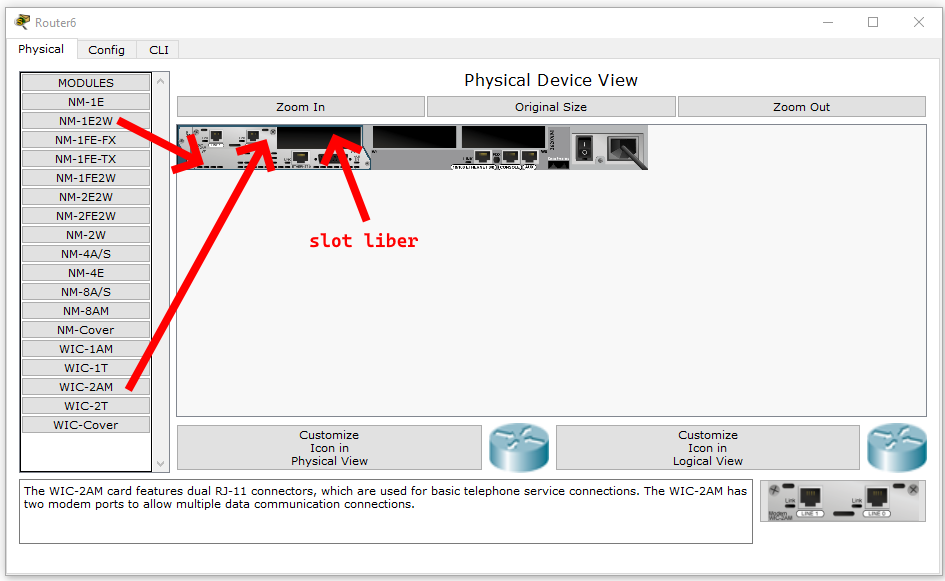
Numele acestor module conțin litera T sau o pereche de simboluri A/S. Modulele cu litera T sunt sincrone, iar modulele cu caracterele simbolice A/S sunt asincrone. Diferența în funcționarea lor este evidentă pentru hardware-ul real, în Packet Tracer nu există nicio diferență între ele:

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.
4. **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.
4. **Module WIC**

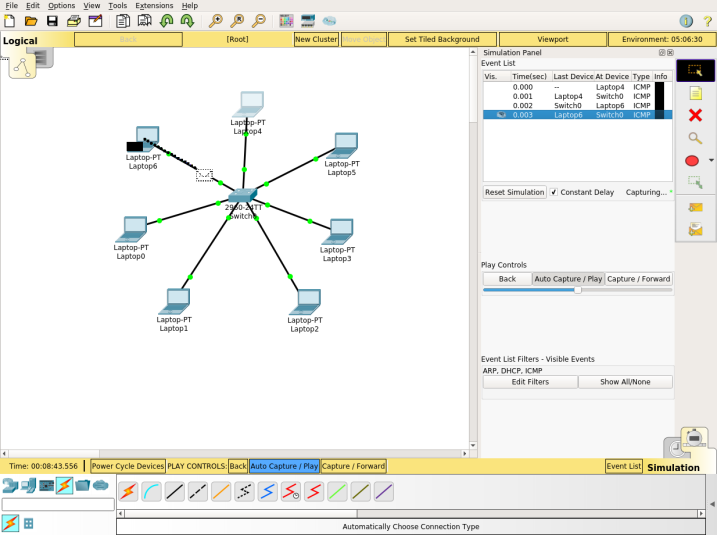
Modulele de rețea WIC nu ocupă întregul slot, module (WIC în cadrul modulelor de rețea(NM)) care au sloturi suplimentare pentru a suporta module mai mici. Aceste module pot fi recunoscute prin litera W la sfârșitul denumirii:



