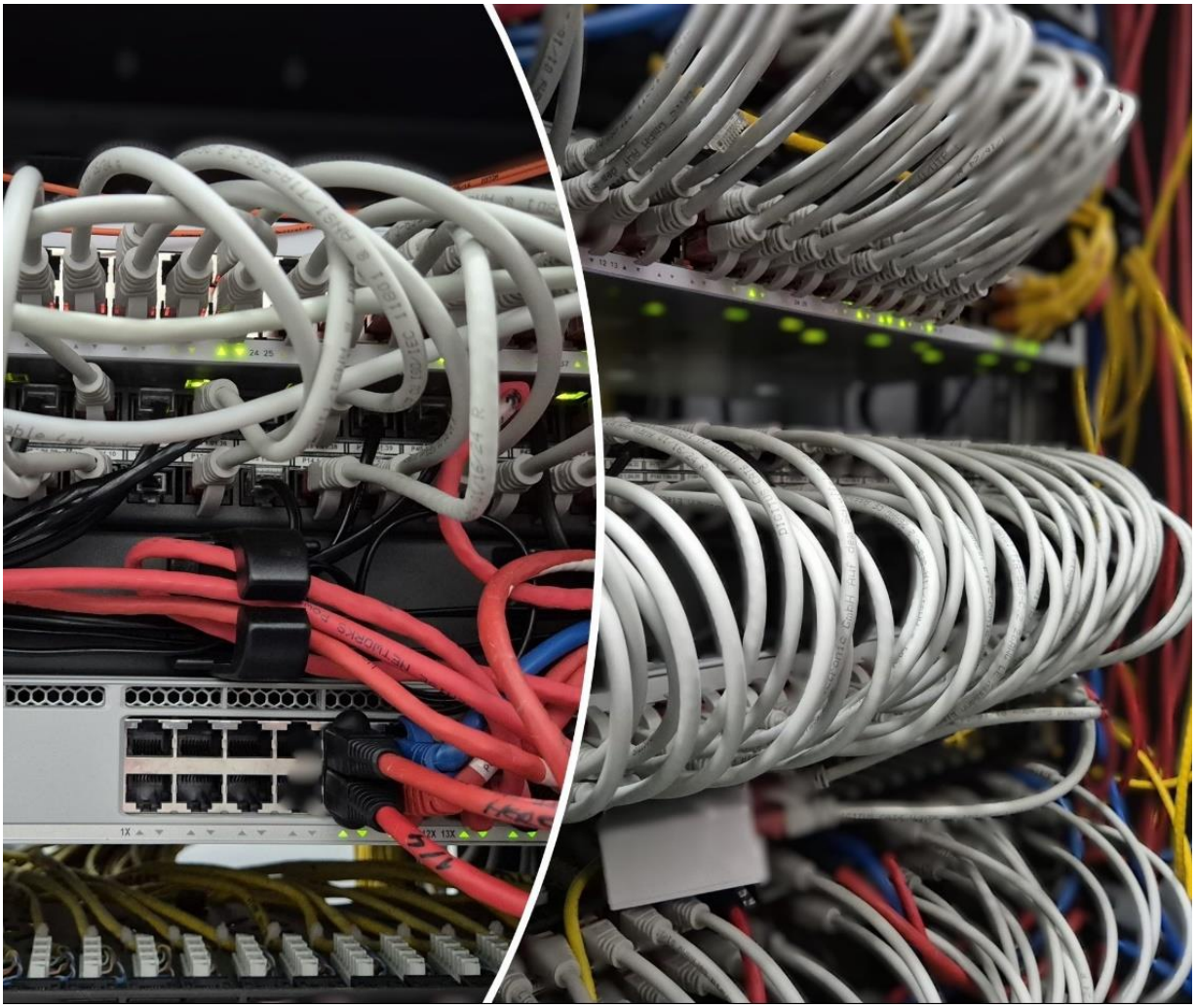
Adrian PECULEA, Bogdan IANCU, Sorin BUZURA, Vlad RAȚIU
Coordonatori: Vasile Teodor DĂDÂRLAT, Emil CEBUC

REȚELE DE CALCULATOARE

Activități practice



U.T.PRESS
Cluj-Napoca, 2024
ISBN 978-606-737-730-9

Adrian PECULEA, Bogdan IANCU, Sorin BUZURA, Vlad RAȚIU
Coordonatori: Vasile Teodor DĂDÂRLAT, Emil CEBUC

Rețele de Calculatoare

Activități practice

U.T.PRESS
Cluj - Napoca, 2024
ISBN 978-606-737-730-9

Editura U.T.PRESS
Str. Observatorului nr. 34
400775 Cluj-Napoca
Tel.: 0264-401.999
e-mail: utpress@biblio.utcluj.ro
http://biblioteca.utcluj.ro/editura

Recenzori: Prof.dr.ing. Ionuț Anghel
Conf.dr.ing. Lia-Anca Hangan

Pregătire format electronic on-line: Gabriela Groza

ISBN 978-606-737-730-9

Introducere

Proiectată ca un instrument operațional - suport pentru activități de (auto)instruire, cartea „Rețele de calculatoare. Activități practice” își propune să abordeze un spectru larg de probleme și abordări teoretice, însoțite de exemple reale și aplicații practice bazate pe partea teoretică.

Cartea se adresează în primul rând studenților din cadrul programelor de studii ale Facultății de Automatică și Calculatoare, care sunt la primul lor contact cu domeniul rețelelor de calculatoare. În același timp, problemele abordate în carte, conținutul teoretic și exercițiile practice pot servi drept invitație pentru toți cei interesați de studiul rețelelor de calculatoare utilizate în principal în sistemele moderne (profesori, cercetători, studenți din alte domenii de studiu, absolvenți, ingineri din diferite specializări etc.). Materialul de studiu oferă suport atât studenților în studiul individual sau de grup, orientându-i către auto-organizarea eficientă a propriei activități, cât și profesorilor în optimizarea proceselor de proiectare-organizare-evaluare, pentru a asigura calitatea formării universitare.

Obiectivul principal al cărții este de a furniza informații specifice și de a pregăti cititorul pentru înțelegerea, proiectarea și depanarea rețelelor de calculatoare. Această carte utilizează, într-un mod operațional, conținutul cursului „Rețele de calculatoare”, concentrându-se în principal pe crearea de oportunități de învățare, prin furnizarea de diverse sarcini didactice, exerciții, analize, reflecții, întrebări și comentarii.

Subiectele sunt concepute într-un mod activ și interactiv și includ elemente teoretice esențiale, abordări de clarificare și clasificare conceptuală, completate de aplicații și sarcini didactice. Structura cărții este graduală în complexitate. Sarcinile practice nu sunt atât un scop în sine, cât ocazii, mijloace de orientare către exercitarea abilităților și capacităților pe care studenții le vor folosi ulterior, ca indicator al profesionalizării lor în inginerie.

Prima parte prezintă principalele medii de transmisie cablate utilizate în rețelele de calculatoare moderne și uneltele și tehnicile necesare pentru analizarea și evaluarea funcționării corecte a rețelelor de calculatoare. Nivelul de rețea și protocoalele sale, împreună cu strategiile de rutare statică, sunt acoperite în a doua parte a cărții. Aspectele legate de programarea rețelelor, în principal software pentru aplicații socket și depanarea aplicațiilor de rețea, sunt introduse în partea a treia. Partea a patra a cărții prezintă aspecte legate de organizarea rețelelor locale și virtuale. Secțiunea finală a cărții se concentrează pe înțelegerea și analiza amenințărilor comune de securitate care apar în rețelele de calculatoare.

Sperăm că această carte va contribui la dezvoltarea modului specific de gândire în domeniul ingineriei, va extinde spiritul de lucru în echipă între studenți și va eficientiza comunicarea, contribuind la creșterea calității învățământului universitar.

Autorii,

Cluj-Napoca, 2024

Cuprins

CAPITOLUL 1: INTRODUCERE ÎN WIRESHARK ȘI PACKET TRACER

1. Obiective

Obiectivele acestui capitol cuprind trei aspecte:

- O scurtă continuare a introducerii teoretice în comunicații/rețele și stive de rețea
- Introducere în utilizarea utilitarului Wireshark
- Introducere în utilizarea emulatorului Cisco Packet Tracer

2. Considerații teoretice

Vă rugăm citiți următoarele înainte de a continua. Noțiunile prezentate în activitățile de laborator sunt destinate utilizării în moduri strict etice și legale. Orice altă utilizare a datelor derivate din informațiile prezentate de acum înainte poate fi supusă legislaţiei aferente, iar prin continuarea acestui laborator și folosirea informațiilor prezentate cititorii recunosc că Universitatea Tehnică din Cluj-Napoca și personalul implicat nu sunt în niciun fel răspunzători pentru nicio acțiune ilegală întreprinsă de entitățile care au acces la materialele prezentate în cadrul acestui laborator/curs. Vă rugăm să utilizați toate cunoștințele pe care urmează să le dobândiți în moduri etice și legale.

2.1 Comunicaţie/Reţelistica

Pentru a comunica cu succes, dispozitivele au nevoie de reguli. În general, dispozitivele se încadrează într-una dintre următoarele două categorii: dispozitive endpoint și dispozitive de rețea. Dispozitivele endpoint reprezintă entitățile care comunică, în timp ce dispozitivele de rețea reprezintă dispozitivele de infrastructură necesare pentru comunicaţie (de exemplu, case și servicii poștale; locații fizice și drumuri, semne și reglementări rutiere) .

2.2 Stive de rețea

Stivele de rețea sunt un concept esențial pentru crearea de rețele. Vă rugăm să luați în considerare termenii importanți și diferențele dintre ei. Un model de stivă reprezintă o separare a funcțiilor (care sunt supuse reglementărilor și directivelor IEEE). O stivă specifică reprezintă combinația exactă de protocoale implementate la fiecare nivel și configurația lor specifică (de exemplu: un mic dejun ar putea fi analog laptelui cu cereale ca model de stivă, dar ca o stivă ar putea fi lapte ecologic 3,5% grăsime și cereale de hrișcă). Pe parcursul acestui laborator vom lucra în principal cu modelul de stivă TCP/IP (Figura 1.1), datorită faptului că Internetul a fost proiectat bazat pe modelul TCP/IP, înainte ca modelul OSI, mai rafinat, să fie adoptat. Notă: există multe eforturi de migrare a Internetului către modelul OSI și există multe alte rețele diferite care utilizează modelul OSI (de exemplu, rețele industriale sau rețele IoT).

Notă importantă: Mesajele sunt denumite după cum urmează:

- PHY – biți/simboluri („bits/symbols”)
- DLL – cadre („frames”)
- Internet – pachete („packets”)

Pe parcursul acestui laborator vom investiga doar mediile cu fir („wired media”), deși unele aspecte ale mediilor fără fir („wireless media”) vor fi prezentate pe scurt în viitor.

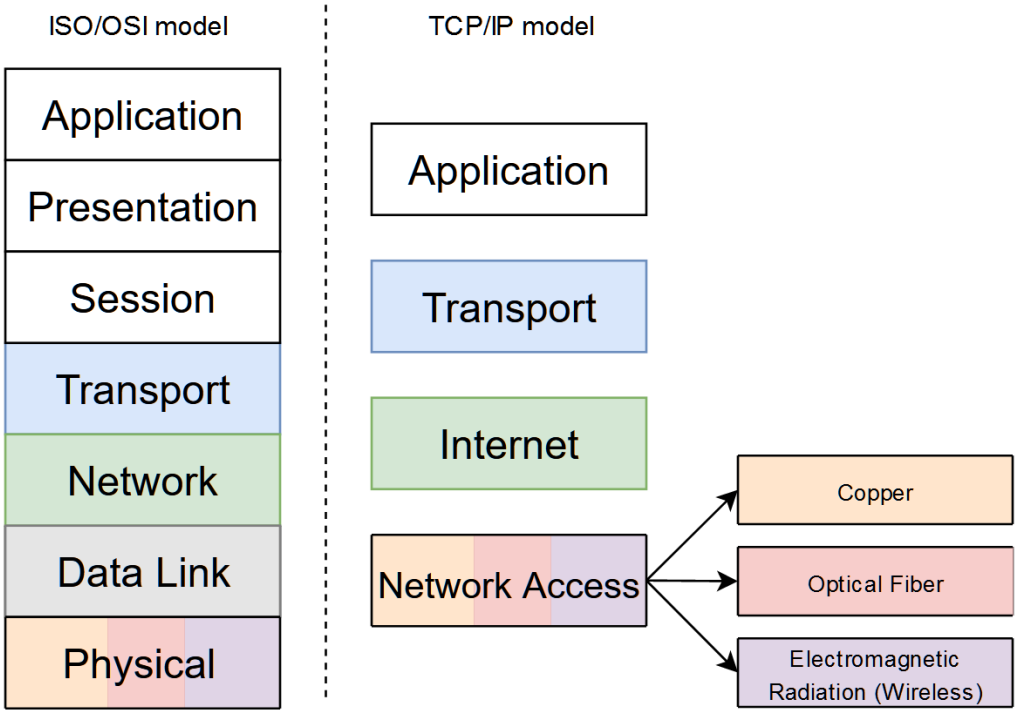


Figura 1.1 *Modelul de stivă TCP/IP*

3. Desfășurarea lucrării practice

3.1 Instalarea și verificarea funcționalității Wireshark

Wireshark este un analizor de pachete (uneori denumit "sniffer"). Pentru a capta traficul de rețea, Wireshark are nevoie de o interfață specifică pe care să capteze traficul. Vă rugăm să rețineți că, deși exercițiile din această secțiune constau în investigarea traficului local, Wireshark poate fi utilizat pentru a identifica trafic care nu este generat local și nici destinat gazdei („host”) locale, în funcție de interfața utilizată sau log-urile capturate cu ajutorul altor instrumente. Dacă lucrați pe propria stație de lucru, navigați la www.wireshark.org și instalați Wireshark.

Veți investiga pachetele capturate cu ajutorul Wireshark, în special corelând datele cu nivelul de stivă TCP/IP corespunzător. Nu trebuie să înțelegeți semnificația acestor date acum, dar este necesar să înțelegeți că un pachet conține date care sunt întotdeauna corelate cu unul dintre nivelele stivei – identificarea straturilor va fi extrem de utilă în viitoarea carieră de inginer (și necesară pentru acest curs / laborator).

Pentru a lansa prima captură Wireshark, deschideți Wireshark și selectați interfața corespunzătoare. Aceasta este probabil conexiunea LAN sau, așa cum se vede în Figura 1.2, conexiunea wireless (notă: Wireshark poate, de asemenea, să capteze Bluetooth și interfețe USB, printre altele, care depășesc obiectivele acestui curs/laborator).

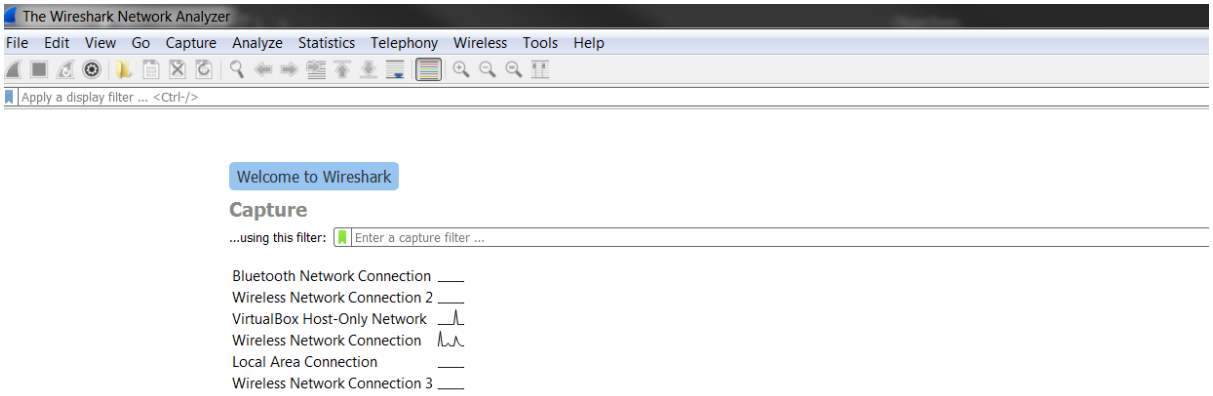


Figura 1.2 *Interfețe Wireshark*

Puteți fie să faceți dublu clic pe interfața dorită, fie să navigați la Capture -> Options -> Start, așa cum se vede în Figura 1.3.

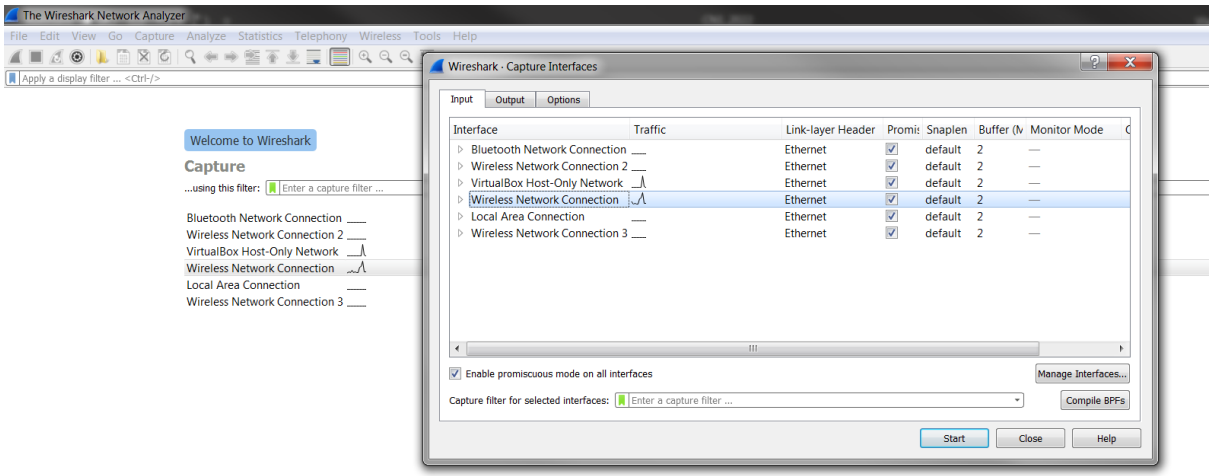


Figura 1.3 *Selectați interfețele Wireshark*

Ar trebui să începeți să vedeți pachetele capturate (Figura 1.4). Odată ce consideraţi că ați capturat suficiente pachete, opriți captura de la butonul indicat (sau nu, dar memoria locală nu va fi fericită).

Veți observa, probabil, foarte multe pachete, nu ezitați să le analizaţi, dar concentrați-vă pe a doua fereastră (Figura 1.5), care asociază datele capturate cu fiecare nivel din stiva TCP/IP. Este extrem de important să puteți asocia datele din această fereastră cu fiecare nivel individual. Primele patru nivele ale stivei de rețea sunt prezentate în această fereastră după cum urmează, de sus în jos: Fizic („Physical”), Legătură de Date („DLL”), Internet, Transport. Observați că fiecare strat prezintă protocolul specific.