***Figura 1.10. Module cu suport pentru modulele WIC***

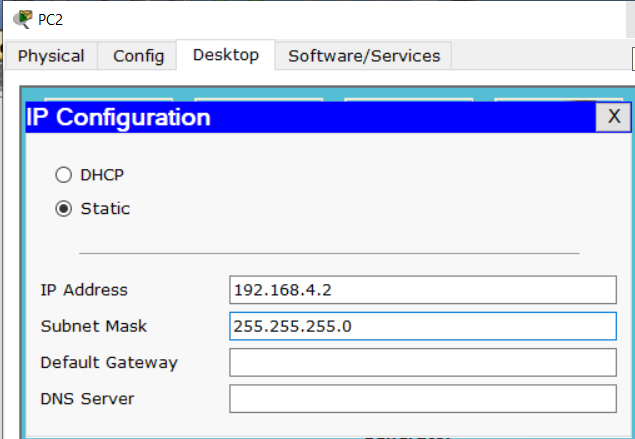
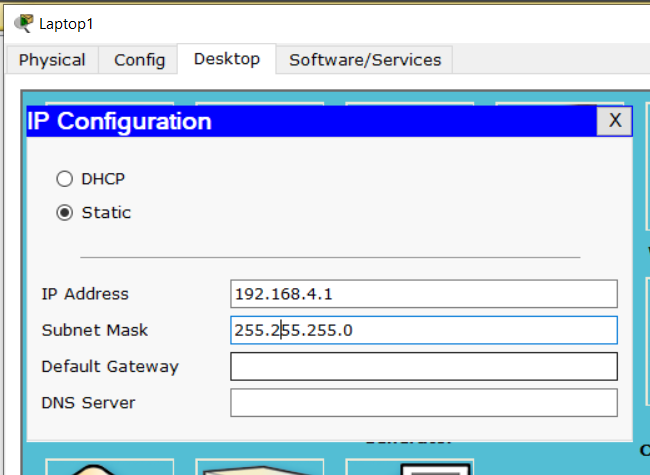
1. NM-1E2W, NM-1FE2W – un port Ethernet/două porturi Fast Ethernet cu suport pentru două sloturi WIC; un port Ethernet/două porturi Fast Ethernet cu suport pentru două sloturi WIC.
2. NM-2E2W, NM-2FE2W – două porturi Ethernet/ Fast Ethernet cu două sloturi WIC;
3. NM-2W – nu are porturi, conceput pentru a suporta două sloturi WIC.
4. **Ordinea efectuării lucrării de laborator**
5. Să se proiecteze o subrețea pe baza unui switch conform figurii 1.11).
6. Să se atribuie adrese IP și masca subrețelei în regim static (figura 1.12).
7. Să se verifice conexiunea dintre hosturile conectate în subrețea, folosind comanda ping în meniul consolei (figura 1.14).
8. 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.
9. Folosind un cablu de conexiune, să se conecteze switchiurile între ele (figura 1.15).
10. Să se verifice conexiunea dintre hosturile subrețelelor nr.1 și nr.2, folosind comanda ping (figura 1.17).
11. Să se noteze și să se facă concluziile în urma efectuării punctelor de mai sus.
12. 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.
13. Folosind comanda ping, să se verifice conexiunile.
14. **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:



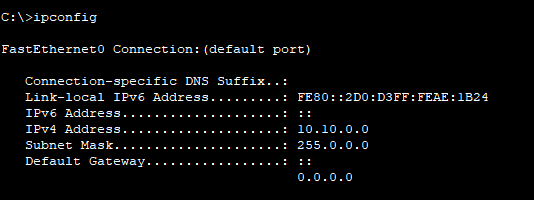
***Figura 1.11. Simularea CISCO a subrețelei pe bază de switch***

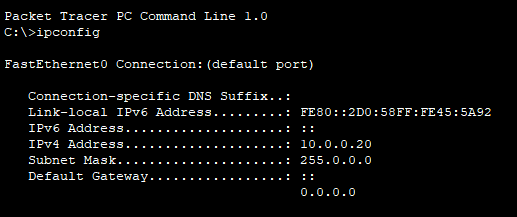
Este necesar să se configureze adresa IP pentru a permite comunicația între două dispozitive dintr-o subrețea. Adresa IP și mască trebuie să fie setate corect pentru a asigura conectivitatea și comunicarea eficientă dintre cele două dispozitive din subrețeaua respectivă.