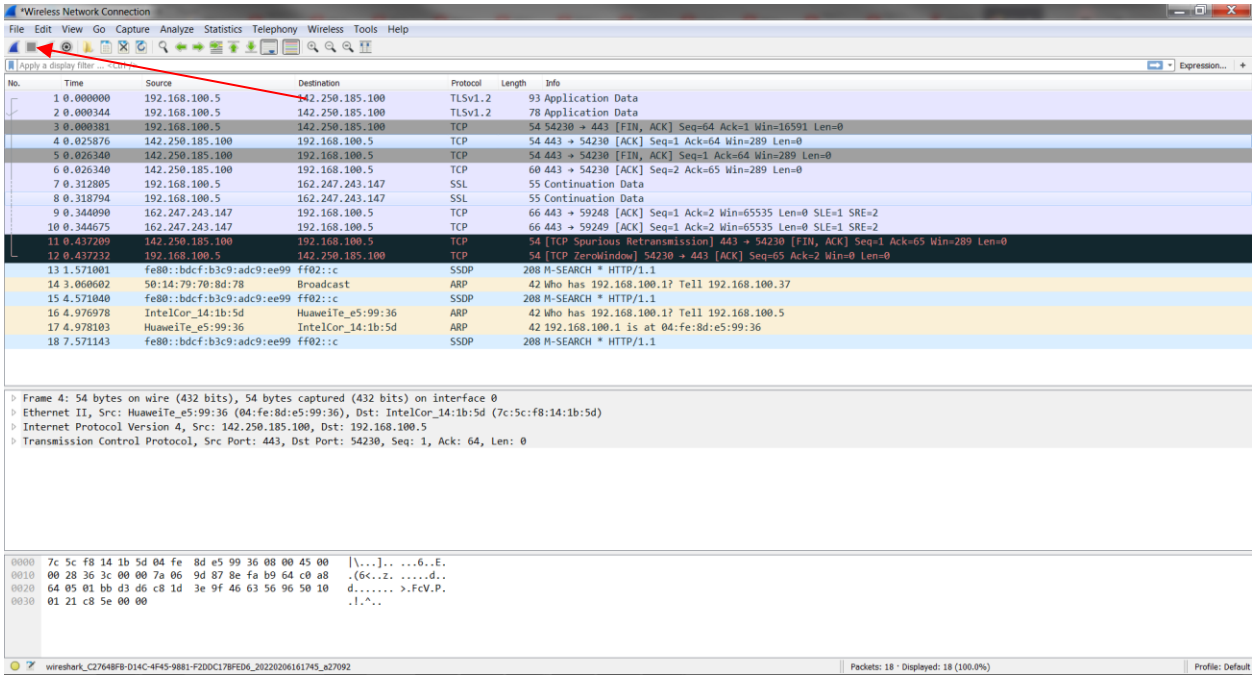


Figura 1.4 *Analiza pachetelor Wireshark*

```
▷ Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▷ Ethernet II, Src: IntelCor_14:1b:5d (7c:5c:f8:14:1b:5d), Dst: HuaweiTe_e5:99:36 (04:fe:8d:e5:99:36)
▷ Internet Protocol Version 4, Src: 192.168.100.5, Dst: 40.101.55.130
▷ Transmission Control Protocol, Src Port: 57631, Dst Port: 443, Seq: 1, Ack: 86, Len: 0
```

Figura 1.5 *Conținutul individual al pachetelor*

Puteți vizualiza conținutul detaliat al fiecărui pachet făcând clic pe săgeata de lângă fiecare nivel, așa cum se vede în Figura 1.6.

```
◢ Transmission Control Protocol, Src Port: 60853, Dst Port: 80, Seq: 1, Ack: 1, Len: 653
    Source Port: 60853
    Destination Port: 80
    [Stream index: 4]
    [TCP Segment Len: 653]
    Sequence number: 1    (relative sequence number)
```

Figura 1.6 *Conținut detaliat*

Puteți continua și captura cât de multe pachete doriți. Butonul de acces rapid "Start capturing packets" se află lângă butonul "Stop capturing packets". Puteți utiliza acest buton pentru a începe capturarea pachetelor fără a schimba interfața. Ori de câte ori închideți Wireshark sau începeți o nouă captură după ce ați rulat una anterioară, Wireshark vă va întreba dacă doriți să salvați datele capturate undeva. Salvarea datelor pentru analiza ulterioară este utilă în investigarea criminalistică a activităților din rețea (inclusiv a atacurilor), dar, punctul de vedere ale acestui laborator, nu trebuie să salvați aceste date nicăieri (cu excepția cazului în care observați ceva interesant și doriți să verificați mai târziu).

În continuare sunt două provocări tehnice.

- Provocarea 1: încercați să faceți ping către unele adrese IP, folosind comanda "ping ip_address" de pe consola (cmd) a stației de lucru. Ping este un instrument de testare a conectivității în rețea. Echivalentul în rețelistică la "Hello World" este efectuarea unui ping către proriul sistem ("ping 127.0.01" sau "ping localhost"). Acesta este folosit

pentru a testa funcționalitatea interfeței de rețea (de exemplu, dacă nu aveți hardware de rețea instalat pe stația de lucru, sau dacă este defect, ping-ul va eșua). Puteți vedea comanda ping pe o captură Wireshark? Este atomică sau compusă din mai multe mesaje?

- Provocarea 2: cu Wireshark capturând pachete pe interfața locală, încercați o autentificare („login") la un site HTTP, apoi la un site HTTPS (nu trebuie să aibă succes). În zilele noastre, majoritatea site-urilor web oferă servicii HTTPS și nu HTTP, dar puteți găsi în continuare unele site-uri HTTP căutând pe Internet pe un motor de căutare la alegere. Puteți vedea numele de utilizator/parola în conținutul pachetului la o încercare de autentificare HTTP? Dar la autentificarea HTTPS? (Sugestie: puteți vedea pachetele HTTPS?). Vă puteți explica constatările? Ce nivel din stiva TCP/IP este responsabil cu implementarea HTTP și HTTPS? (Sugestie: încercați să vă dați seama fără ajutor, dar căutați dacă este necesar). Pentru a face această provocare mai ușoară, Wireshark oferă un mecanism de filtrare a pachetelor pe care îl puteți utiliza fie în timpul capturării, fie ulterior. Vom investiga detaliile mai târziu în timpul semestrului. Deocamdată, pentru a filtra pachetele fie introduceţi „string"-ul corespunzător filtrului dorit, fie selectaţi mai multe opţiuni de la butonul indicat (Figura 1.7) şi selectați „Apply this filter string to the display" (Figura 1.8). Faceţi clic pe butonul „X" adiacent pentru a reseta filtrul.

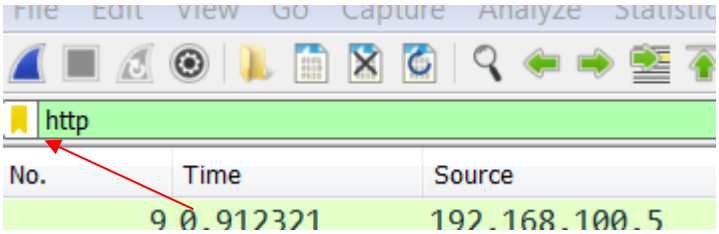


Figura 1.7 *Filtru Wireshark*

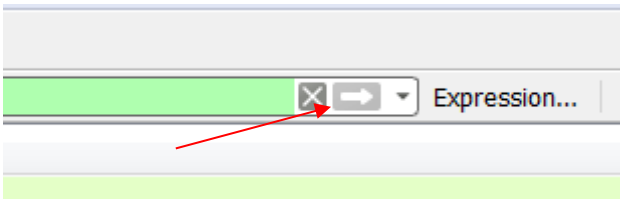


Figura 1.8 *Aplicarea filtrului*

3.2 Instalarea și verificarea Cisco Packet Tracer

Packet Tracer (PT) este un instrument de simulare a rețelelor furnizat de Cisco Systems. Este extrem de util în proiectarea rețelelor fără/înainte de accesul la echipamente fizice.

Vă rugăm să descărcați și să deschideți fișierul Intro.pkt furnizat. Ar trebui să vă conectați la PT cu contul Netacad/Skillsforall. Dacă nu aveți deja un cont de la descărcarea PT, vă rugăm să vă creați unul. Fișierul conține o rețea configurată anterior. Pe parcursul semestrului veți dobândi abilități care vă vor permite să configurați și să depanați o rețea similară. Notă: PT oferă funcționalități de simulare atât pentru rețelele cu fir, cât și pentru cele fără fir; pe parcursul acestui laborator vă veți concentra pe rețelele cu fir.

Investigaţi PT. Cele două categorii principale de dispozitive pe care le veți utiliza sunt dispozitivele de rețea (care furnizează infrastructură de rețea) și dispozitivele gazde/endpoint (care, în general, sunt calculatoare, servere, etc.). Încercați să adăugați un PC în rețea (Figura

1.9) fie făcând clic pe PC, apoi pe zona de lucru, fie făcând „drag and drop” cu PC-ul. Puteți șterge un dispozitiv din zona de lucru selectând Delete, apoi făcând clic pe dispozitiv, sau efectuând o selecție de unul sau mai multe dispozitive și făcând apsând pe tasta Delete.

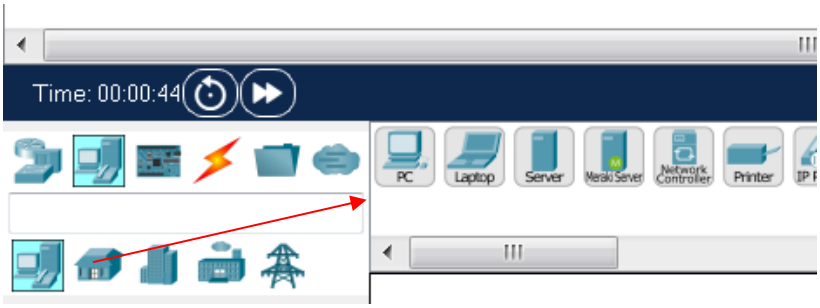


Figura 1.9 *Adăugați PC-ul*

Conectați PC-ul la switch, utilizând o conexiune automată (Figura 1.10).

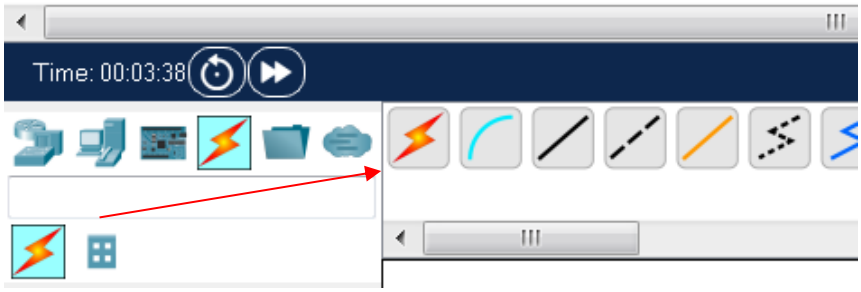


Figura 1.10 *Conectați PC-ul pentru a comuta*

Selectați opțiunea de conectare automată, faceți clic pe PC și în cele din urmă pe switch. Nu vă concentrați prea mult acum asupra înțelegerii a ceea ce se întâmplă, veți intra în mai multe detalii în activitățile viitoare.

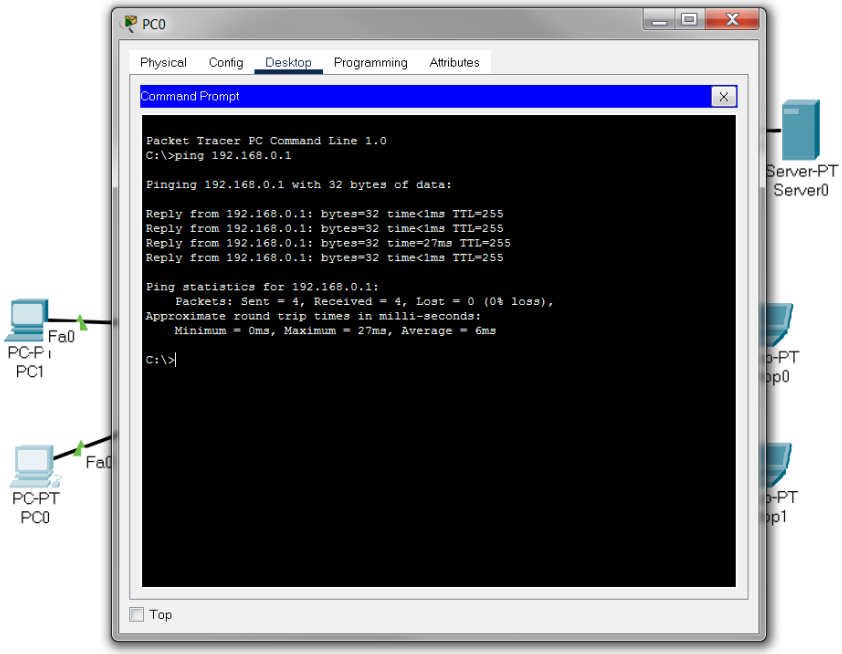


Figura 1.11 *Ping în PT*

Pentru a testa conectivitatea, puteți accesa orice PC făcând clic pe acesta; selectați Desktop -> Command prompt efectuaţi un ping către o adresă IP în rețea. Puteți vizualiza aceste adrese IP fixând cursorul deasupra oricărui dispozitiv. Ar trebui să vedeți ceva similar activității anterioare (Figura 1.11). Încercați să faceţi ping de pe PC-ul nou adăugat. Funcţionează? Vă puteți da seama de ce? (Sugestie: încercați să comparați configurațiile PC-ului cu PC-urile existente anterior). Vom analiza aceste aspecte în detaliu în cadrul viitoarelor laboratoare.

PT poate rula în timp real şi in modul simulat (Figura 1.12). Încercați să comutați la modul simulat. Rulați o comandă ping și apăsați butonul de redare. Puteți modifica viteza de simulare din bara de dedesubtul acestui buton. Ar trebui să puteți vedea pachete care se deplasează prin rețea. Regulile exacte și natura schimbului de mesaje vor fi prezentate în activitățile viitoare.

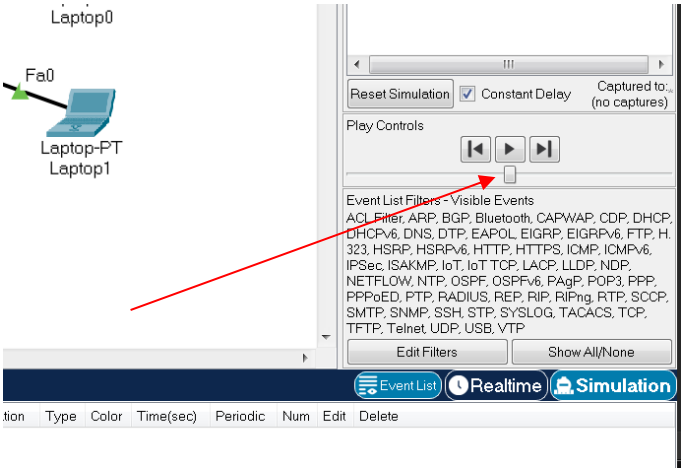


Figura 1.12 *PT în timp real și selectarea modului simulat*

PT are multe funcționalități pe care puteţi să le explorați. Funcționalitățile mai detaliate vor fi prezentate pe măsură ce treceți la activitățile viitoare.

3.3 Întrebări

- Ce este un model de stivă de rețea? Ce este o stivă de rețea?
- Ce este Wireshark și pentru ce se utilizează?
- Ce este Cisco Packet Tracer și pentru ce se utilizează?

CAPITOLUL 2: MEDII DE TRANSMISIE BAZATE PE CUPRU ŞI CABLAREA UTP

1. Obiective

Obiectivul acestui capitol este cunoașterea și înțelegerea mediilor de transmisie bazate pe cupru, ai principalilor parametrii asociați, precum și cablarea și testarea cablării UTP.

2. Considerații teoretice

Modelul de referință ISO Open Systems Interconnection (OSI) încorporează 7 niveluri (fizic, legătură de date, rețea, transport, sesiune, prezentare și aplicație). Primele trei niveluri definesc conceptele fizice/hardware ale unei rețele de comunicații. Celelalte patru niveluri definesc conceptele logice ale unei rețele de comunicații. Lucrarea actuală de laborator se concentrează pe nivelul fizic al stivei ISO/OSI, în principal medii de transmisie pe bază de cupru.

În Europa, familia de standarde ISO/IEC-11801 definește documentele generale și specifice de proiectare a cablajului. Acesta cuprinde ISO/IEC 11801-1:2017 Tehnologia informației — Cablare generică pentru sediul clienților — Partea 1: Cerințe generale și include ISO/IEC 11801-2, ISO/IEC 11801-3, ISO/IEC 11801-4, ISO/ IEC 11801-5, ISO/IEC 11801-6. ISO/IEC 11801-1 specifică cerințele pentru cabluri coaxiale (coax), cabluri torsadate (eng. twisted-pair) și fibre optice. In SUA și Canada este utilizat standardul ANSI/TIA-568-C (in locul ISO/IEC 11801).

2.1 Cabluri coaxiale și torsadate

În transmisia de date, mediul de transmisie reprezintă calea fizică între emițător și receptor; acesta trebuie să asigure performanțe superioare exprimate sub forma unor parametri cum ar fi: viteza de comunicare, rata de erori a transmisiei, costul, necesarul de amplificare.

Caracteristicile și calitatea unei transmisii de date sunt determinate atât de caracteristicile mediului suport pentru transmisie cât și de cele ale semnalului propagat. Standardul IEC 61935-1 este utilizat pentru „proceduri de măsurare de referință pentru parametrii de cablare și cerințele privind precizia testerului de teren pentru măsurarea parametrilor de cablare”.

În proiectarea sistemelor de transmisie de date elementele determinante pentru performanțele sistemului sunt:

- *lățimea de bandă* – reprezintă volumul de date transferate pe un canal de comunicație astfel încât, dacă ceilalți factori rămân constanți, cu cât lățimea de bandă este mai mare cu atât se va obține o rată de transmisie a semnalului mai bună;
- *interferența* – este generată de suprapuneri de semnale în aceeași bandă de frecvență, fapt ce poate genera distorsionarea semnalului. Ecranarea corectă a mediului de transmisie poate determina minimizarea efectelor de acest tip;

- *numărul de receptori* - presupune construirea de legături punct la punct sau partajate.

Parametri electrici principali ai mediilor de transmisie bazate pe cupru sunt:

- *impedanța* – pentru transmisiile de date interesează nu doar valoarea impedanței la o frecvență dată ci și variația ei în funcție de frecvență;
- *viteza de propagare* - reprezintă un procent din viteza luminii;
- *atenuarea (insertion loss)* – de acest parametru depinde comportarea la frecvențe înalte a canalului. Această valoare crește proporțional cu lungimea cablului.
- *diafonia* - este măsura influenței produse de un cablu asupra altui cablu aflat în vecinătate.

Cablul coaxial este mediul de transmisie versatil, utilizat într-o mare varietate de aplicații, de la transmisia telefonică pe distanțe lungi, rețele locale de calculatoare, până la distribuția TV pentru conectarea diverselor dispozitive. Acesta este un mediu ce permite operarea pe un spectru larg de frecvențe.

Cablul conține un miez de cupru izolat de al doilea conductor exterior, realizat sub forma unui ecran dintr-o țesătură de fire subțiri (Fig. 2.1). Principalele caracteristici ale cablului coaxial sunt:

- permite transmisie de semnale digitale și analogice;
- datorită modului de construcție concentrică, este rezistent la interferență magnetică.

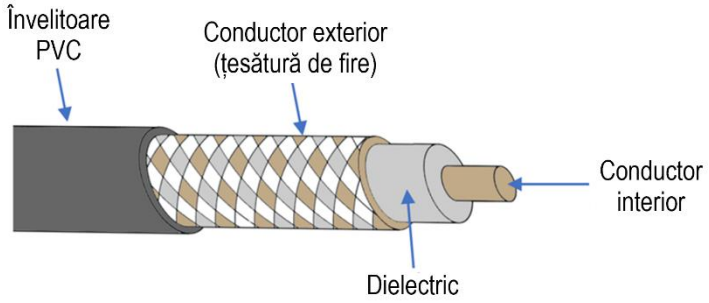


Figura 2.1 *Structura cablului coaxial*

Topologiile moderne de Internet folosesc fibra optică pentru a transporta date de la un ISP (Internet Service Provider) către comunitățile locale și, de acolo, folosesc cablu coaxial (disponibil de la CATV) pentru a conecta abonații. La capătul dinspre abonați, un modem de cablu acționează ca o punte între rețeaua coaxială și LAN-ul clientului. Pentru a obține transferuri de date cu lățime de bandă mare, specificațiile standard, cum ar fi Data Over Cable Service Interface Specification (DOCIS), sunt utilizate pentru rețelele hibride coaxial-fibră optică (HFC) (de exemplu, DOCSIS 3.1 specifică o viteză de descărcare a datelor de 10 Gbps și viteze în încarcare de până la 1 Gbps). De asemenea, sistemele moderne de distribuție utilizează acum și protocolul Ethernet Passive Optical Networks (EPON) peste medii coaxiale (EPoC) (IEEE Std 802.3bn) cu o specificație de nivel fizic pentru până la 10 Gb/s descărcare și până la 1,6 Gb/s încarcare pe o legătură la punct la multipunct. Alte aplicații, cum ar fi Ethernet 10Gb până la Ethernet 100 Gb pentru legături full-duplex punct-la-punct între dispozitivele de rețea, folosesc un cablu coaxial special cu doi conectori interiori denumit cablu Twinaxial sau Twinax.

Pentru rețelele LAN acest tip de cablu a fost înlocuit cu alte tehnologii cu lățime de bandă mare. Performanțele sale au fost atinse și depășite pe distanțe scurte de către cablu torsadat și pe distanțe mari de către fibra optică.

Constrângerile principale legate de performanțe se referă la atenuarea introdusă, zgomotele intermodulare și încălzirea sa.

Cablul coaxial folosit în rețele locale de calculatoare avea impedanța de 50 Ohmi si era de 2 tipuri:

- *cablul coaxial subțire* (RG58 în rețele IEEE 802.3 de tip **10BASE2**) este cel mai răspândit și utilizat pentru instalări de interior datorită unui raport preț/performanță bun;
- *cablul coaxial gros* (RG213 în rețele IEEE 802.3 tip **10BASE5**) este utilizat pentru instalări de exterior datorită rezistenței mecanice mai mari și limitei de lungime mai bune.

Conectarea calculatoarelor la cablul coaxial se realiza prin două metode: folosind joncțiuni T sau conectori speciali numiți *conector vampir* plasați în cadrul unui dispozitiv numit transceiver, care permit înfigerea lor în cablu fără a fi necesară tăierea acestuia. Conectorul străpunge stratul izolator realizând contactul direct cu stratul conductor. Conexiunea de la transceiver la placa de rețea se realizează printr-un cablu de transceiver care se conectează la portul AUI (Attachment Unit Interface). Pentru transmisia analogică pe distanțe mari sunt necesare amplificatoare de semnal, iar pentru semnalele digitale sunt necesare repetoare, standardele specificând exact distanța de amplasare a acestora. În cazul cablului coaxial subțire, distanța maximă este 185m iar in cazul cablului coaxial gros, distanța maximă este 500m. Pentru Twinax, modul de interfață de rețea SFP+ (SFP = small form-factor pluggable) se poate utiliza.