***Figura 1.12. Configurarea adreselor IP și a măștilor de subrețea***

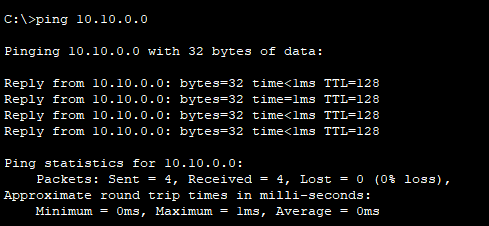
Pentru a verifica corectitudinea adresei, se utilizează comanda *ipconfig.* Comanda *ipconfig* oferă informații detaliate despre configurația rețelei, inclusiv adresele IP atribuite. Prin analizarea rezultatelor furnizate de comanda *ipconfig,* se poate asigura că adresele IP sunt configurate în mod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





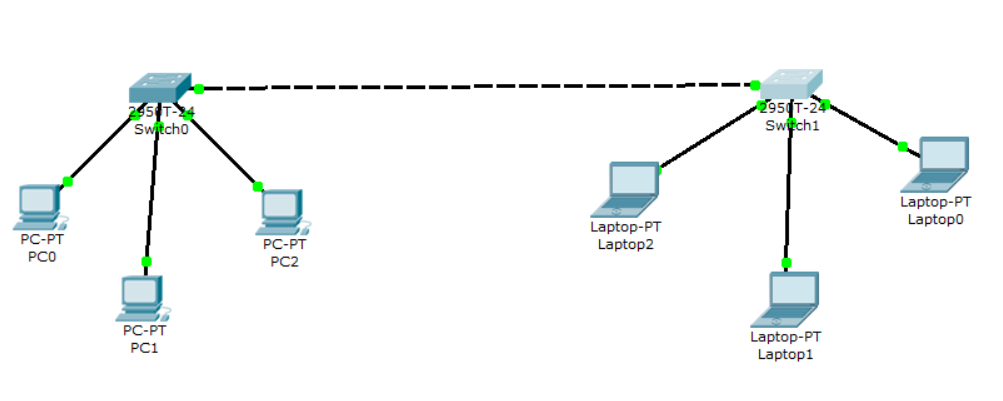
***Figura 1.13. Îndeplinirea comenzii ipconfig***

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.



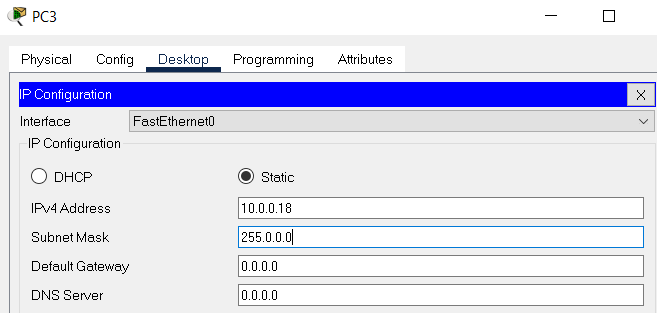
***Figura 1.14. Îndeplinirea comenzii ping***

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.