Cablul torsadat (*twisted pair - TP*) sau cablul cu perechi de fire de cupru răsucite, având un înveliș comun (cu sau fără ecranare), reprezintă tipul de cablu uzual folosit în rețele locale de calculatoare și telefonie. Răsucirea firelor are drept scop reducerea distorsiunilor magnetice, a interferențelor între perechile adiacente de cablu. Acest cablu acționează asemeni unei singure legături de comunicație. Pentru cablurile cu mai multe perechi de fire răsucite, pașii de răsucire trebuie să fie diferiți pentru fiecare pereche astfel încât diafonia între perechi să fie minimă. Datorită progreselor realizate în tehnologia de realizare a cablurilor TP, acestea pot fi utilizate într-o gamă foarte largă de frecvențe permițand transmisii de date ordinul Gbps, iar în rețele Gigabit oferind pe distanțe scurte performanțe comparabile cu fibra optică. Cablul TP reprezintă mediul de transmisie pentru semnale analogice și digitale utilizat de obicei în telefonie și rețele locale de calculatoare.

Cablurile TP utilizate în rețelele de calculatoare au patru perechi de fire răsucite, permit o distanță maximă de 100 m și sunt utilizate în rețelele de 10, 100, 1000 Mbps și 1, 2,5, 5 sau 10 Gbps. Impedanța standard a cablului este de 100 Ω. Mai mult, rețelele de 25 și 40 Gbps permit o distanță maximă de 30 m folosind cabluri de clasă I și II (cat. 8.1 și 8.2).

Există diametre diferite pentru cablurile de cupru și sunt măsurate în standardul AWG (American Wire Gauge): de la 22 AWG la 26 AWG și, pentru distanțe scurte 28 AWG.

Convenția de denumire a cablurilor din ISO/IEC 11801 prezintă diferitele tipuri de construcție a cablurilor, pe baza ecranării lor: XX / XXX. Exemple de denumire a cablurilor sunt: U/UTP, U/FTP, F/UTP, S/UTP, SF/UTP, F/FTP, S/FTP, SF/FTP etc.

Tabel 2.1 *Denumirea cablurilor (XX / XXX)*

XX			**/**	**X**		**XX**
overall screen				element screen		balanced element
F = foil screen	S = braid screen	SF =braid and foil screen		U = unscreened	F = foil screened	TP

In figura 2.2, sunt exemplifcate cablurile F/UTP and U/FTP.

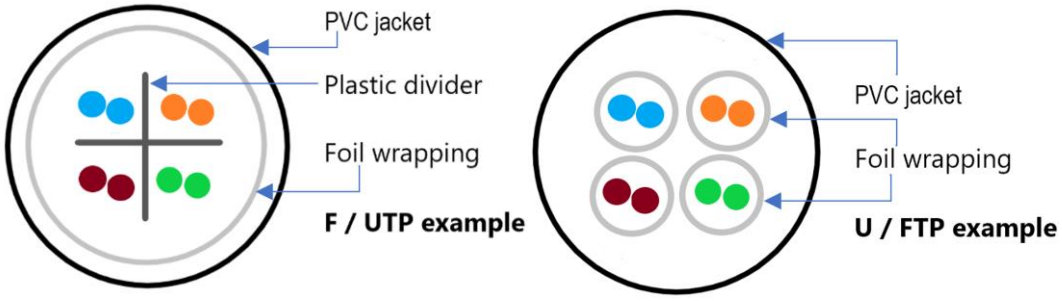


Figure 2.2 *F/UTP și U/FTP*

Categoriile de cabluri torsadate utilizate în transmisiile de date sunt diferențiate în funcție de utilizările suportate. Tabelul 2.2 prezintă specificațiile clasei TP echilibrate (simetrice).

Tabel 2.2 *Specificațiile clasei TP echilibrate*

Clasa	**Lățimea de bandă**	**Categoria**
Clasa A	până la 100 kHz	Categoria1
Clasa B	până la 1 MHz	Categoria2
Clasa C	până la 16 MHz	Categoria3
Clasa D	până la 100 MHz	Categoria5e
Clasa E	până la 250 MHz	Categoria6
Clasa EA	până la 500 MHz	Categoria6a
Clasa F	până la 600 MHz	Categoria7
Clasa FA	până la 1000 MHz	Categoria7a
Clasa I și Clasa II	până la 2000 MHz	Categoria8.1, 8.2

Toate aceste clasificări nu se referă doar la cabluri ci și la întreaga conectică asociată: mufe, prize, patch panel-uri etc. Cablul torsadat permite realizarea de legături punct la punct, realizând topologii diverse ale rețelei de tip stea sau stea extinsă.

2.2 Cablarea UTP

La cablarea UTP a retelelor Ethernet și Fast Ethernet perechea de fire 1-2 se folosește pentru transmisie, iar perechea 3-6 pentru recepție. Acest tip de dispunere a firelor se numește MDI (Media Dependent Interface) sau dispunere normală. În mod uzual firele se conectează după aceeași regulă la mufele din cele două capete ale cablului, caz în care cablul (patch-cord) se numeste *drept* sau *direct (eng. straight-through)*. Cablul direct a fost conceput pentru a fi utilizat la conectarea a două dispozitive de tip diferit (ex. computer – modem, router – switch etc.)

În unele cazuri speciale trebuie inversată recepția cu transmisia pentru a face posibilă comunicarea, caz în care cablul (patch-cord) se numește *inversor (eng. crossover)*. După cum este specificat de către IEEE 802.3, funcția de încrucișare conectează emițătoarele de la un capăt la receptorii de la celălalt capăt al segmentului de legătură. Cablul inversor a fost conceput pentru a fi utilizat la conectarea a două dispozitive de același tip (ex. computer – computer, router – router etc.). În interfețele moderne, funcția Automatic MDI/MDI-X detectează automat tipul de conexiune prin cablu necesar și configurează conexiunea corectă, astfel încât cablul direct poate fi utilizat în întreaga rețea.

Tabel 2.3 *EIA/TIA-T568-A*

Pin#	**Pereche#**	**Funcție**	**Culoare fir**	**Folosit în 10/100BASE-T**	**Folosit în 1000 BASE-T**
1	3	BI_DA+ (Transmission+)	White/Green	Yes	Yes
2	3	BI_DA- (Transmission-)	Green	Yes	Yes
3	2	BI_DB+ (Reception+)	White/Orange	Yes	Yes
4	1	BI_DC+	Blue	No	Yes
5	1	BI_DC-	White/Blue	No	Yes
6	2	BI_DB- (Reception-)	Orange	Yes	Yes
7	4	BI_DD+	White/Brown	No	Yes
8	4	BI_DD-	Brown	No	Yes

Tabel 2.4 *EIA/TIA-T568-B*

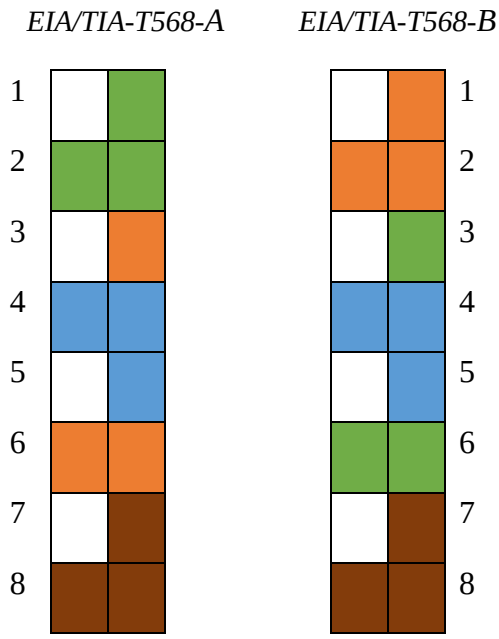
Pin#	**Pereche#**	**Funcție**	**Culoare fir**	**Folosit în 10/100BASE-T**	**Folosit în 1000 BASE-T**
1	2	BI_DA+ (Transmission+)	White/Orange	Yes	Yes
2	2	BI_DA- (Transmission-)	Orange	Yes	Yes
3	3	BI_DB+ (Reception+)	White/Green	Yes	Yes
4	1	BI_DC+	Blue	No	Yes
5	1	BI_DC-	White/Blue	No	Yes
6	3	BI_DB- (Reception-)	Green	Yes	Yes
7	4	BI_DD+	White/Brown	No	Yes
8	4	BI_DD-	Brown	No	Yes

La cablarea UTP a rețelelor Gigabit Ethernet toate patru perechile de fire se folosesc atât pentru transmisie cât și pentru recepție. Cablurile UTP conțin patru perechi de fire torsadate fiecare pereche identificându-se printr-o culoare: albastru, oranj, verde și maro. Fiecare pereche conține un fir colorat și un fir alb combinat cu culoarea respectivă. Mufele folosite pentru acest cablu sunt mufe tată de tip RJ-45 (mufă 8P8C) conținând 8 pini corespunzători celor 8 fire.

Privit din față, pinii sunt numerotați de la 1 în dreapta la 8 în stânga. Modul de conectare a firelor la pini determină tipul cablului. Exista două standarde de conectare a firelor la mufa RJ-45: EIA/TIA-T568-A și EIA/TIA-T568-B. Aceste conectări sunt prezentate în tabelul 2.3 și 2.4 (BI_DX înseamnă Pereche Bidirecțională *X*).

Așadar, pentru a obține un cablu drept sau direct ambele capete ale cablului trebuie mufate după același standard (A-A sau B-B) și pentru a obține un cablu inversor fiecare capăt al cablului trebuie mufat după câte un standard (A-B sau B-A).

Tabel 2.5 a. *Examplu codare culori* *b. Conector RJ-45*



La cablarea UTP se folosesc atât dispozitive pasive cât și dispozitive active. Dispozitivele pasive nu sunt alimentate de la o sursă de tensiune în vreme ce dispozitivele active necesită alimentare. Cele mai importante dispozitive pasive sunt: mufă RJ-45, priza și patch panel-ul. La nivel 1, cele mai important dispozitiv active este transceiver-ul. O mufă RJ-45 este un dispozitiv cu opt pini in care se conecteaza cablul TP. Mufele se inserează în prize și în patch panel-uri. În prize se conectează calculatoarele cu ajutorul patch cord-urilor. Prizele sunt legate la patch panel, care se află în dulapul de distribuție. Cu ajutorul unui patch cord se conectează patch panel-ul la switch care se afla localizat tot in dulapul de distribuție. Switc-ul este un bridge multiport. Transceiver-ul este un dispozitiv bidirecțional care receptionează semnalele de la un tip de interfață, le convertește în semnale specifice altui tip de interfață și le transmite unei interfețe de acel tip.

Pe baza standardului IEC 61935-1, se efectuează teste pentru măsurarea parametrilor de cablare: pierdere de inserție, întârziere de propagare și variație a întârzierii, diafonie la capătul apropiat (NEXT) și suma de putere NEXT, diafonia la capătul îndepărtat (FEXT) și suma de putere FEXT, diferite atenuări și diafonii (eng.: insertion loss, propagation delay and delay skew, near-end cross-talk (NEXT) and power sum NEXT, far-end cross-talk (FEXT) and power sum FEXT, different attenuation and crosstalk types).

Pentru cablarea unui cablu TP și a unei prize TP, ar trebui utilizate mai multe instrumente, așa cum se arată în tabelul 2.6: unealtă de dezipare/tăiere a cablurilor (a.), unealtă de sertizare a cablurilor (b.), unealtă de perforare (eng. punch down) (c.) și testere de cabluri (d., e.).

Tabel 2.6 *Unelte pentru cablare și testare*

				
a	b.	c.	d.	e.

Pe piață se găsesc atât cabluri torsadate plate, cât și rotunde (Fig. 2.3). Ele servesc aceluiași scop, dar pot fi folosite în scenarii diferite. Cablurile rotunde sunt cablurile cel mai des folosite în rețele, totuși cablurile plate ar putea fi utile pentru a fi rulate sub un covor, de-a lungul unui perete sau a unui colț.

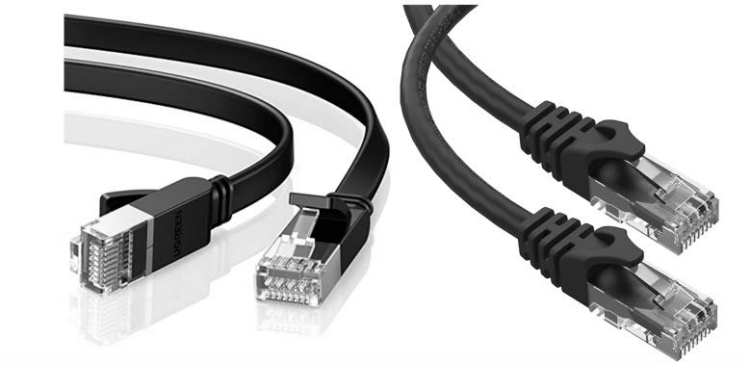


Figure 2.3 *Cablu plat cat.6 (stânga) și cablu rotund cat.6 (dreapta)*

3. Desfăşurarea lucrării practice

3.1 Mufarea și testarea cablurilor UTP

- Identificați interfață de rețea (NIC - network interface card) cablată a computerul din laborator.
- Identificați cablurile folosite în laborator (PC – priză). Ce standard a fost folosit pentru cablarea acestora?
- Folosind standardul EIA/TIA-T568-A sau B, vor fi realizate și testate cabluri drepte.

- Folosind standardele EIA/TIA-T568-A și B, se vor realiza și se vor testa cabluri încrucișate.
- Folosind instrumentul punch down, mufați o priză de perete.
- Cercetați online diferitele tipuri de cablu discutate în lucrarea de laborator.

3.2 Cablarea și testarea rețelelor

- Folosindu-se un cablu inversor se va testa conectivitatea dintre două calculatoare.
- Cablați și testați conectivitatea rețelei prezentată în figura 3.1.

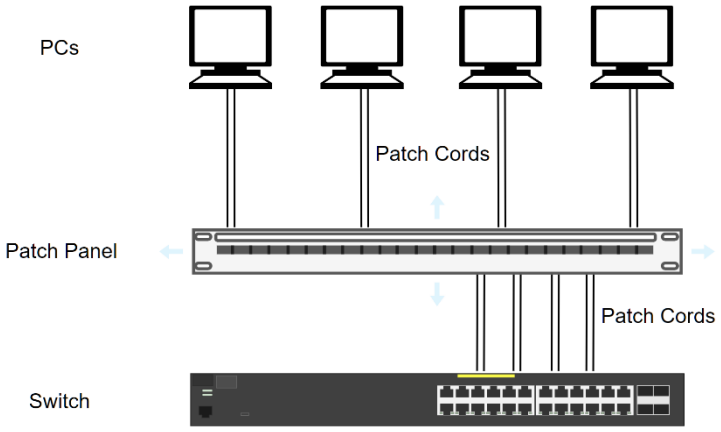


Figure 3.1 *Rețea de testare a cablurilor*

3.3 Întrebări de reflecție

- De ce este importantă ecranarea în alegerea cablului de rețea adecvat?
- De ce cablurile TP utilizate în rețelele de calculatoare sunt limitate la o distanță maximă de 100 m?
- Ce tip/categorie de cablu ar trebui utilizat pentru o nouă rețea LAN?

CAPITOLUL 3: FIBRE OPTICE ŞI COMPONENTE OPTICE

1. Obiective

Obiectivul acestui capitol este cunoașterea și înțelegerea fibrelor optice, a componentelor optice, principalele metodelor de testare, precum şi calculul bugetului optic.

2. Consideraţii teoretice

2.1 Fibre şi componente optice

Capitolul continuă să se concentreze asupra nivelului fizic al stivei ISO/OSI, oferind cunoștințe despre fibrele optice și componente optice. În plus, în partea 3b sunt prezentate principalele dispozitive de rețea și elementele cablării structurate.

Odată cu scăderea accentuată a preţului **fibrei optice**, şi a echipamentelor de comunicaţie corespunzătoare, aceasta a devenit mediul preferat pentru noile conexiuni de mare viteza (în mediul exterior, cât şi în interiorul clădirilor).

Pentru transmiterea datelor, fibrele optice trimit semnale luminoase de-a lungul miezurilor de sticlă sau plastic (de ordinul zecilor de microni (μ), care constituie un ghid de undă pentru lumină, obținut dintr-o combinație de dioxid de siliciu și alte elemente).

Un fir de fibră optică (eng. *fiber strand*) este elementul de bază al unui cablu de fibră optică (un cablu conține mai multe fire). Un fir optic este format din trei straturi: miez, îmbrăcăminte și învelitoare de protecție. Un cablu de fibră optică este format din mai multe componente: fire de fibră, zona tampon/buffer, materiale de protecție și mantaua exterioară.

Miezul este învelit de un material realizat din dioxid de siliciu având un indice de refracţie mai mic decât al miezului numit imbrăcăminte. Pentru a proteja îmbrăcămintea, aceasta este învelită într-un material plastic. Acest inveliş se numeşte protecţie şi este învelit la rândul său de un material întăritor, de obicei Kevlar, care conferă rezistenţă fibrei în momentul instalării. Zonele tampoan ale fibrelor optice sunt de două categorii: strânse (se aplică o acoperire de protecție peste învelișul fiecărui fir de fibră) sau cu tub liber (mai multe fire în interiorul unui tub umplut cu un gel protector). Ultimul inveliş este mantaua care protejează fibra împotriva materialelor abrazive, a solventilor şi a altor factori. Culoarea mantalei în cazul fibrei optice multimod este de obicei portocaliu şi în cazul fibrei optice monomod este de obicei galben. Fiecare cablu de fibră optică este compus din doua fibre invelite separat, o fibră fiind folosită pentru transmisie şi alta pentru recepţie, asigurându-se în acest mod o legatură full-duplex. Un cablu de fibră optică poate contine de la 2 până la sute de fibre separate, învelite într-un strat protector.

Figura 3.1 prezintă o straturile unei fibre și o secţiune transversală prin fibra optică.

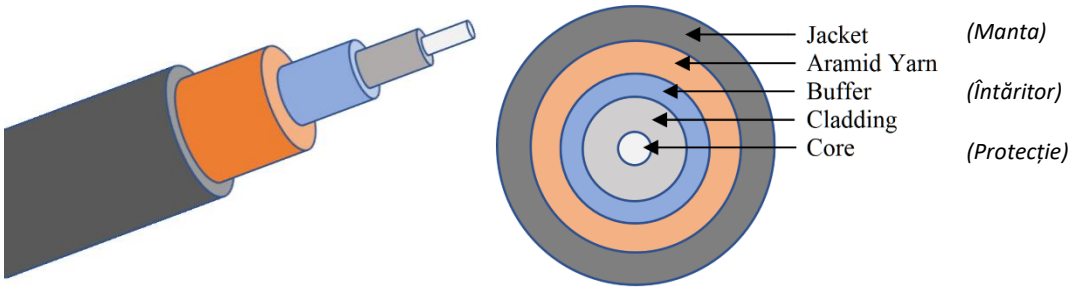


Figure 3.1 a. *Straturile unei fibre optice* b. *Secţiune transversală prin fibra optică*

Pentru ca semnalul luminos să fie reflectat fără pierderi trebuiesc îndeplinite următoarele două condiţii:

- fibra optică trebuie să aibă un indice de refracţie mai mare decât materialul care o înconjoară;
- unghiul de incidenţă al semnalului luminos trebuie să fie mai mare decât unghiul critic al fibrei şi al materialului care o inconjoară. Unghiul de incidenta al semnalului luminos poate fi controlat cu ajutorul următorilor doi factori:
    - apertura numerică a fibrei este gama unghiurilor semnalului luminos pentru care reflexia este totală;
    - modurile reprezintă căile pe care semnalul luminos le poate urma.

Spre deosebire de mediile de transmisie bazate de cupru, fibra optică nu este susceptibilă la și nu generează interferențe electromagnetice sau probleme de diafonie.

Două tipuri principale de fibre optice sunt utilizate în mod obișnuit în rețele LAN și WAN: *monomod* (eng. *single-mode*) și *multimod* (eng. *multimode*). Fibra optică monomod este utilizată pentru conexiuni pe distanțe lungi și pentru cablarea verticală în clădiri (coloana vertebrală a clădirii). Fibra optică multimod este utilizată în cablarea orizontală și verticală. Fibra multimod are un diametru miezului mai mare în comparație cu cel al fibrei monomod. Astfel, fibra multimod nu necesită aceeași precizie ca în cazul fibrei monomod, rezultând astfel elemente optice (conectori, transmițători etc) mai puțin costisitoare.

Miezul fibrei **monomod** are diametrul suficient de mic încât să permită doar un singur mod (o singură cale) semnalului luminos, acesta fiind transmis în linie dreaptă prin mijlocul miezului. Cablurile de fibră optică monomod folosesc miezul cu diametrul între 8µ şi 10µ. Cele mai folosite fibre optice monomod au diametrul de 9µ şi îmbrăcămintea cu diametrul de 125µ. Acestea sunt de obicei referite ca şi fibre optice de 9/125µ. Sursa de lumină folosită la fibra monomod este laserul infraroşu. Se recomandă precauţie atunci când se foloseşte laserul ca şi sursă de lumină deoarece acesta poate afecta ochii. Fibra monomod poate transmite date la distanţe de peste 100km. Pierderea pe km de fibră optică monomod este specificată de către producator. În cazul fibrei monomod indicele de refracţie al sticlei este constant. Acest tip de sticlă se numeşte sticlă cu index pas.

Miezul fibrei **multimod** are diametrul suficient de mare încât să permită mai multe moduri (mai multe căi) semnalului luminos. Cablurile de fibră optică multimod standard folosesc miezul cu diametrul de 62,5µ sau 50µ şi îmbrăcămintea cu diametrul de 125µ. Acestea sunt de obicei referite ca şi fibre optice de 62.5/125µ sau 50/125µ. De obicei, sursele de lumina folosite

cu fibra multimod sunt Infrared Light Emitting Diode (LED) sau Vertical Cavity Surface Emitting Lasers (VCSEL). LED-urile sunt mai ieftine şi necesită mai puţine măsuri de siguranţă decât laserele. Dezavantajul LED-urilor este că nu pot transmite semnalele luminoase la distante la fel de mari ca şi laserele. Fibra multimod de 62.5/125 poate transmite date la distante de până la 2000m. În cazul fibrei multimod indicele de refracţie al sticlei poate fi constant (sticlă monomod cu index pas) sau poate scădea de la centru spre exterior (sticlă monomod cu index variabil sau gradat şi permite diferitelor moduri luminoase să ajunga la receptor în acelaşi moment).

În fibra optică lumina suferă, pe lângă propagare, două fenomene principale: atenuare şi dispersie. Atenuarea sau absorbţia se datorează în principal prezenţei ionilor hidroxil -OH şi a diferiţilor ioni de metale. Lumina poate fi de asemenea împrăştiată de microcristale, mai mici decât lungimea de undă, care se formează la răcirea sticlei. Atenuarea limitează utilizarea fibrei optice în lungime. Dispersia sau lărgirea lăţimii impulsurilor se datorează în fibra multimod lungimii diferite pe care o au diferitele moduri. O altă dispersie cea cromatică este datorată variaţiei indicelui de refracţie în funcţie de culoarea sau lungimea de undă a luminii. Dispersia limitează utilizarea fibrei optice în frecvenţă sau lărgime de bandă. Cele două limitări înmulţite caracterizează cel mai corect o fibră optică. Valori de 20MHz-km se obţin pentru fibra cu index pas, de 1GHz-km pentru cea cu index variabil şi de 1000GHz-km pentru cea monomod la care nu există dispersie modală.

Transmiţătoarele pentru fibra optică convertesc semnalele electrice în pulsuri luminoase echivalente. Există două tipuri de surse de lumină folosite de transmiţătoarele pentru fibra optică:

- LED-ul care produce lumina în infraroşu având lungimea de undă de 850nm sau 1310nm. Acestea sunt folosite cu fibre multimod. Cuplarea la fibra optică poate fi îmbunătăţită prin utilizarea unei lentile sferice;
- dioda semiconductoare LASER care produce lumina în infrarosu având lungimea de undă de 1310nm sau 1550nm. Acestea sunt folosite cu fibre multimod sau monomod.

Există două tipuri constructive de bază pentru LED-uri: cu emisie pe suprafaţă şi cu emisie pe muchie. La LED cu emisie pe suprafaţă, emisia luminii are loc perpendicular pe planul joncţiunii printr-un strat subţire transparent. Acestea emit într-un spectru geometric radial. La LED cu emisie pe muchie lumina este emisă într-un plan paralel cu joncţiunea la muchia semiconductorului. Materialele cel mai des utilizate sunt compuşi III-V ca GaAs sau $Al_xGa_{1-x}As$ pentru lungimi de undă de 0,8-0,9 μm şi $Ga_xIn_{1-x}P_yAs_{1-y}$ pentru lungimi de undă de 1,3-1,6 μm. Spectrul de emisie a unui LED este cuprins între 25-40 μm pentru lungimi de undă mici şi 50-100 μm pentru lungimi de undă mai mari.

Diodele semiconductoare LASER, diode laser (LD), se obţin prin introducerea unui LED într-o cavitate rezonantă optic. Efectul de LASER apare numai la existenţa unui curent direct suficient de mare pentru a se realiza o inversare de populaţii a electronilor şi a golurilor din cele două benzi energetice de conducţie şi de valenţă. Valoarea de curent de la care apare acest efect se numeşte curent limită. Sub acest curent dispozitivul se comportă ca un LED obişnuit. Deoarece lumina emisă de un laser este mult mai coerentă decât cea emisă de un LED, eficienţa de cuplare la fibra optică este superioară. De asemenea puterea optică captată de la un laser este mai mare decât cea emisă de LED.

O analiză comparată între cele două tipuri de emiţătoare este clar în favoarea LD prin posibilitatea de utilizare la frecvenţe mai mari, spectru mai restrâns şi în favoarea LED ca preţ şi stabilitate mai mare a puterii în raport cu temperatura.

Timpul de viaţă al ambelor dispozitive este egal şi este de ordinul a 10 milioane ore.

Receptoarele pentru fibra optică convertesc pulsurile luminoase în semnale electrice echivalente. Dispozitivele semiconductoare folosite de obicei de receptoarele pentru fibra optică se clasifică în două tipuri: simple şi cu câştig intern. Primele se mai numesc şi fotodiode PIN după tipul de dopare (p intrinsec şi n) iar cea de a doua categorie se numeşte APD (Avalanche Photo-Diodes). Aceste dispozitive sunt sensibile la lungimile de undă ale luminii de 850, 1310 şi 1550nm, lungimi de undă folosite de transmiţătoarele pentru fibra optică. Ca materiale semiconductoare sunt folosite Si pentru lungimi de undă de 800-900 nm şi Ge sau InGaAsP pentru 1300 şi 1500 nm. Si are sensibilitate optimă doar într-o zonă de frecvenţe redusă pe când Ge are un curent de întuneric apreciabil şi este mai sensibil la zgomot. Din acest motiv ultima variantă este cea mai bună dar necesită o tehnologie de fabricaţie mai sofisticată şi în consecinţă are şi un preţ mai mare.

Pentru a conecta fibrele sau pentru a realizare unei fibre mai lungi se folosesc **joncţiuni** (*eng. splices*). Joncţiunile sunt de două tipuri: mecanice şi de fuziune. Atenuările introduse sunt mai mici de 0.5dB (ANSI/TIA-568-C.3 specifică că joncțiunile mecanice sau de fuziune nu trebuie să depășească o pierdere maximă de inserție optică de 0,3 dB). La joncţiunile mecanice cele două capete de fibră, atent tăiate, curăţate şi şlefuite sunt prinse într-o montură mecanică rigidă care le fixează una faţă de cealaltă într-un ansamblu imobil. Joncţiunile de fuziune se execută prin încălzirea aproape până la punctul de topire. În acest moment cele două fibre sunt lipite una de alta şi răcite. Aceste operaţii sunt precedate de operaţii de tăiere şi finisare a capetelor şi de aliniere prealabilă a celor două capete de jonctat. Joncţiunile de fuziune refac şi rezistenţa la tragere/rupere a fibrei la aproximativ 90% din cea iniţială. Pentru a proteja joncțiunile, se folosesc incinte speciale.

Conectorii pentru fibra optică permit conectarea fibrelor la porturi. Cei mai folosiţi conectori sunt SC (Subscriber Connector) - snap on type, ST (Straight Tip) - twist on type, FC (Ferrule Connector) - screw on type, LC (Lucent Connector) - snap on type and MTP/MPO - push/pull type, pentru fibre optice multimod si fibre optice monomod. Atenuarea introdusă de un conector optic, chiar de calitate superioară este mai mare decât cea introdusă de o joncţiune, având valori de aproximativ 1dB. Conectorii sunt echipamente mecanice de mare precizie şi de obicei un capăt al fibrei se află în conector iar unul este liber. În acest caz ataşarea unui conector se reduce la execuţia unei joncţiuni. O astfel de soluţie este de obicei mai avantajoasă decât montarea unui conector direct pe capătul fibrei deoarece conectorii prefabricaţi asigură o precizie de montare mult mai mare. Dacă fibra optică este terminată într-un terminator de fibră optică pentru redistribuire acest conector de capăt se mai numeşte şi pig-tail şi este de tipul prefabricat. O categorie specială de conectori o constituie cordoanele optice de distribuire sau legătură. Acestea sunt fibre optice speciale cu conectori la ambele capete care permit raze de curbură a fibrei mici de ordinul 2,5-5 cm. Culoarea acestora este galben pentru fibra monomod şi portocaliu pentru fibra multimod.

Repetoarele sunt amplificatoare optice care receptionează semnalele luminoase atenuate ca urmare a distanţei parcurse prin fibra optică, refac forma, puterea şi parametri de timp a acestor semnale şi le transmit mai departe.

Patch panel-urile pentru fibră sunt similare patch panel-urilor pentru cablul de cupru mărind flexibilitatea rețelelor optice. Pentru conectarea diferitelor echipamente, se folosește un patch cord de fibră optică (cunoscut și sub denumirea de *zip cord* - două fibre optice flexibile cu conectori la fiecare capăt).

În plus, alte câteva dispozitive active sau pasive sunt folosite împreună cu fibrele optice (exemple: cuploare optice - combină sau împart semnale optice; atenuatoare optice - reduc nivelul de putere al unui semnal optic; izolatori optici; comutatoare de fibră optică; multiplexoare optice etc.).

ISO/IEC 11801-1 specifică cerințele pentru fibre coaxiale, cu perechi răsucite și fibre optice. Standardele ISO/IEC 11801 (Europa) și ANSI/TIA-568-C (SUA și Canada) definesc 7 clase de fibre optice (monomod și multimod) așa cum se arată în tabelul 3.1, împreună cu câțiva parametri importanți (specificațiile pentru fibre optice, performanța transmisiei prin cablu și specificațiile fizice ale cablurilor):

Tabel 3.1 *Caracteristicile fibrelor optice*

		Multimod					**Monomod**	
Tip		*OM1 62,5/125 µm*	*OM2 50/125 µm*	*OM3 50/125 µm*	*OM4 50/125 µm*	*OM5 50/125 µm*	*OS1 9/125 µm*	*OS2 9/125 µm*
Lungime de undă		850, 1300nm	850, 1300nm	850, 1300nm	850, 1300nm	850, 1300nm	1300nm, 1550nm (1383nm)	1300nm, 1550nm
Atenuare max. (db/km)		2.6 / 2.4	3.56 / 2.3	2.6 / 1.9	2.9 / 1.5	2.9 / 1.5	1	0.4
Sursă luminoasă		LED (Light-Emitting Diode) / VCSEL (Vertical Cavity Surface-Emitting Lasers Light Source)					LASER (Light Amplification by Stimulated Emission of Radiation)	
Distanță/ rată de date	**1 Gbps**	275m	550m	-	-	-	5-120km	
	10Gbps	33m	82m	300m	400m	400m	10-80km	
	40-100 Gbps	-	-	100m	150m	150m	2-80km	
Culoare		orange/ slate	orange	albastru deschis (aqua)	violet/ albastru deschis (aqua)	verde/ lime	galben	galben

Instalarea incorecta a fibrelor optice are ca şi rezultat creşterea atenuării semnalului optic. Intinderea sau curbarea exagerată a fibrei optice poate cauza mici fisuri ale miezului care vor dispersa semnalul luminos. Curbarea exagerată a fibrei optice poate avea ca urmare scăderea unghiului incident al semnalului luminos sub unghiul critic de reflexie totală. Pentru instalarea conectorilor capetele fibrei trebuiesc taiate si finisate. Dupa instalare, capetele fibrelor optice, conectorii şi porturile de fibră trebuiesc păstrate curate pentru a nu introduce atenuări. Înaintea folosirii cablurilor de fibră optică, trebuie testată atenuarea introdusă de acestea. La proiectarea unei legaturi pe fibră optică, trebuie calculată pierderea puterii semnalului care poate fi tolerată. Aceasta se numeste bugetul de pierdere a legaturii optice. Pierderea puterii se masoara in decibeli (dB).

Pentru testarea unei legături prin fibră optică există mai multe procedee: testare de continuitate, localizare vizuală a erorilor, procedeul de măsurare a puterii optice la ieşire, procedeul OTDR şi testul BER de rată a erorilor.

Testerele de continuitate sunt folosite pentru a testa continuitatea unei fibre optice. Un instrument de localizare vizuală a defecțiunilor (VFL) permite unui tehnician să identifice rupturi, macro-îndoituri (se referă la raza minimă de îndoire) sau joncțiuni de fuziune slabe.

Procedeul de măsurare a puterii optice la ieşire determină pierderile de putere prin legătura optică măsurând puterea la ieşire la o putere de intrare cunoscută. Unitatea de măsură pentru puteri optice este miliwattul (mW) insă din considerente practice se utilizează o altă unitate de măsură care măsoră câştigul (G) sau pierderea (L) într-un sistem şi anume deciBell-ul (dB).

Procedeul OTDR Optical Time Domain Reflectometer este procedeul prin care se pot vizualiza caracteristicile de atenuare ale unei fibre optice precum şi lungimea acesteia. Acest procedeu este singurul prin care se pot detecta pozițiile întreruperilor în fibra optică. OTDR afişează un grafic care are ca axă x lungimea fibrei şi ca axă y atenuarea. Din graficul astfel afişat se pot deduce atenuarea fibrei, calitatea joncţiunilor şi a conectoarelor. Deasemenea se poate determina poziţia rupturilor în cablu dacă extern cablul nu este afectat.

Testul BER (Bit Error Rate) este testul final la care se supune o legătură de date prin fibră optică. Acest test sau criteriu arată la câţi biţi transmişi prin fibră se produce o eroare datorată fibrei. Testul BER trebuie să îndeplinească cerinţele impuse de producătorii de echipamente DTE ce se cuplează la fibra optică. Pentru reţele de calculatoare acestea cer să fie mai mici decât 1 bit de eroare la $10^9/10^{12}$ biţi transmişi sau BER < $10^{-9}/10^{-12}$. Pentru testare este nevoie de un generator de secvenţe de bit aleatoare şi de o interfaţă la fibra optică dacă se testează o buclă sau de două dacă se testează o singură fibră. Pentru a avea rezultate semnificative testul trebuie să se desfăşoare pe o perioadă suficient de lungă astfel încât să se transmită un număr suficient de mare de biţi. Perioade de testare de o zi sau două sunt obişnuite dacă se lucrează la rată de bit mare în utilizarea legăturii prin fibră optică şi BER mic. Un numărător poate contoriza automat numărul de erori detectate.

2.2 Calculul bugetului de putere optică

Tabelul 3.2 *Calcul buget de putere optica*

Crt.	Pierdere sau Putere Optică	dB
1.	Pierderea pe km în Fibra Optică ___dB/km X __ km fibră	___dB
2.	Pierderea în Joncţiuni ___dB/joncţiune X __ joncţiuni	___dB
3.	Pierderea în Conectoare ___dB/conector X ___ conectoare	___dB
4.	Pierderi pe alte Componente	___dB
5.	Margine de Eroare	___dB
6.	Pierderea Totală pe Legătură (1+2+3+4+5)	___dB
7.	Puterea de Emisie Medie a Emiţătorului	___dB
8.	Puterea Medie Recepţionată de Receptor (7-6)	___dB
9.	Dinamica Receptorului _____dB la _____dB	
10.	Sensibilitatea Receptorului la o Rată de Erori dată BER ____	___dB
11.	Putere Rămasă Disponibilă (8-10)	___dB

Observaţii:

La punctul 3. nu se iau în considerare pierderile de conectare a emiţătorului la fibra optică, acestea fiind deja incluse. Valoarea calculată la punctul 8. trebuie să fie în intervalul de la punctul 9. pentru ca receptorul să funcţioneze corect. Valoarea calculată la punctul 11. trebuie să fie pozitivă pentru a avea o legătură de date optică funcţională.

Marginea de eroare se datorează luării în calcul a unor valori medii pentru toate componentele legăturii. Dispersia acestor valori în jurul valorii medii este cunoscută şi se poate lua o margine de eroare suficient de mare ca aceasta să acopere deviaţiile de la medie cu o probabilitate de 99,9% sau mai mare. Cu cât numărul de elemente este mai mare şi cu cât se doreşte o probabilitate de acoperire mai mare cu atât se va lua o margine de eroare mai mare.

Puterea de emisie optică a emiţătorului este o dată de catalog şi conţine în ea inclusă şi pierderea de conectare la un capăt de fibră optică în cazul în care conectarea se face conform recomandărilor. Puterea este mai mare la diode LASER şi mai mică la LED. În cazul utilizării de LASER este nevoie pentru distanţe relativ scurte chiar de un atenuator pentru a nu distruge receptorul.

Dinamica receptorului reprezintă plaja de puteri pe care un receptor le poate transforma în semnal electric fără pierderi de informaţie.

De asemenea este nevoie de o putere optică minimă necesară pentru îndeplinirea condiţiei de rată de erori tolerată care pentru reţele de calculatoare se situează la valoarea de 1 bit eronat la un miliard de biţi transmişi.

Exemplu de calcul al bugetului de putere optică

Diametrul fibrei optice: Miez 62.5µm/Înveliş 125µm. Apertura numerică a fibrei NA:0,275. Lungimea de undă a echipamentului optic: 1310µm.

Tabelul 3.3 *Exemplu de calcul*

Crt.	Pierdere sau Putere Optică	dB
1.	Pierderea pe km în Fibra Optică 1,8dB/km X 3,5km fibră	6,3dB
2.	Pierderea în Joncţiuni 0,5dB/joncţiune X 2 joncţiuni	1,0dB
3.	Pierderea în Conectoare 1,0dB/conector X 2 conectoare	2,0dB
4.	Pierderi pe alte Componente	0,0dB
5.	Margine de Eroare	2.0dB
6.	Pierderea totală pe Legătură (1+2+3+4+5)	11,3dB
7.	Puterea de Emisie Medie a Emiţătorului	-10,0dB
8.	Puterea Medie Recepţionată de Receptor (7-6)	-21,3dB
9.	Dinamica Receptorului -10,0dB la -30,0dB	
10.	Sensibilitatea Receptorului la o Rată de Erori dată BER 10^{-9}	-26,0dB
11.	Putere Rămasă Disponibilă (8-10)	+4,7dB

Puterea ajunsă la receptor se încadrează în dinamica receptorului, ceea ce face posibilă funcţionarea sa, iar puterea rămasă disponibilă este pozitivă ceea ce ne asigură de o legătură viabilă.

Trebuie ţinut cont şi de faptul că în cursul vieţii legăturii pot apare fenomene de îmbătrânire a materialelor, care duc la creşterea pierderilor de putere, precum şi de faptul că fibra optică poate fi ruptă accidental şi trebuie joncţionată.

Un calcul făcut la limită periclitează durata de exploatare a unei legături prin fibră optică.

3. Desfăşurarea lucrării practice

3.1 Se vor discuta caracteristicile diferitelor tipuri de fibre şi componente optice şi aspectele legate de cablarea reţelelor de calculatoare folosindu-se acest mediu de transmisie.

3.2 Explorați infrastructura de fibra optică din oceane: *https://www.submarinecablemap.com/*

3.3 Se consideră o fibră optică monomod de 9/125µ având lungimea de 2,5km şi pierderea egală cu 0,5dB/km, care conectează două echipamente DTE. Atenuarea introdusă de joncţiuni şi conectori este egală cu 0,5 şi respectiv 1dB. Marginea de eroare luată în considerare este de 3dB. Puterea de emisie medie a emiţătorului este de -15dB, sensibilitatea receptorului la o rată de erori dată BER 10^{-9} este de -25dB şi dinamica receptorului este în intervalul -10 ÷ -30dB. Să se calculeze bugetul de putere optică.

CAPITOLUL 4: CABLAREA STRUCTURATĂ

1. Obiective

Obiectivul acestui capitol este cunoașterea și înțelegerea cablării structurate, a topologiilor de rețele şi a funcţiilor diferitelor dispozitive de reţea.