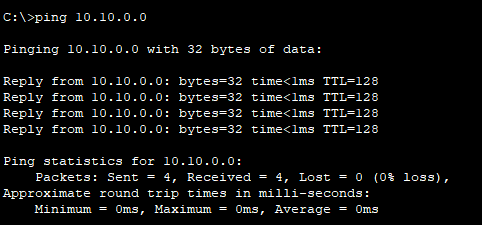


***Figura 1.15. Subrețea cu 2 switch-uri***

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***



***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

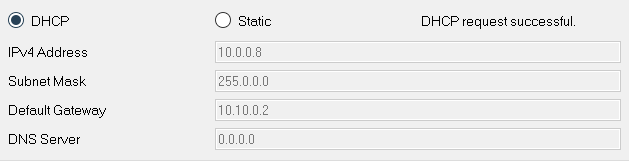
Router(dhcp-config)#exit

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***

1. **Conținutul raportului**
2. Introducere:
   1. 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.
3. Configurarea Switch-urilor:
   1. Detalii privind setarea parametrilor switch-urilor, cum ar fi adresa IP, masca de subrețea și gateway-ul.
   2. Descrierea topologiei subrețelei, inclusiv numărul de switch-uri și echipamente conectate.
4. Conectarea dispozitivelor la Switch:
   1. Pași detaliați pentru conectarea echipamentelor la switch-uri.
   2. Verificarea fizică a conexiunilor și asigurarea unei infrastructuri fizice corespunzătoare.
5. Configurarea adreselor IP:
   1. Instrucțiuni privind configurarea adreselor IP pentru dispozitivele conectate la switch-uri.
   2. Utilizarea comenzilor specifice pentru setarea parametrilor de rețea.
6. Verificarea conexiunilor și testarea comunicării:
   1. Utilizarea comenzilor precum ping pentru a verifica conectivitatea dintre echipamente.
   2. Testarea comunicației dintre diferitele dispozitive pentru a asigura o funcționalitate corespunzătoare.
7. Probleme întâmpinate și soluții:
   1. Identificarea potențialelor probleme și descrierea modului în care acestea au fost rezolvate.
   2. Sugestii pentru optimizarea performanței subrețelei.
8. Concluzii:
   1. Sumar al rezultatelor obținute în cadrul lucrării.
   2. Observații și concluzii generale privind proiectarea și implementarea subrețelei.
9. Referințe:
   1. Menționarea tuturor resurselor și documentației utilizate în procesul de proiectare și configurare a subrețelei.
10. Anexe:
    1. 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.

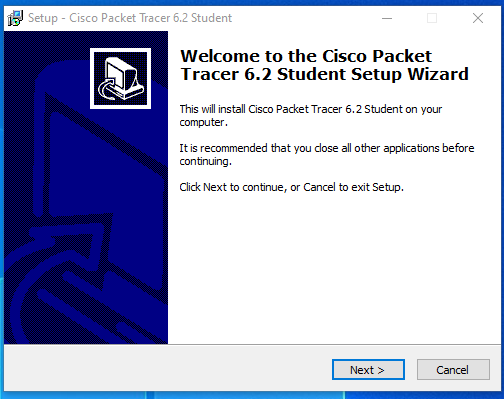
**ANEXĂ**

**Pregătirea pentru lucrările de laborator**

**Instalarea programului Cisco Packet Tracer 6.2**

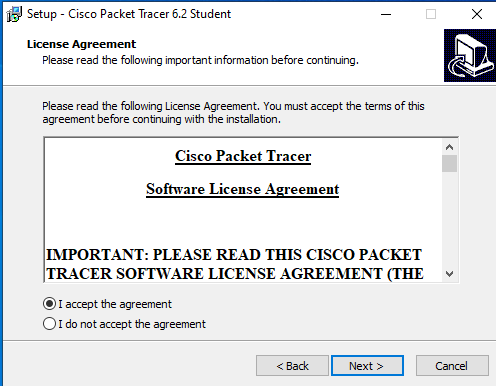
Instalarea programului în Windows este simplă. Trebuie găsit fișierul corespunzător (de exemplu, cu numele "Cisco Packet Tracer 6.2 for Windows Student Version.exe"). Este suficient să deschideți acest fișier pentru a porni asistentul de instalare, apoi să acceptați acordul de licență, să alegeți o locație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

* 1. 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.



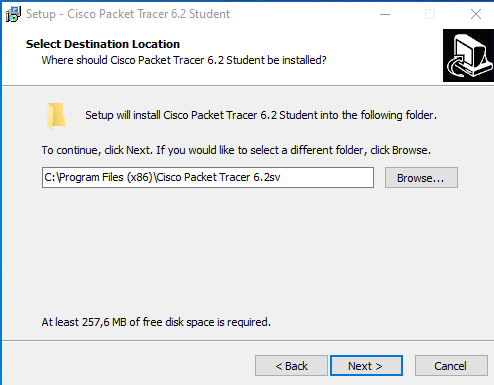
***Figura A1.1. Inițierea procesului de instalare a softului CISCO Packet Tracer***

* 1. Este necesară acceptarea condițiilor de licență pentru a continua procesul.



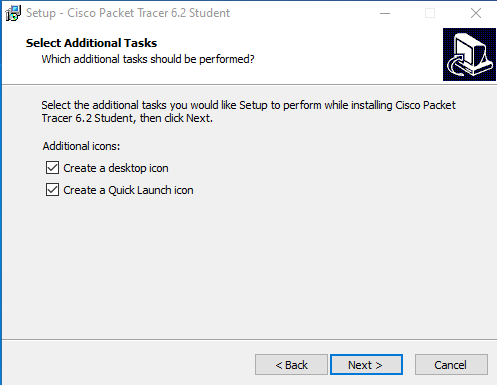
***Figura A1.2. Acceptarea condițiilor de licență***

* 1. Utilizatorului i se cere să aleagă folderul destinatar pentru instalarea programului.



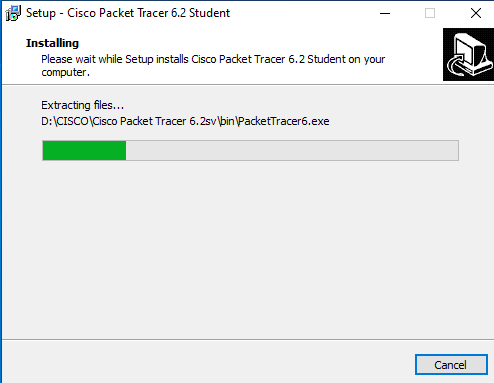
***Figura A1.3. Alegerea locației de instalare***

* 1. Utilizatorul trebuie să decidă asupra formării etichetei în procesul de instalare.



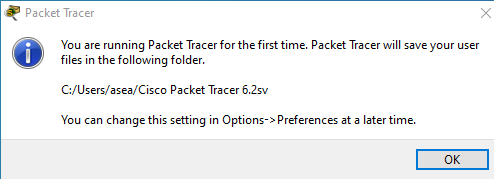
***Figura A1.4. Generarea etichetelor***

* 1. Facem clic pentru a începe instalarea programului.



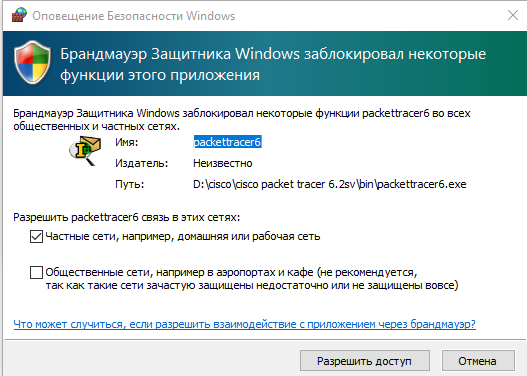
***Figura A1.5. Procesul de instalare***

* 1. Ultimul pas constă în alegerea folderului de destinație pentru stocarea fișierelor elaborate în Cisco.



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

* 1. În caz de necesitate, se acceptă utilizarea programului în cadrul sistemului de operare Windows.



***Figura A1.7. Acceptarea programului în sistemul de operare***

* 1. După finalizarea instalării programului, este finisată etapa de pregătire pentru îndeplinirea lucrărilor de laborator.