2. Consideraţii teoretice

2.1 Analiza mediilor fizice

În analiza mediilor fizice se pot alege mai mulţi factori de performanţă cum ar fi: viteza de transfer, lărgimea de bandă, fiabilitatea sau rata de erori, durata de exploatare, durata medie între două defecte, toleranţă la defecte, costuri directe, costuri indirecte, costul per port sau echipament conectat, costul per lărgime de bandă sau costul total per port per lărgime de bandă. Lărgimea de bandă, L_b este un factor de performanţă intrinsec fiecărui mediu. Fiabilitatea sau rata de erori, F, este tot un factor de performanţă intrinsec a fiecărui mediu şi reprezintă raportul dintre numărul de biţi transmişi eronat faţă de numărul total de biţi transmişi. Durata de exploatare, D_e, este durata de timp după care mediul trebuie înlocuit el suferind fenomenul de îmbătrânire. Durata medie între două defecţiuni, DMDD, este timpul mediu statistic între două defectări succesive ale mediului pe perioada normată de viaţă. Toleranţa la defecte, T_d, este un factor de performanţă indus asupra mediului fizic de tehnologia şi arhitectura reţelei utilizate, în multe cazuri însă un anumit mediu nu permite realizarea unei arhitecturi tolerante la erori sau doar a uneia limitate. Costurile directe, C_d, sunt reprezentate de costul efectiv al mediului împreună cu conectori, materialele auxiliare necesare pozării corecte a acestuia şi costul manoperei pentru realizarea mediului de comunicaţie şi a testării mediului astfel realizat. Costul per port, C_p, este un factor sintetic care are o valoare de decizie mai mare, fiind un criteriu de decizie global si reflectând costurile totale pentru realizarea infrastructurii fizice raportat la numărul total de porturi sau echipamente conectate. Costul per port per viteză de transfer, C_{pv}, este un factor de performanţă mult mai util şi care uşurează luarea unei decizii corecte în realizarea unei retele locale de calculatoare el incluzând şi posibilităţi de extensie viitoare fără a fi necesară schimbarea mediului. Costul total per port per viteză, C_{tpv}, este un factor de performanţă complex care caracterizează o retea locala de calculatoare la nivel global încluzând de asemenea şi costurile de echipamente sau tehnologie. O caracterizare din prisma factorilor de performanţă mai sus menţionaţi a mediilor fizice de comunicaţie prezentate anterior se află sintetizată în următorul tabel. Factorii de performanţă, în special cei de tip cost, vor fi clasificaţi relativ fără a da valori absolute care pot fi alterate foarte rapid în timp.

Tabelul 4.1 *Indicatori de performanță*

Mediu	L_b Gbps	$F_{iabilitate}$	D_e ani	DMDD	T_d	C_d	C_p	C_{pv}	C_{tpv}	Recomandat în utilizare	Utilizare viitoare
UTP Cat 5e,6,7	>1	Medie	15	ani	Da	Mediu	Mic	Mic	Mic	DA	DA
F.O. multimod	>1	Mare	30	ani	Da	Mare	Mediu	Mediu	Mediu	DA	DA
F.O. monomod	>1	Mare	30	ani	Da	F. mare	F. mare	Mare	Mare	DA	DA

2.2 Cablarea structurată

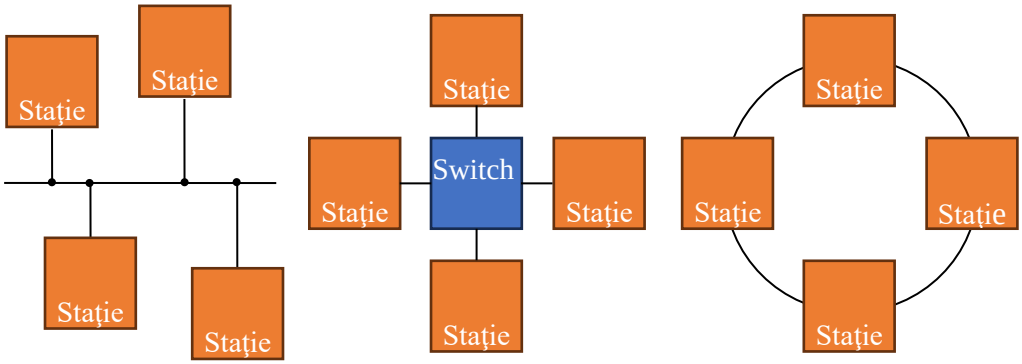
Există trei topologii standard de reţele şi anume topologia magistrală, stea şi respectiv inel:

- **topologia magistrală** este cea mai veche şi cunoscută metodă de conectare a calculatoarelor în rețea. Datele sunt transmise tuturor calculatoarelor dar sunt acceptate doar de calculatorul destinaţie, iar oprirea reflectării semnalului se realizează folosind terminatoare. Figura 4.1 a. prezintă topologia magistrală.

- **topologia stea** a înlocuit în mare măsură vechea topologie magistrală, ea este caracterizată de faptul că există o componentă centrală numită concentrator (hub) prin intermediul căreia semnalele sunt transmise de la un calculator la toate celelalte. Topologia stea oferă resursele şi posibilitatea administrării centralizate. Figura 4.1 b. prezintă topologia stea.

- **topologia inel** conectează calculatoarele printr-un cablu în forma unei bucle şi fiecare calculator actionează ca un repetor amplificând semnalul. Figura 4.1 c. prezintă topologia inel.

În prezent majoritatea topologiilor folosite sunt combinaţii ale topologiilor stea, inel şi magistrală. Topologia magistrală – stea presupune conectarea unor reţele cu topologie stea prin intermediul unor trunchiuri lineare tip magistrală. Probleme de conectivitate apar în situaţia în care se defectează un concentrator. Topologia inel-stea este cunoscută şi sub numele de inel cablat în stea. În acest caz există un concentrator central care leagă celelalte concentratoare la care sunt ataşate staţiile.



a. topologia magistrală b. topologia stea c. topologia inel

Figura 4.1 *Topologii standard de reţele*

Sub denumirea generică de elemente active se grupează toate componentele reţelei care necesită alimentare şi pot lucra cu semnale electrice, optice sau cu ambele tipuri de semnale. **Plăcile/interfețele de reţea** sunt elemente active de Nivel 2 care asigură conectarea la reţea a calculatoarelor. Fiecare placă de reţea are o adresă proprie MAC pe 48 biti asignată din fabricaţie. Aceasta adresa este unica pentru fiecare placă de retea si este compusă din două părti: cei mai semnificativi 24 biţi identifică producătorul iar cei mai puţin semnificativi 24 biţi sunt asignaţi de către acesta. Plăcile de reţea folosite în PC-uri au nevoie de un spaţiu de adrese de I/O şi de o întrerupere hardware. Întreruperea este activată de fiecare dată când apare un eveniment (de regulă recepţie de cadru) care necesită atenţia software-ului, iar spaţiul de I/O

este regiunea de adrese în care sunt accesibili regiştri plăcii (scrişi şi citiţi de către driverul acesteia). De regulă atât întreruperea cât şi spaţiul de I/O sunt configurabile pentru a se putea evita conflictele cu alte dispozitive.

Depăşirea limitărilor de lungime caracteristice cablurilor se realizează folosind **repetoare**. Acestea sunt dispozitive simple, conectate la mai multe segmente de reţea care amplifică semnalul care le străbate. Repetoarele operează la nivel fizic (nu au noţiunea de cadru sau pachet transmis în reţea) şi transmit semnalele amplificate pe toate ieşirile lor.

Odată cu creşterea dimensiunilor reţelei, încep să apară probleme dacă se folosesc doar repetoare. Limitarea pentru calculatoarele care formează o astfel de reţea este faptul ca repetoarele/hub-urile (repetoare multiport) partajează lăţimea de bandă, aflându-se într-un singur **domeniu de coliziune**. Pentru rezolvarea acestei probleme se folosesc **bridge-uri**, echipamente ce operează pe Nivelul 2 în ierarhia OSI, şi care reprezintă echipamente mult mai complexe decât repetoarele deoarece realizează o filtrare a cadrelor pe baza adreselor MAC şi o separare a domeniilor de coliziune. Bridge-urile nu trimit mai departe cadrele locale uneia din reţelele conectate, ci doar pe cele destinate calculatoarelor din alte reţele. Ele memorează cadrele şi realizează retransmisie numai către reţeaua in care se află destinaţia. La punerea sub tensiune, bridge-urile nu cunosc nimic despre configuraţia reţelei şi despre adresele calculatoarelor conectate la ea, dar învaţă topologia reţelei pe măsură ce dirijează cadrele. Iniţial ele permit trecerea tuturor cadrelor în toate direcţiile. Ulterior, pe măsură ce cadrele trec prin ele, bridge-urile inspectează adresa sursă a fiecărui cadru şi îşi completează tabelele de dirijare, cu adresa statiei si portul la care este conectata. Pe baza acestor tabele se decide pe care porturi trebuiesc retransmise cadrele. Cadrele trimise la adrese de broadcast sau multicast vor fi retransmise mai departe pe toate porturile. **Switchurile** sunt echipamente de Nivel 2 care iau decizii de comutare a cadrelor pe baza adreselor MAC pentru a dirija datele doar pe portul căruia îi corespunde hostul destinaţie. Acestea pot fi privite ca dispozitive capabile să ofere conectivitatea unui hub şi reglarea traficului caracteristică bridge-urilor. Majoritatea switchurilor permit conectarea segmentelor Ethernet cu segmente Fast Ethernet.

Ruterele sunt echipamente de Nivel 3 care ruteaza pachetele pe baza adresei folosite de protocoalele rutabile (spre exemplu Internet Protocol - IP sau Internetwork Packet Exchange - IPX) cu ajutorul protocoalelor de rutare (spre exemplu Routing Information Protocol RIP, Interior Gateway Routing Protocol – IGRP, Enhanced Interior Gateway Routing Protocol – EIGRP sau Open Shortest Path First - OSPF). Există două categorii principale de rutere: rutere dedicate şi rutere realizate din calculatoare cu scop general cu mai multe interfeţe. Ruterele realizate din calculatoare au avantajul că sunt mai ieftine, mai simple şi pot fi folosite şi pentru alte sarcini. Ruterele dedicate sunt mai eficiente, mai flexibile, au mai multe interfeţe si suportă mai multe protocoale şi mai multe tipuri de medii de acces. Ruterele dedicate sunt calculatoare specializate pentru sarcina de rutare. Datorită hardware-ului lor specializat şi a software-ului puternic optimizat, acestea realizează performanţe superioare. Ele oferă o gamă foarte largă de viteze, interfeţe fizice şi protocoale de comunicaţie. De regulă acestea sunt realizate de firme specializate (Cisco, Bay Networks, Proteon etc.) şi rulează un sistem de operare propriu, specific, care cuprinde tot software-ul necesar funcţionării ruterului. Ruterele dedicate suportă aproape orice mediu de transmisie, utilizat cu orice protocol de comunicaţie, cu o mulţime de tipuri de mufe şi adaptoare.

Având în vedere costurile pe care le implică realizarea unui cablaj sau modificarea acestuia, s-a ajuns la concluzia că este mai bine ca, un cablaj odată realizat să rămână în folosinţă cât mai multă vreme şi să poată fi folosit şi cu noile tehnologii de comunicaţie, mai rapide. Soluţia

acestei probleme a fost elaborarea conceptului de **cablaj structurat**, definit apoi prin mai multe standarde internaţionale.

Standardele ISO/IEC 11801 (Europe) și ANSI/TIA-568-C (USA and Canada) se referă la cablarea edificiilor comerciale, specificând structura cablajului, configuraţia minimală necesară, categoriile de cabluri şi componente care trebuiesc folosite, modul de instalare, caracteristicile de performanţă care trebuiesc satisfăcute, limitele acceptabile de distanţe şi alţi parametri¸ cât şi modalităţile de verificare a acestora. Este abordată deasemenea şi problema realizării cablajului la nivel mai complex pentru un grup de clădiri, astfel un proiect complex de cablaj structurat presupune realizarea unei structuri ierarhice, arborescente, cu posibilitatea adăugării ulterioare de legături redundante. Specificaţiile standardului referă câteva din următoarele aspecte şi anume:

- Cerinţe minime pentru realizarea cablării unei clădiri:
  - topologia cablării şi distanţele premise;
  - elemente componente ale cablajului;
  - medii de transmisie folosite cu specificarea parametrilor necesari;
  - modul de realizare a cablării verticale, respectiv orizontale;
  - mod de identificare a cablurilor folosite;
  - documentarea proiectului;
- subsisteme componente ale sistemului de cablare structurată:
  - subsistem de la intrarea în clădire;
  - camera cu echipamente;
  - cablarea coloanei vertebrale;
  - dulapul pentru telecomunicaţii;
  - cablarea orizontală;
  - componentele zonei de lucru

Topologia cablării specificată în standardul ISO/IEC sau ANSI/TIA este de tip stea, organizată ierarhic (stea extinsă). Centrul topologiei îl constituie comutatorul principal, al doilea nivel ierarhic îl constituie comutatorul intermediar aferent unui edificiu al zonei, iar la nivelul de jos se găseşte oficiul pentru telecomunicaţii asociat unui etaj sau unui grup de încăperi.

Elementele constitutive sunt:

- *comutatorul principal* – centrul de distribuţie către celelalte edificii;
- *comutatoarele intermediare* – sunt locale edificiilor;
- *oficiul pentru telecomunicaţii* – reprezintă dulapurile de distribuţie locale pentru cablurile la care se conectează staţiile sau aferente cablării verticale;
- *tronsonul interedificii* – identifică cablurile principale care interconectează centrul de distribuţie principal;
- *tronsonul intern* - conectează comutatorul intermediar cu oficiile de distribuţie;
- *Încăperea cu echipamente* – corespunzătoare unui plan de cablare cu elemente pasive sau active;
- *Infrastructura de intrare*- pentru interfaţarea sistemului de cablare exterior cu cel interior;
- *zona de lucru* – posturile de lucru, cablurile de interconectare, adaptoare externe între cabluri;

- *panouri intermediare* – identifică panourile de conectare pentru mediile de transmisie;
- *blocuri cu terminatori* – reprezintă terminatorii mecanici ai cablurilor;
- *prize pentru comunicaţie, adaptoare pentru cablaj*.

Mediile de transmisie uzuale sunt:
- cablu torsadat UTP de categorie 6 sau superioară;
- fibra optică multimod sau monomod;

Tipurile de conectori utilizaţi sunt:
- conectori RJ-45 pentru cablu UTP;
- conectori pentru fibra optică de tip LC, SC sau ST;

Astfel, pentru a face posibilă o administrare cât mai uşoară şi mai eficientă a reţelei, cablajul este structurat folosind concentratoare (pe diverse niveluri). La fiecare etaj trebuie să se implementeze un concentrator de etaj, iar dacă aria care trebuie acoperită este prea mare, atunci se pot utiliza mai multe concentratoare. La posturile de lucru cablul UTP este terminat in cutii de conectare RJ-45, iar la concentrator, în cutii sau panouri de conectare (patch panel). Lungimea cumulată a cablului şi a patch cord-urilor UTP folosite pentru legarea unui calculator la echipamentul din concentrator nu are voie să depăşească 100m. În concentratorul de etaj, se plasează hub-uri, switch-uri sau alte echipamente.

Avantajele pe care le oferă concentratoarele, (respectiv topologiile bazate pe concentratoare) sunt:
- posibilitatea extinderii sau modificării sistemului de cabluri;
- folosirea de porturi diferite, adaptate la diferite tipuri de cabluri;
- posibilitatea monitorizării centralizate a activităţii şi traficului în reţea.

Tipurile de concentratoare sunt:
- **concentratoare active** - care regenerează şi transmit semnalulș
- **concentratoare pasive** - pot fi considerate panourile de cablare sau blocurile de conectare reprezentând doar puncte de conectare fără a amplifica semnalul. Deasemenea există şi concentratoare hibride care permit utilizarea pentru conectare de diferite tipuri de cabluri.

Cablurile trebuie etichetate corespunzător, ventilarea trebuie să fie suficientă pentru a preveni supraîncălzirea echipamentelor, trebuie stabilite măsuri de securitate și trebuie asigurată protecție împotriva incendiilor. Concentratoarele de etaj sunt legate la concentratoarele de clădire, legătură care se poate realiza cu cablu de categoria 6 sau cu fibră optică multimod. Se pot proiecta şi realiza legături redundante atât între concentratoarele de etaj cât şi între cele de clădire. Concentratorul de grup de clădiri este legat de concentratoarele de clădiri cu fibră optică multimod sau monomod. Normele de instalare se referă la instalarea cablurilor (tensiune maxim admisă pe fir, mod de conectare mecanic), cablarea orizontală mascată, protecţia la împământare, protecţia specifică cablurilor cu fibre optice.

3. Desfăşurarea lucrării practice

3.1 Se vor discuta topologiile de reţele de calculatoare punându-se în evidenţă avantajele şi dezavantajele acestora.

3.2 Se vor discuta funcţiile următoarelor dispozitive de reţea: placă de reţea, concentrator, repetor, bridge, switch şi router.

3.3 Se vor discuta aspectele legate de cablajul structurat şi standardul ISO-IEC/ANSI-TIA.

3.4 Se va analiza cablarea etajului şi se vor pune în evidenţă elementele cablajului structurat.

3.5 Identificați și analizați proiectarea cablajului structurat la locul dvs. de muncă/acasă. Cum este conectată rețeaua dvs. la WAN/ISP (ce tip de cablu, dispozitiv etc.)? Cum este conectat dispozitivul dvs. la rețeaua internă?

CAPITOLUL 5: NIVELUL REȚEA – FUNDAMENTE IPV4

1. Obiective

La finalul capitolului, cititorii vor fi capabili: să explice caracteristicile nivelului Rețea, să descrie funcționarea protocolului IPv4, să împartă rețelele în subrețele, să explice procesul de translatare a adreselor de rețea și să implementeze configurații IPv4 de bază.

2. Considerații teoretice

2.1 Nivelul Rețea

Nivelul de Rețea din stiva de protocoale ISO/OSI corespunde nivelului Internet din stiva de protocoale TCP/IP (Figura 5.1). Acesta oferă servicii de adresare, rutare și control al traficului pentru a permite dispozitivelor să facă schimb de date între rețele și conține diferite tipuri de protocoale:

- protocoalele IP versiune 4 (IPv4) și IP versiune 6 (IPv6);
- protocoale de rutare precum Open Shortest Path First (OSPF) sau Border Gateway Protocol (BGP);
- protocoale de semnalizare și diagnosticare precum Internet Control Message Protocol (ICMP).

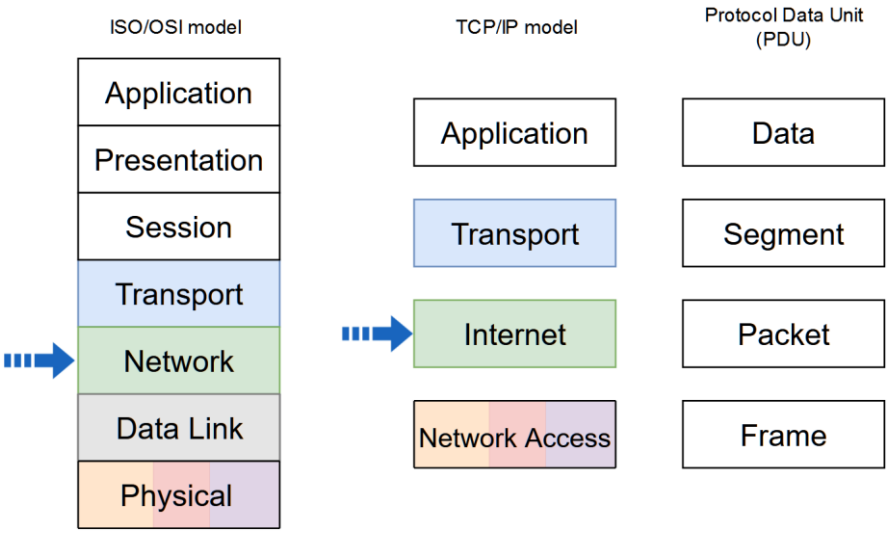


Figura 5.1 *Modele de stivă de rețea și denumire PDU în fiecare nivel. Săgețile indică nivelurile adresate în activitatea curentă*

Nivelul de Rețea efectuează patru operații de bază (Figura 5.2):

- Addresare
- Încapsulare
- Routare
- Deîncapsulare

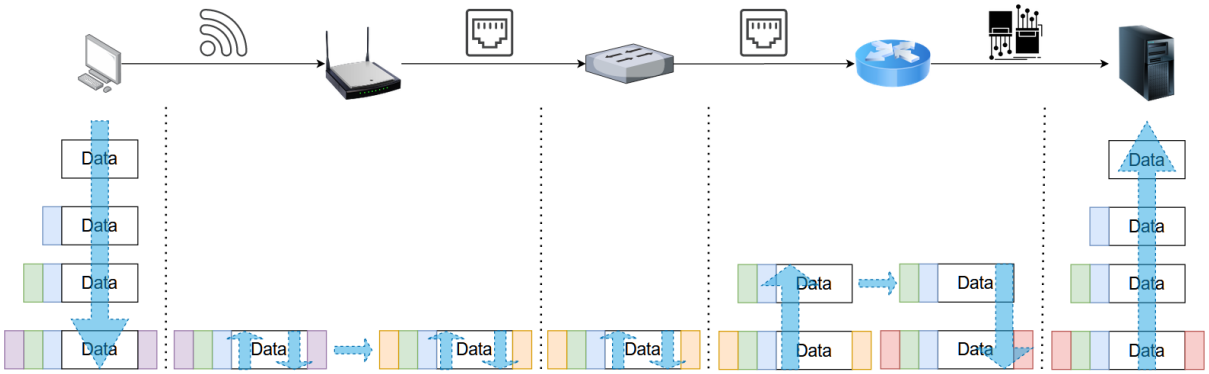


Figura 5.2 *Operațiuni la nivelul de rețea și serializare/deserializare a pachetelor atunci când trec prin diferite dispozitive de rețea*

Protocoalele IP au următoarele caracteristici:

- Fără conexiune
  - nu se stabilește o conexiune între sursă și destinație înainte de transmiterea pachetelor de date;
  - nu se schimbă nicio informație de control (sincronizări, confirmări etc.).
- Best-Effort
  - nefiabil, livrarea pachetelor nu este garantată;
  - nici se utilizează mecanisme de retrimitere a datelor care nu sunt primite, nu se supraîncarcă rețeaua.
- Independent de mediu
  - nu se preocupă de tipul de cadru necesar la nivelul de legătură de date sau de tipul de mediu utilizat la nivelul fizic;
  - poate fi trimis prin orice tip de mediu: cupru, fibră sau wireless.

2.2 IPv4

Structura antetului IPv4 este prezentată mai jos, în figura 5.3:

<table>
<tr><td>Octet</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>Bit</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>0</td><td colspan="4">Version/ Versiune</td><td colspan="4">IHL</td><td colspan="6">DSCP</td><td colspan="2">ECN</td><td colspan="16">Total Length/Lungime totală</td></tr>
<tr><td>32</td><td colspan="16">Identification/Identificare</td><td colspan="3">Flags/ Semnalizare</td><td colspan="13">Fragment Offset</td></tr>
<tr><td>64</td><td colspan="8">Time To Live/ Timp de viață</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum / Sumă de control antet</td></tr>
<tr><td>96</td><td colspan="32">Source IP Address /Adresă IP sursă</td></tr>
<tr><td>128</td><td colspan="32">Destination IP Address / Adresă IP Destinație</td></tr>
<tr><td>160</td><td colspan="32">Options /Opțiuni</td></tr>
</table>

Figura 5.3 *Antetul pachetului IPv4*

- Version / Versiune – câmp care identifică versiune protocolului IP = 4;
- Internet Header Length (IHL) / Lungime Antet - dimensiunea antetului IPv4;
- Differentiated Services Code Point (DSCP) - definită inițial ca fiind Type of Service (ToS), precizează servicii diferenţiate (DiffServ);
- Explicit Congestion Notification (ECN) - permite notificarea congestiei rețelei capăt-la capăt fără a pierde pachetele, caracteristică opțională;
- Total Length/ Lungime totală - definește întreaga dimensiune a pachetului în octeți, inclusiv antetul și datele;
- Identification/Identificare - câmp de identificare, utilizat în principal pentru identificarea unică a grupului de fragmente dintr-o singură datagramă IP;
- Flags/ Semnalizare - utilizat pentru controlul sau identificarea fragmentelor;
  - bit 0 – Rezervat, trebuie să fie zero;
  - bit 1 – Don't Fragment (DF) / Nu se fragmentează
  - bit 2 – More Fragments (MF) / Mai multe fragmente
- Fragment offset – specifică offset-ul unui fragment în raport cu începutul datagramei IP originale nefragmentate;
- Time to live (TTL) / Timp de viată – limitează durata de viață a unei datagrame;
  - în practică, este folosit ca numărător de hop-uri/elemente de nivel rețea traversate;
  - când datagrama ajunge la un router, routerul decrementează câmpul TTL cu valoarea 1;
  - când câmpul TTL atinge zero, routerul renunță la pachet și trimite expeditorului un mesaj ICMP de tip timp depășit.

- Protocol – definește protocolul utilizat în porțiunea de date a datagramei IP;
- Header checksum / Sumă de control antet – folosit pentru verificarea erorilor antetului;
- Source address / Adresă IP sursă – adresa IPv4 a expeditorului pachetului;
- Destination address / Adresă IP destinație – adresa IPv4 a destinatarului pachetului;
- Options – folosit rar; dacă IHL este mai mare de 5, câmpul opțiuni este prezent.

Adresele IPv4 pot fi atribuite static sau dinamic.

Adresa IPv4 este ierarhică, fiind compusă din două părți: partea de rețea și partea gazdă (Figura 5.4).

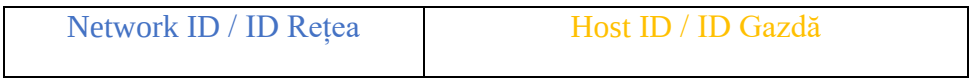


Figura 5.4 *Structura adresei IPv4*

Numărul de biți alocați rețelei și gazdei depinde de clasa căreia îi aparține adresa:

Clasă	**Primul Octet Interval zecimal**	**Primii biți din primul octet**	**ID Rețea (N) / Gazdă (H)**	**Mască de rețea implicită**
A	1 – 126*	0	N.H.H.H	255.0.0.0
B	128 – 191	10	N.N.H.H	255.255.0.0
C	192 – 223	110	N.N.N.H	255.255.255.0
D	224 – 239	1110	Rezervat pentru multicasting	
E	240 – 255**	1111	Experimental; folosit pentru cercetare	

Noteă * Adresele de clasă A de la 127.0.0.0 la 127.255.255.255 nu pot fi utilizate și sunt rezervate pentru funcțiile de loopback și diagnosticare.

** 255.255.255.255 este rezervată ca adresă de brodcast IPv4.

Masca de rețea (NM) IPv4 este utilizată pentru a diferenția porțiunea de rețea de porțiunea gazdă a unei adrese IPv4. La fel ca adresa IPv4, masca de rețea are o structură de 32 de biți. Biții corespunzători porțiunii de rețea sunt setați la 1, iar biții corespunzători porțiunii gazdă sunt setați la 0.

ID Rețea	ID Gazdă
11……..1	00……..0

Figura 5.5 *Masca de rețea IPv4*

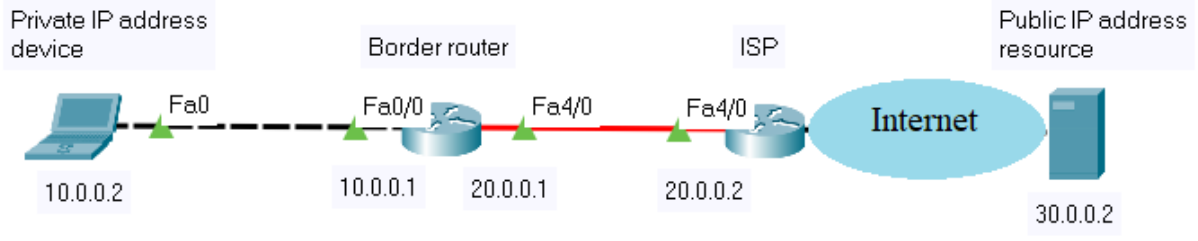
Măștile de rețea corespunzătoare claselor sunt prezentate mai jos:

Clasa A: 255.0.0.0 sau /8 (11111111.00000000.00000000.00000000)
Clasa B: 255.255.0.0 sau /16 (11111111.11111111.00000000.00000000)
Clasa C: 255.255.255.0 sau /24 (11111111.11111111.11111111.00000000)

Adresele publice IPv4 sunt adrese atribuite în mod unic și utilizate pentru a direcționa pachetele la nivel global între furnizorii de servicii de internet (ISP). Există, de asemenea, blocuri de adrese, numite adrese private, care sunt folosite de majoritatea organizațiilor pentru a atribui adrese IPv4 dispozitivelor interne. Aceste adrese nu sunt adrese atribuite în mod unic și nu sunt direcționate global între routerele ISP. Aceste blocuri de adrese private sunt prezentate mai jos.

Clasa A: 10.0.0.0 - 10.255.255.255 /8
Clasa B: 172.16.0.0 - 172.31.255.255 /12
Clasa C: 192.168.0.0 - 192.168.255.255 /16

Pentru a permite unui dispozitiv cu o adresă IPv4 privată să acceseze dispozitive și resurse din afara rețelei locale, adresa privată trebuie să fie translatată într-o adresă publică. Acest proces se numește translatarea adresei de rețea (NAT – Network Address Translation) și oferă translatarea adreselor private în adrese publice (Figura 5.6). Un router NAT funcționează de obicei la granița unei rețele. Când un dispozitiv din interiorul rețelei dorește să comunice cu un dispozitiv din afara rețelei sale, pachetul este redirecționat către routerul de graniță; acesta efectuează procesul NAT, translatând adresa privată internă a dispozitivului într-o adresă publică, exterioară.



```
BorderRouter#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 20.0.0.3:1027      10.0.0.2:1027      30.0.0.2:80        30.0.0.2:80
```

Figura 5.6 *Exemplu NAT*

Adresa de rețea are toți biții gazdă setați la 0, iar adresa de broadcast (difuzare) are toți biții setați la 1. Aceste adrese nu pot fi atribuite unei gazde. Toate celelalte adrese sunt adrese de gazdă valide.

Exercițiu

Se consideră următoarea adresă: 192.168.1.10/24. Calculați adresa de rețea și adresa de broadcast, intervalul de adrese IPv4 gazdă valid, numărul total de biți gazdă și numărul total de IP gazdă.

IP: 11000000.10101000.00000001.00001010
NM: 11111111.11111111.11111111.00000000

IP ȘI logic cu NM:
11000000.10101000.00000001.00001010
11111111.11111111.11111111.00000000

11000000.10101000.00000001.00000000 – Adresa de rețea (toți biții gazdă setați la 0)

192.168.1.0 – Adresa de rețea (notație zecimală)

11000000.10101000.00000001.11111111 – Adresa de broadcast (toți biții gazdă setați la 1)

192.168.1.255 – Adresa de broadcast (notație zecimală)

11000000.10101000.00000001.00000001 – Prima adresă IPv4 gazdă validă

192.168.1.1 – First valid host address

11000000.10101000.00000001.11111110 – Ultima adresă IPv4 gazdă validă

192.168.1.254 – Ultima adresă IPv4 gazdă validă (notație zecimală)

192.168.1.1-192.168.1.254 – Interval de adrese IPv4 gazda valide (notație zecimală)

Numărul total de biți gazdă este **8.**
Numărul total de IPuri gazdă este 2^8**-2=254.**

2.3 Subnetare

Pentru a crea subrețele, biții sunt împrumuți de la IDul gazdei. Este creată o nouă mască de rețea pentru a afișa noua structură. În masca de rețea, biții corespunzători porțiunii de subrețea sunt setați la 1 (Figura 5.7).

Network ID	Host ID	
11……..1	00……..0	
Network ID	Subnetwork ID	Host ID
11……..1	11……..1	00……0

Figura 5.7 *Masca de subrețea IPv4*

Exercițiu

Se consideră următoarea adresă: 192.168.1.0/24. Împărțiți această adresă în 4 subrețele și împărțiți în continuare a patra subrețea într-un număr maxim de subrețele. Specificați pentru subrețele: mască de rețea, adresa de rețea, adresa de broadcast, numărul de biți gazdă, numărul de gazde și intervalul de adrese ale acestora.

Vom împrumuta 2 biți pentru a obține 4 subrețele. Pentru a împărți în continuare a patra subrețea într-un număr maxim de subrețele, vom rezerva pentru porțiunea gazdă 2 biți, numărul minim posibil (Figura 5.8(.

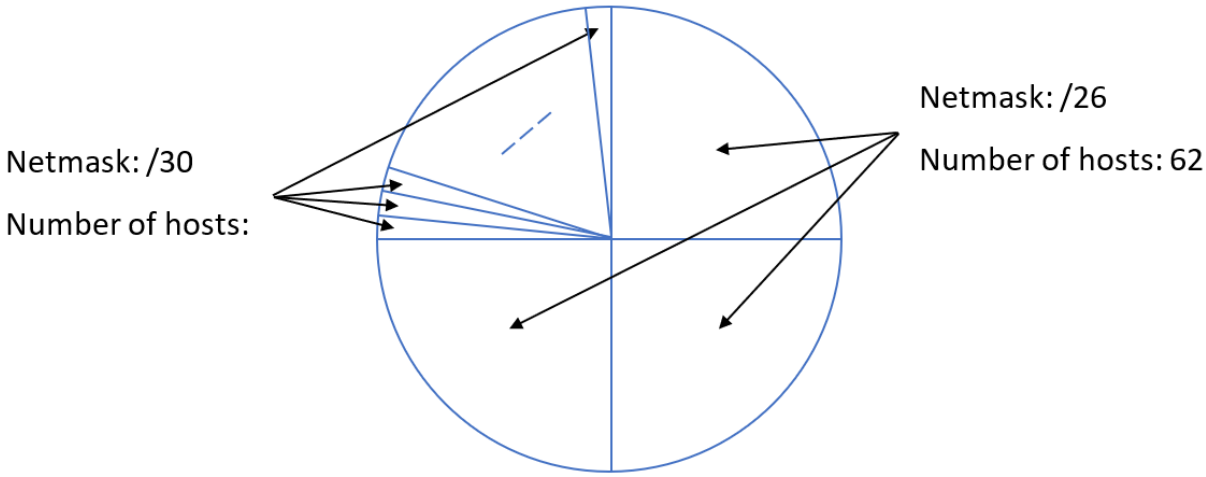


Figura 5.8 *Împărțirea unei adrese de rețea în subrețele*

Prima subrețea cu masca /26:

Rețea Subrețea Gazdă	
11000000.10101000.00000001.00000000	192.168.1.0/26 - Adresa de rețea
11000000.10101000.00000001.00000001	192.168.1.1/26 - Prima adresă IPv4 gazdă
…	…
11000000.10101000.00000001.00111110	192.168.1.62/26 – Ultima adresă IPv4 gazdă
11000000.10101000.00000001.00111111	192.168.1.63/26 - Adresa de broadcast

Masca de rețea (Netmask): /26 (255.255.255.192)

Adresa de rețea (Network address): 192.168.1.0/26

Adresa de broadcast (Broadcast address): 192.168.1.63/26

Numărul de biți gazdă (host bits): 6

Numărul de IPuri gazdă valide: 2^6-2=62

Interval de adrese IPv4 gazda valide: 192.168.1.1/26-192.168.1.62/26

First /30 subnet:

Network Subnetwork Host	
11000000.10101000.00000001.11000000	192.168.1.192/30 - Adresa de rețea
11000000.10101000.00000001.11000001	192.168.1.193/30 - First Host Address
…	…
11000000.10101000.00000001.11000010	192.168.1.194/30 - Ultima adresă IPv4 gazdă
11000000.10101000.00000001.11000011	192.168.1.195/30 - Adresa de broadcast

Masca de rețea (Netmask): /30 (255.255.255.252)

Adresa de rețea (Network address): 192.168.1.192/30

Adresa de broadcast (Broadcast address): 192.168.1.195/30

Numărul de biți gazdă (host bits): 2

Numărul de IPuri gazdă valide: 2^2-2=2

Interval de adrese IPv4 gazda valide: 192.168.1.193/30-192.168.1.194/30

3. Desfăşurarea lucrării practice

3.1 Discutați aspectele teoretice.

3.2 Rezolvați următoarele probleme:

A. Determinați adresele de rețea și broadcast, numărul de biți gazdă și numărul IPuri gazdă posibile, pentru adresele și prefixele IPv4 date:

Adresă IPv4 / Prefix	**Adresa de rețea**	**Adresa de broadcast**	**Numărul de biți gazdă**	**Numărul IPuri gazdă posible**
172.16.104.99/27				
198.133.219.250/24				
10.1.113.75/19				

B. Având următoarele informații și constrângeri, calculați subrețele:
- Un număr de 62 de subrețele
- Adresa IP gazdă: 172.16.0.0
- Masca de rețea originală: 255.255.0.0

C. Având următoarele informații și constrângeri, calculați subrețele:
- Un număr maxim de 29 gazde/subrețea
- Adresa IP gazdă: 192.168.200.0
- Masca de rețea originală: 255.255.255.0

D. Având următoarele informații și constrângeri, calculați subrețele:
- Un număr de 250 de subrețele
- Adresa IP gazdă: 10.0.0.0
- Masca de rețea originală: 255.0.0.0

3.3 Testați următoarele comenzi (folosind Command Prompt pe sistemul de operare Windows sau Terminal în sistemul de operare Linux):

- Comandă: **ipconfig /all** (Windows) și **ifconfig (**Linux)
- *Rol: afișează toate valorile de configurare a rețelei pentru toate interfețele de rețea*

- Comandă: **ipconfig /release** și **ipconfig /renew** (Windows) și **dhclient (**Linux)
- *Rol: reîmprospătează valorile DHCP și DNS*

- Comanda: **ping**
- *Rol: depanează conexiunea de rețea; verifică conexiunile IP, folosind pachete ICMP*

- Comanda: **tracert** (**traceroute** în Linux)
- *Rol: depanează conexiunea de rețea; rezolvă calea către o destinație IP, folosind pachete ICMP*

- Comanda: **nslookup**
- *Rol: efectuează interogări DNS*

- Comanda: **route print**
- *Rol: afișează tabelul de rutare al dispozitivului gazdă*

- Comanda: **netstat**
- *Rol: instrument de statistică de rețea*

- Comanda: **arp -a**
- *Rol: afișează memoria cache ARP (maparea adresei IP la adresele fizice)*

Sugestie: puteți utiliza sisteme de operare online pentru a testa diverse comenzi (de exemplu https://bellard.org/jslinux/ pentru Alpine Linux sau Windows 2000)

3.4 Folosind Wireshark, capturați diferite tipuri de pachete IP și analizați anteturile acestora. De exemplu:
- capturați traficul generat de comanda **ping** prin utilizarea filtrului de protocol ICMP
- capturați traficul generat de comanda **nsloookup** prin utilizarea filtrului de protocol DNS

3.5 Configurați și testați următoarea rețea (Figura 5.9) folosind Cisco Packet Tracer:

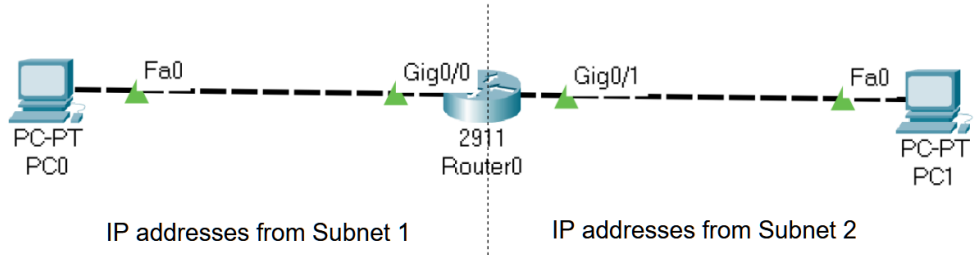


Figura 5.9 *Topologia rețelei de tes*

Considerând adresa IP 172.16.0.0 /16, calculați 2 subrețele și atribuiți adresa IP corectă interfețelor routerelor și computerelor gazdă (PC0 și PC1).

Pas 0: Pentru a afișa numele și numerele interfețelor, accesați meniul Options -> Preferences și bifați "Always Show Port Labels in Logical Workspace" (Figura 5.10).

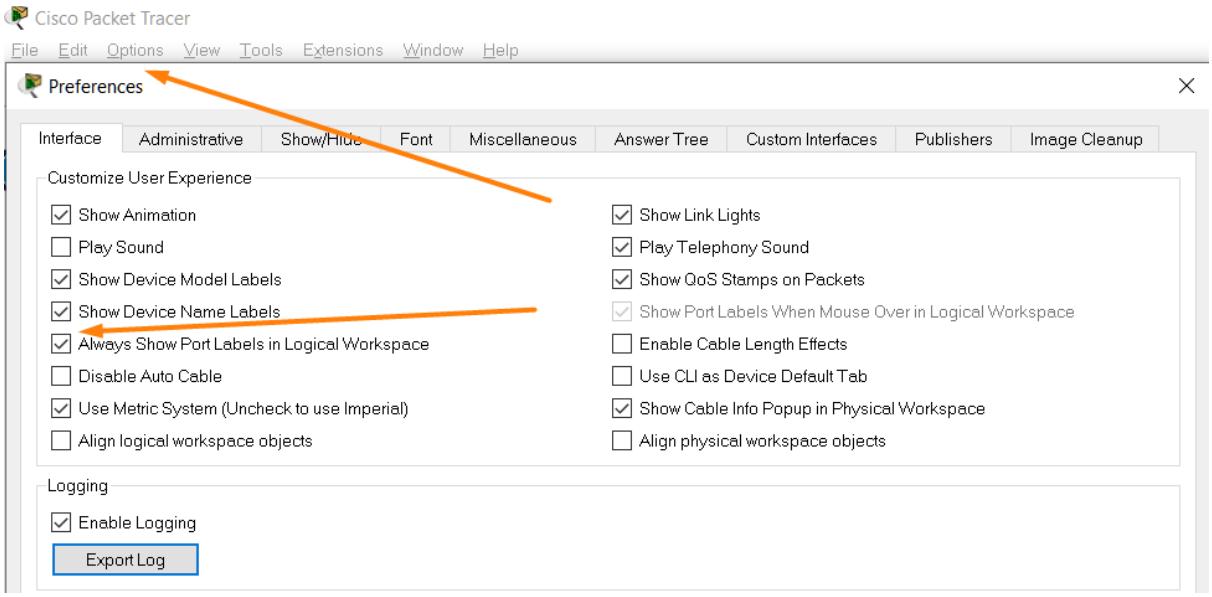


Figura 5.10 *Meniul Preferences*

Pas 1: Creați cele două subrețele

Pas 2: Înainte de a configura dispozitivele de rețea, atribuiți o adresă IP unică și masca de subrețea corespunzătoare fiecărei interfețe de rețea:

Dispozitiv	**Interfață**	**Adresă IP**	**Mască de rețea**
PC0	Fa0	172 . ___ . ___ . ___	___ . ___ . ___ . ___
Router0	Gig0/0	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Router0	Gig0/1	___ . ___ . ___ . ___	___ . ___ . ___ . ___
PC1	Fa0	___ . ___ . ___ . ___	___ . ___ . ___ . ___

Pas 3: Configurați routerul utilizând comenzile furnizate la pașii de mai jos. Comenzile oferă exemple de nume de interfață și adrese IP. Trebuie să utilizați numele interfeței și adresele IP completate în tabelul anterior și exemplu din Figura 5.11:

Exemplu de configurare a topologiei ilustrate

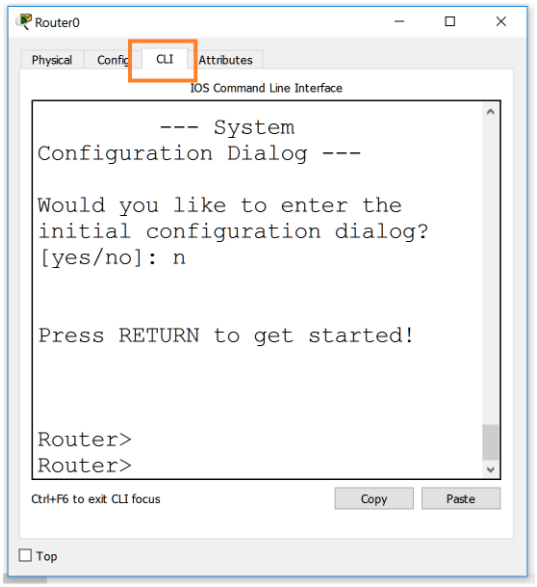


Figura 5.11 *Accesare CLI*

Pas 3.1: Intrați în modul de configurare pe router
Router>enable
Router#configure terminal
Router(config)#

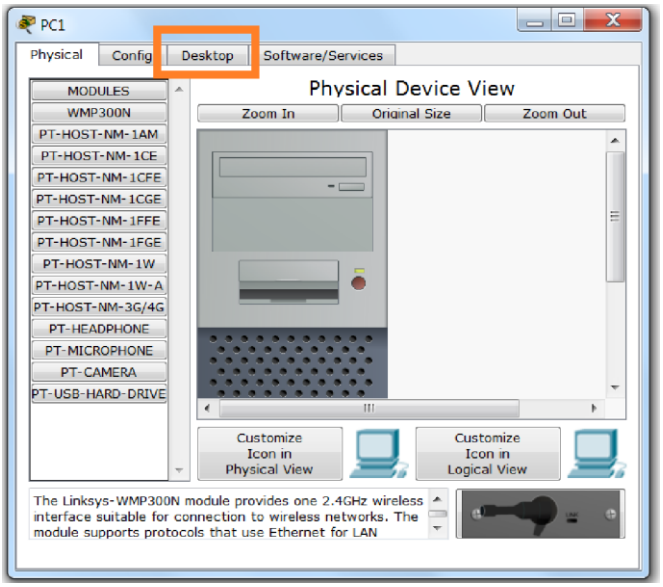
Pas 3.2: Atribuiți adresa IPv4 statică interfețelor routerului
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

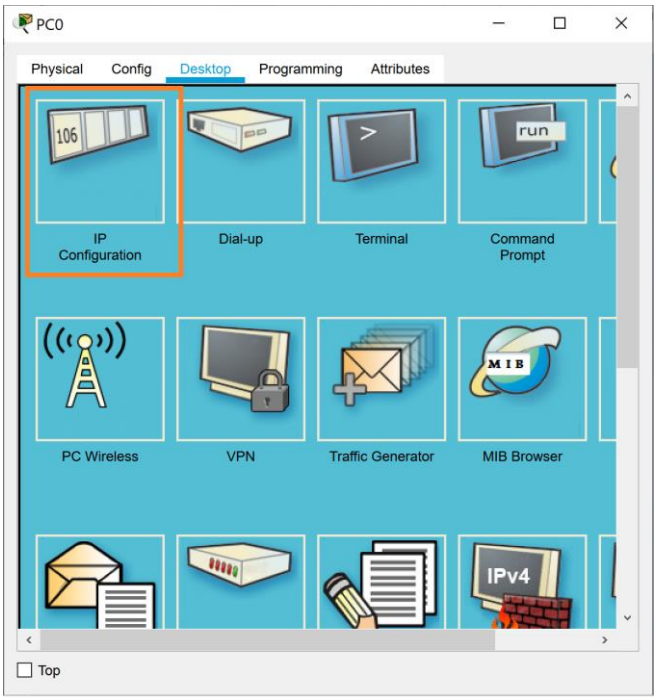
Configurați cealaltă interfață de router cu adresa IP corespunzătoare
Router(config)# interface ___
Router(config-if)#ip address _____ _____
Router(config-if)#no shutdown

Pas 3.3: Afișații informații despre configurația routerului
Router#show ip interface brief
Descriere: Afișează informațiile IP despre interfețele routerului
Router#show ip route
Descriere: Afișează tabela de rutare IP

Pas 3.4: Repetați pașii de mai sus și pentru celălalt router, considerând informațiile din tabelul anterior

Pas 4: Configurați adresele IP pe computere folosind următoarele capturi de ecran (Figura 5.12)





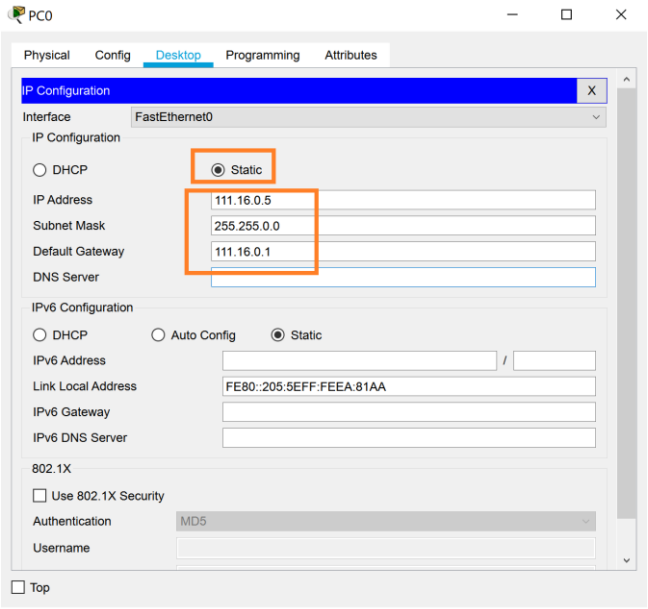


Figura 5.12 *Capturi de ecran - configurare PC*

Testați conectivitatea.

a. *verificați adresele IP ale computerelor gazde: PC -> Desktop -> IP Configuration*
b. *Verificați conectivitatea între computere folosind comanda* ***ping <target IP>*** *(PC -> Desktop -> Command prompt)*

CAPITOLUL 6: NIVELUL REȚEA – RUTARE IPV4 ȘI DHCP

1. Obiective

La finalul capitolului, cititorii vor fi capabili să explice procesul de rutare, să descrie funcționarea protocolului DHCPv4 și să implementeze configurații de rețea IPv4 de bază.

2. Considerații teoretice

Capitolul curent se concentrează pe stratul de rețea al stivei ISO/OSI (Figura 6.1).

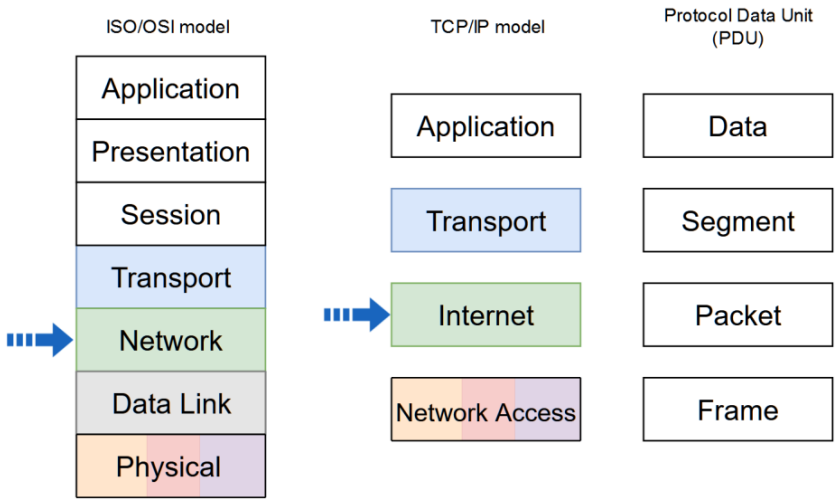


Figura 6.1 *Modele de stivă de rețea și denumire PDU în fiecare nivel. Săgețile indică nivelurile adresate în activitatea curentă*

2.1 Rutare

Pachetele IP sunt create de dispozitivele sursă și sunt direcționate către destinație. Direcționarea pachetelor IP către destinație se bazează pe procesul de rutare. Acesta este un proces distribuit: fiecare nod, care direcționează pachetele în funcție de adresa IP, va alege nodul următor în conformitate cu propria sa tabelă de rutare. Direcționarea pachetelor IP este un proces pas cu pas, fiecare nod direcționând pachetul către nodul următor.

Dispozitivele gazdă și routerele direcționează pachetele în funcție de adresa IP a destinației. Switch-urile și punctele de acces sunt dispozitive de nivel 2 și nu direcționează pachetele în funcție de adresa IP a destinației (Figura 6.2)..

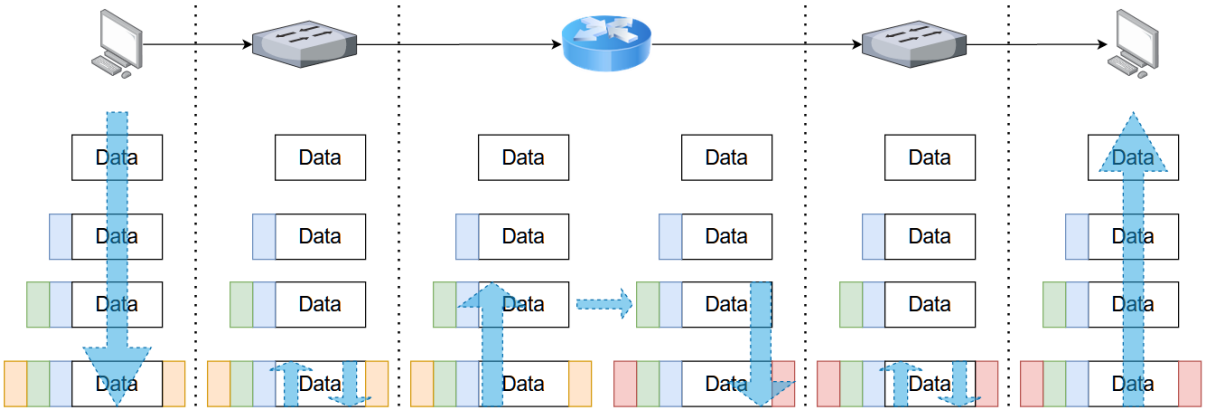


Figura 6.2 *Operațiuni la nivelul de rețea și serializare/deserializare a pachetelor atunci când trec prin diferite dispozitive de rețea*

Gazda sau routerul examinează adresa IP de destinație a pachetului și caută în tabela sa de rutare pentru a determina unde să transmită mai departe pachetul. Tabela de rutare conține o listă a tuturor adreselor de rețea cunoscute (prefixe) și unde să trimită pachetele care aparțin rețelelor corespunzătoare. Aceste intrări sunt cunoscute sub numele de intrări de rută sau rute. Gazda sau routerul vor transmite pachetul folosind cea mai bună (cea mai lungă) potrivire a intrării de rută. Majoritatea gazdelor și a routerelor includ, de asemenea, o intrare de rută implicită, 0.0.0.0/0. Rută implicită este folosită atunci când nu există o potrivire mai bună (mai lungă) în tabela de rutare IP.

Pentru a identifica adresa de rețea a unui dispozitiv gazdă IPv4, adresa IPv4 este combinată logic, bit cu bit, cu masca de subrețea. Combinarea logică între adresă și masca de subrețea produce adresa de rețea. Exercițiu: găsiți adresa de rețea pentru gazda configurată cu adresa IPv4 192.168.50.106 și masca de subrețea 255.255.255.0.

IPv4 host address		192	.	168	.	50	.	106
		11000000		10101000		00110010		01101010
	AND							
Subnet Mask		255	.	255	.	255	.	0
		11111111		11111111		11111111		00000000
IPv4 network address	Equals	192	.	168	.	50	.	0
		11000000		10101000		00110010		00000000

O gazdă poate trimite un pachet către (Figura 6.3)::

- Ea însăși - către interfața loopback, adresa IPv4 127.0.0.1 sau adresa IPv6 ::1;
- Gazda locală - gazda destinație se află în aceeași rețea locală ca și gazda sursei, gazdele sursă și destinație au aceeași adresă de rețea;
- Gazda la distanță (remote) - gazda destinație se află într-o altă rețea, gazdele sursă și destinație nu au aceeași adresă de rețea.

Gateway-ul implicit este dispozitivul de rețea care poate ruta traficul către alte rețele. Are o adresă IP locală în același interval de adrese ca și celelalte gazde din rețeaua locală, acceptă date în rețeaua locală, trimite date din rețeaua locală și rutează traficul către alte rețele.

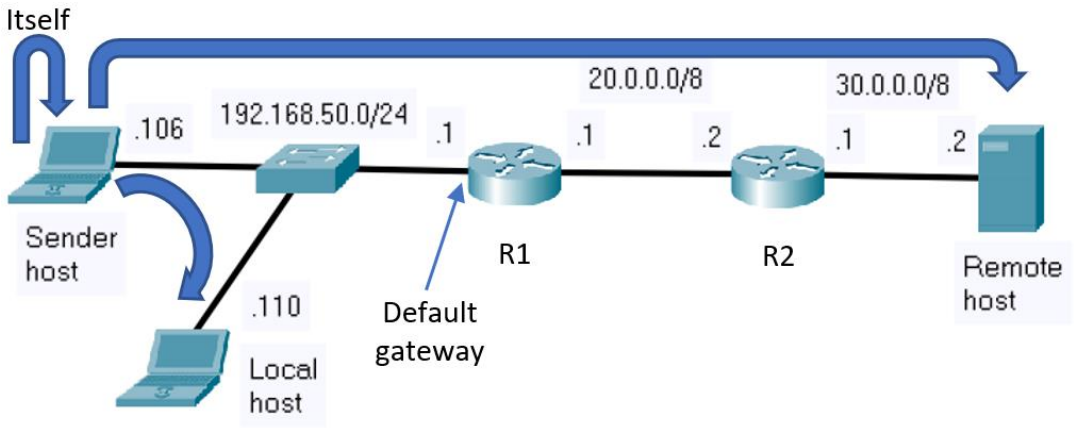


Figura 6.3 *Destinații posibile ale pachetelor atunci când o gazdă transmite date*

Când o gazdă este configurată cu adresă IPv4, mască de subrețea și gateway-ul implicit (Figura 6.4), își actualizează tabela de rutare în consecință (Figure 6.5).

```
C:\Users\Admin>ipconfig

   IPv4 Address. . . . . . . . . . . : 192.168.50.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1
```

Figura 6.4 *Configurația IP pentru o gazdă*

```
C:\Users\Admin>route print

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.50.1   192.168.50.106     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.50.0    255.255.255.0         On-link    192.168.50.106    311
   192.168.50.106  255.255.255.255         On-link    192.168.50.106    311
   192.168.50.255  255.255.255.255         On-link    192.168.50.106    311
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    192.168.50.106    311
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    192.168.50.106    311
===========================================================================
```

Figura 6.5 *Tabela de rutare a gazdei*

Dacă o gazdă trimite un pachet către un dispozitiv configurat cu aceeași rețea IP ca și dispozitivul gazdă, pachetul este trimis prin interfața gazdă, prin dispozitivul intermediar și către dispozitivul destinație direct. Luând în considerare rețeaua de mai jos (Figura 6.6), pachetul este transmis de la 192.168.50.106 la 192.168.50.110. Cea mai bună (cea mai lungă) rută în acest caz este marcată cu roșu (Figura 6.7).

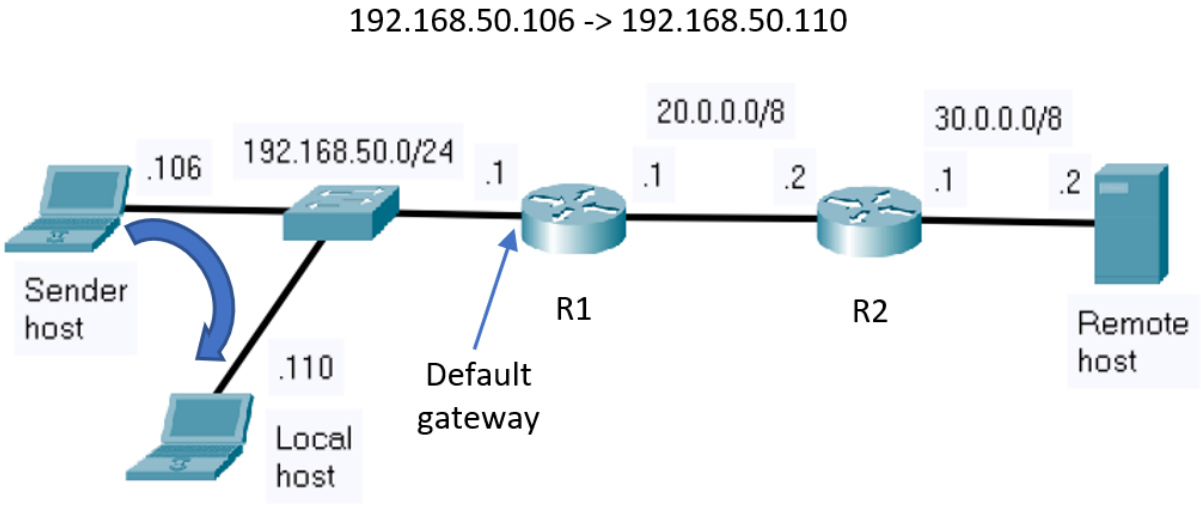


Figura 6.6 *Comunicare de la gazda sursă către o gazdă locală*

```
C:\Users\Admin>route print

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.50.1   192.168.50.106     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.50.0    255.255.255.0         On-link    192.168.50.106    311
    192.168.50.106  255.255.255.255         On-link    192.168.50.106    311
    192.168.50.255  255.255.255.255         On-link    192.168.50.106    311
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    192.168.50.106    311
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    192.168.50.106    311
===========================================================================
```

Figura 6.7 *Cea mai bună potrivire de rută pentru o gazdă locală*

Dacă o gazdă trimite un pachet către o gazdă dintr-o rețea la distanță (remote), pachetul este transmis din interfața gazdei, prin dispozitivul intermediar și către gateway. Luând în considerare rețeaua de mai jos (Figura 6.8), pachetul este transmis de la 192.168.50.106 către 30.0.0.2. Cea mai bună (cea mai lungă) rută (Figura 6.9) în acest caz este ruta implicită, marcată cu roșu.

Când pachetul ajunge pe interfața unui router, acesta decapsulează antetul și secvența terminală (trailer) de Nivel 2. Apoi, examinează adresa IPv4 destinație a pachetului și caută cea mai bună potrivire în tabela sa de rutare IPv4. Odată ce cea mai bună potrivire din tabela de rutare este găsită, routerul înaintează pachetul conform informațiilor din intrarea de rutare, încapsulându-l în noul antet și secvență terminală de Nivel 2. În exemplul nostru, cea mai bună (cea mai lungă) intrare de rutare (Figura 6.10) este o rută statică, marcată cu roșu.

Și procesul de trimitere salt-cu-salt (hop-by-hop) continuă până când pachetul ajunge la destinație.

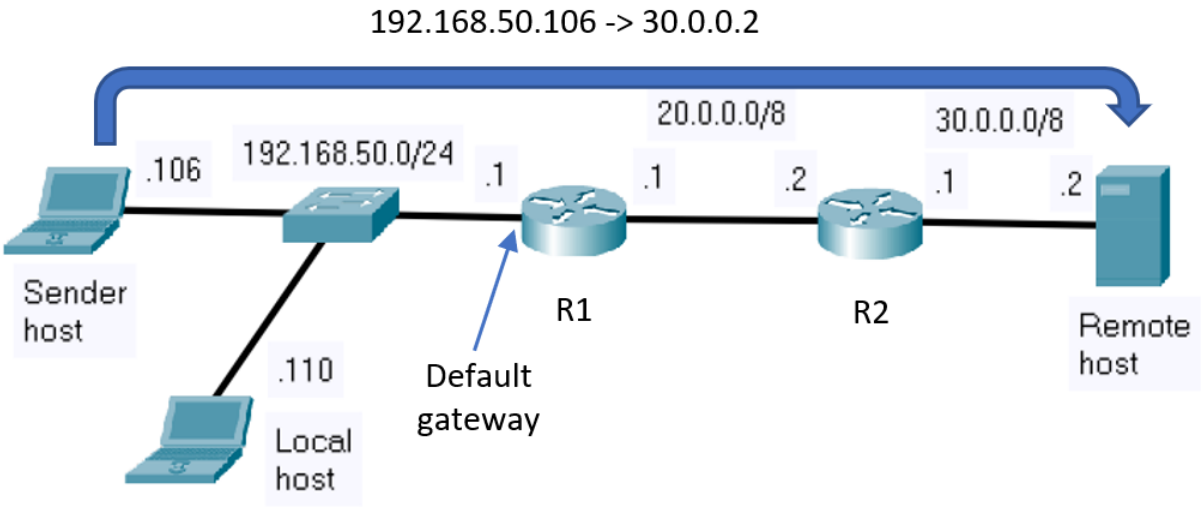


Figura 6.8 *Comunicare de la gazda sursă către o gazdă la distanță*

```
C:\Users\Admin>route print

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.50.1    192.168.50.106     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.50.0    255.255.255.0         On-link    192.168.50.106    311
  192.168.50.106  255.255.255.255         On-link    192.168.50.106    311
  192.168.50.255  255.255.255.255         On-link    192.168.50.106    311
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    192.168.50.106    311
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    192.168.50.106    311
===========================================================================
```

Figura 6.9 *Cea mai bună potrivire de rută pentru o gazdă la distanță*

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    20.0.0.0/8 is directly connected, FastEthernet1/0
S    30.0.0.0/8 [1/0] via 20.0.0.2
C    192.168.50.0/24 is directly connected, FastEthernet0/0
```

Figura 6.10 *Cea mai bună potrivire de rută pentru o gazdă la distanță în tabela de rutare a routerului R1*

Când un router este configurat cu o adresă IPv4 și o mască de subrețea, acesta își actualizează tabela de rutare în consecință. În plus, un router poate afla despre rețelele la distanță (remote) în două moduri: manual și dinamic. În primul caz, rețelele la distanță (remote) sunt introduse manual în tabela de rutare folosind rute statice. În al doilea caz, rețelele la distanță (remote) sunt învățate automat folosind un protocol de rutare dinamic.

În exemplul anterior, routerul R1 a fost configurat manual cu o rută statică pentru a ajunge la adresa rețelei la distanță (remote), 30.0.0.0/8, prin adresa IP a routerului următor, 20.0.0.2 (Figura 6.11).

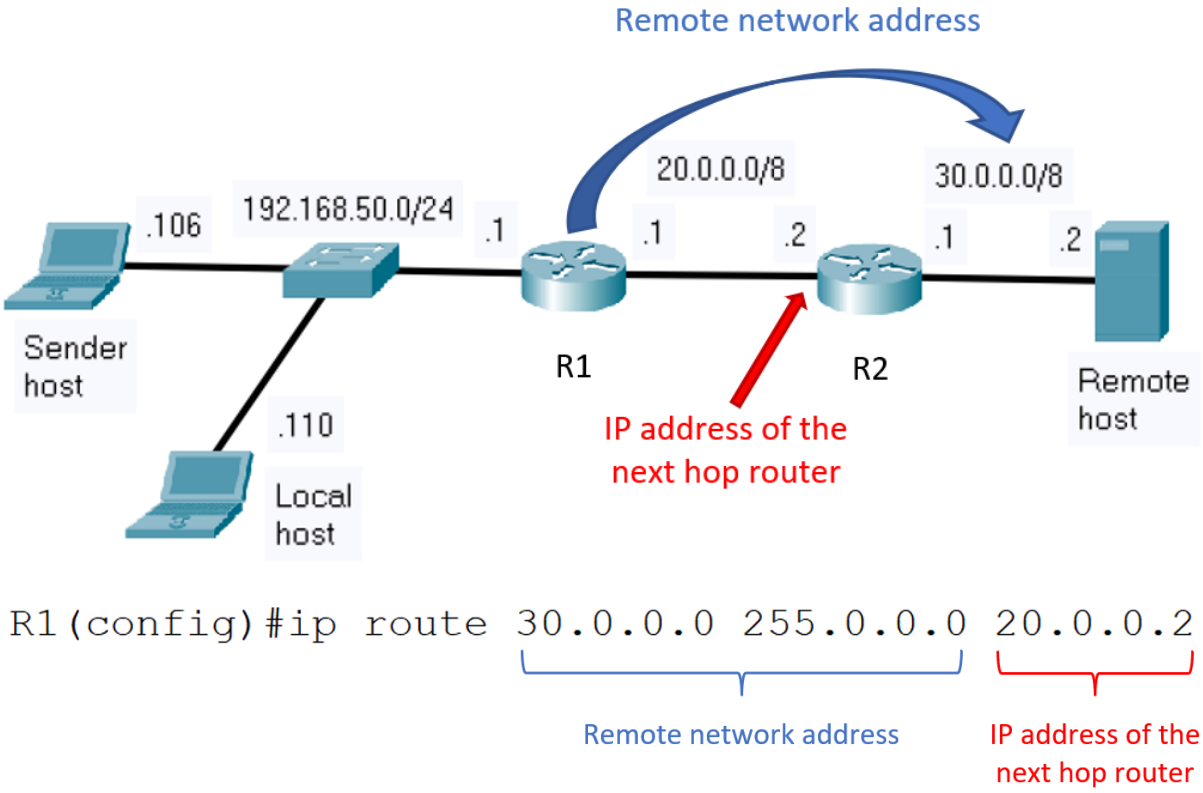


Figura 6.11 *Configurația rutei statice*

2.2 DHCP v4 (Dynamic Host Configuration Protocol)

Protocolul Dynamic Host Configuration Protocol v4 (DHCPv4) atribuie, în mod dinamic, informațiile de configurare a rețelei. Adresa IPv4 este atribuită sau închiriată pentru o perioadă limitată de timp. Atunci când închirierea expiră, clientul trebuie să solicite o altă adresă. De obicei, serverul reatribuie aceeași adresă clientului.

Serviciul DHCPv4 poate rula pe diverse dispozitive, cum ar fi un server dedicat sau un router. Procesul DHCP începe atunci când clientul se alătură unei rețele. Clientul trimite un mesaj de tip broadcast DHCPDISCOVER pentru a găsi serverul DHCPv4. Serverul DHCPv4 rezervă o adresă IPv4 disponibilă pentru a o închiria clientului și trimite mesajul de ofertă DHCPOFFER pentru crearea unei legături (binding) între adresa IPv4 și acel client. Clientul trimite un mesaj de tip boradcast DHCPREQUEST ca notificare de acceptare a legături. Serverul răspunde cu un mesaj DHCPACK (Figura 6.12).

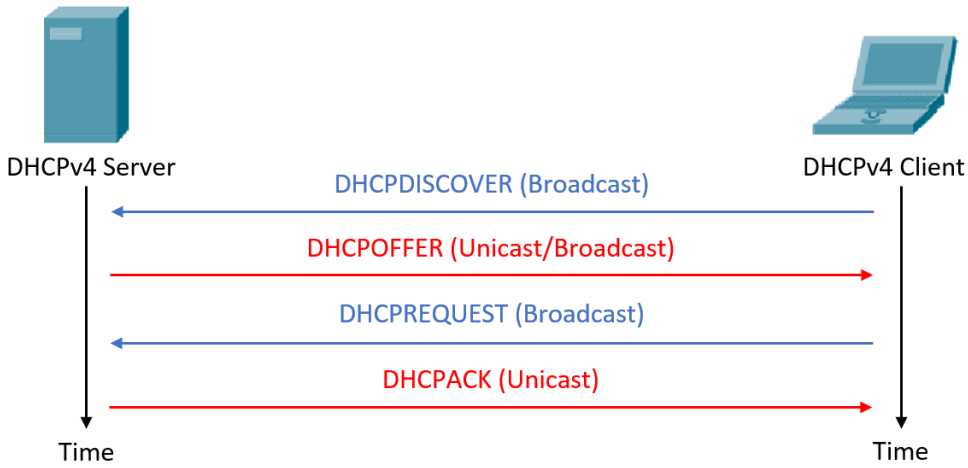
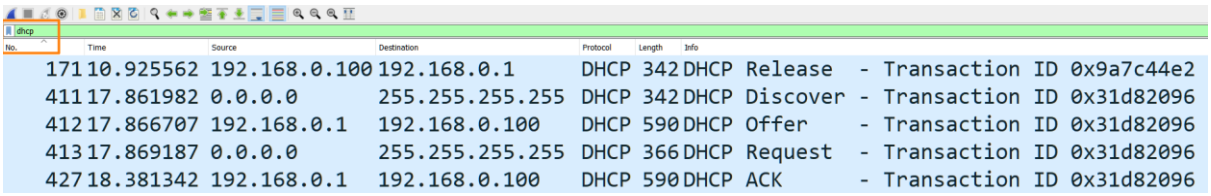


Figura 6.12 *Procesul DHCP*

Secvența anterioară de operații poate fi observată și în Wireshark (Figura 6.13) atunci când se folosesc comenzile **ipconfig /release** și **ipconfig /renew** (pe sistemele de operare Windows) și **dhclient** (pe sisteme de operare Linux):


dhcp

No.	Time	Source	Destination	Protocol	Length	Info
171	10.925562	192.168.0.100	192.168.0.1	DHCP	342	DHCP Release - Transaction ID 0x9a7c44e2
411	17.861982	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x31d82096
412	17.866707	192.168.0.1	192.168.0.100	DHCP	590	DHCP Offer - Transaction ID 0x31d82096
413	17.869187	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x31d82096
427	18.381342	192.168.0.1	192.168.0.100	DHCP	590	DHCP ACK - Transaction ID 0x31d82096

Figura 6.13 *Captura de către Wireshark a procesului DHCP*

3. Desfășurarea lucrării practice

3.1 Discutați aspectele teoretice.

3.2 Vizualizați pachetele DHCP care sunt trimise de către calculatorul local. Pentru aceasta, urmați pași următori:

- Porniți o captură Wireshark
- Aplicați filtru de pachte “dhcp” în fereastra Wireshark
- Deschideți o fereastră de comandă (command promt / terminal)
- Rulați comenzile: **ipconfig /release** și apoi **ipconfig /renew** (pe sistemele de operare Windows) și **dhclient (**pe sistemele de operare Linux)
- Inspectați captura Wireshark care arată secvența de operațiuni DHCP
- În captura Wireshark, identificați adresa de tip broadcast în încapsularea Nivelului 2 (încapsulare Ethernet).

3.3 Considerați topologia de mai jos (Figura 6.14):

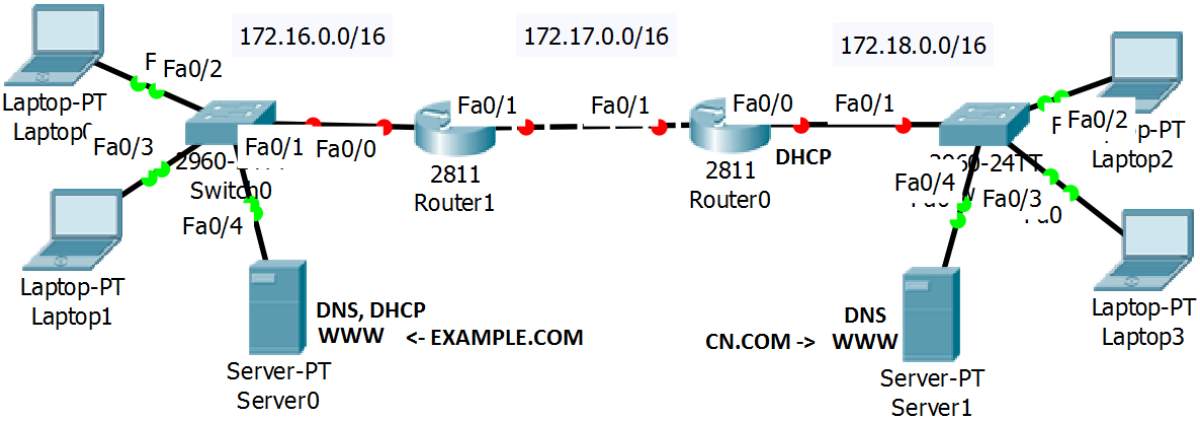


Figura 6.14 *Topologia rețelei de test*

Pas 1: Înainte de a configura dispozitivele de rețea, atribuiți o adresă IP unică și masca de subrețea corespunzătoare fiecărui interfețe de rețea și completați Tabelul 6.1:

Tabelul 6.1 *Adrese IPv4 și măști de rețea pentru rețeaua de testare*

Dispozitiv	Interfață	Adresă IP	Mască de subrețea
Laptop0	Fa	asignat de DHCP	asignat de DHCP
Laptop1	Fa	asignat de DHCP	asignat de DHCP
Server0	Fa	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Router1	Fa0/0	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Router1	Fa0/1	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Router0	Fa0/1	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Router0	Fa0/0	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Laptop2	Fa	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Laptop3	Fa	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Server1	Fa	___ . ___ . ___ . ___	___ . ___ . ___ . ___

Notă*: Acordați atenție numelor interfețelor routerului pe care îl folosiți, deoarece unele routere ar putea avea doar interfețe GigabitEthernet (nu FastEthernet sau Fa).

Pas 2: Atribuiți adrese IPv4 statice interfețelor routerului
Router1>enable
Router1#configure terminal
Router1(config)#interface _____
Router1(config-if)#ip address _____ _____
Router1(config-if)#no shutdown
Router1(config-if)#exit

Pas 3: Configurați DHCP

Tabelul 6.2 de mai jos conține pașii de configurare și comenzile corespunzătoare pentru a configura funcționalitatea DHCP pe un router Cisco:

Tabelul 6.2 *Configurarea funcționalității DHCP pe un router Cisco*

Nr	Operație	Comandă	Exemplu
1	Exclude anumite adrese IP	*Router(config)#ip dhcp excluded-address start_address end_address*	*ip dhcp excluded-address 192.168.0.1 192.168.0.7*
2	Configurează numele pool-ului	*Router(config)# ip dhcp pool name*	*ip dhcp pool TestDHCP*
3	Configurează adresele (specificând adresa rețelei și masca care va fi folosită)	*Router(dhcp-config)# network network-number [mask|prefix-length]*	*network 192.168.0.0 255.255.255.0*
4	Configurează routerul implicit (gateway-ul) pentru clienți	*Router(dhcp-config)# default-router address*	*default-router 192.168.0.1*
5	Configurează adresa IP a serverele de nume de domeniu (DNS) pentru clienți	*Router(dhcp-config)# dns-server address [address2 ...address5]*	*dns-server 8.8.8.8*
6	Vizualizează informațiile despre pool-urile DHCP și legăturile cu adresele DHCP	*Router#show ip dhcp pool*	*show ip dhcp binding*

Pas 4: Configurați rutele statice

Pas 4.1: Identificați ruta statică necesară pe fiecare router completați Tabelul 6.3:

Tabelul 6.3 *Rute statice pentru rețeaua de testare*

Dispozitiv	Adresă destinație	Mască destinație	Următorul hop
Router0	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___
Router1	___ . ___ . ___ . ___	___ . ___ . ___ . ___	___ . ___ . ___ . ___

Pas 4.2: Configurați toate rutele statice pe routerele Cisco

Sintaxă generală: *Router(config)#ip route netw_dest_address next_hop_address/interface*

Exemplu: *Router1(config)#ip route 172.18.0.0 255.255.0.0 172.17.0.2*

Notă: folosiți propriile adrese IP și masca de rețea atunci când configurați dispozitivele, nu pe cele furnizate în acest exemplu*

Vizualizați tabela de rutare:

Router1#show ip route

Pas 5: Testați conectivitatea între dispozitivele gazdă din rețele opuse

a. ping <target IP>

b. tracert <target IP>

Pas opțional: Configurați DHCP și pe Server0, similar cu exemplul din Figura 6.15 (*înlocuiți adresa IP din exemplu cu adresele IP*)

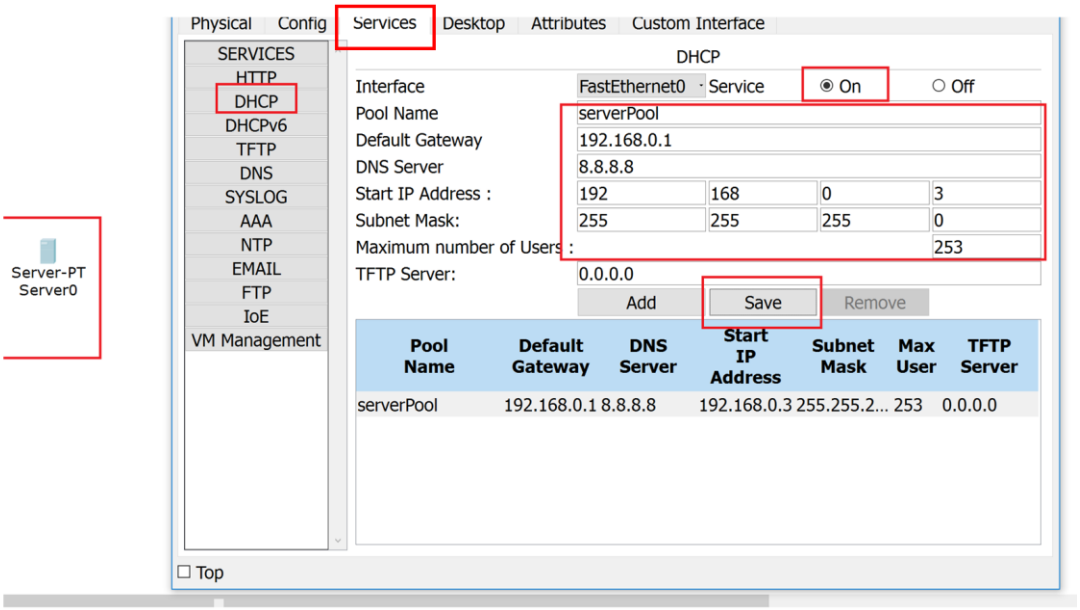


Figura 6.15 *Exemplu de configurare DHCP*

CAPITOLUL 7: NIVELUL REȚEA –IPV6

1. Obiective

La finalul activității practice, cititorii vor fi capabili să: explice caracteristicile protocolului IPv6, să descrie configurația dinamică IPv6, să explice procesul de rutare și să implementeze configurații de rețea IPv6 de bază.

2. Considerații teoretice

Lucrarea practică curentă se concentrează pe stratul de rețea al stivei ISO/OSI (Figura 7.1).

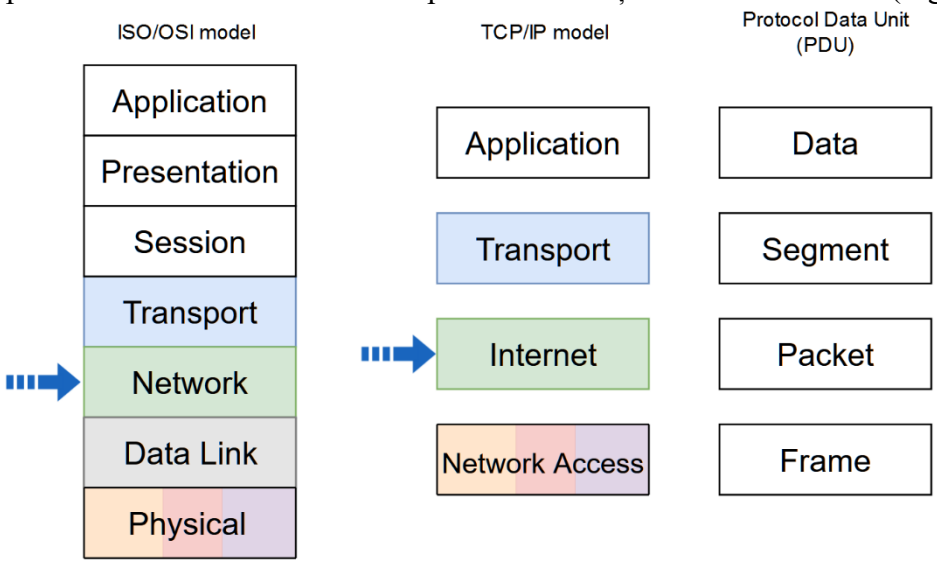


Figura 7.1 *Modelele de stivă de rețea și denumirea PDU (Protocol Data Unit - Unitate de Date la nivelul Protocolului) în fiecare nivel. Săgețile indică nivelurile adresate în activitatea curentă*

2.1 IPv6

IPv6 a fost dezvoltat de către Internet Engineering Task Force (IETF) pentru a depăși limitările IPv4.

Principala limitare a IPv4 este epuizarea adreselor, deoarece cererea de adrese este mai mare decât spațiul de adresare furnizat de cei 32 de biți ai adresei. Soluția pentru epuizarea adreselor IPv4 este adresarea privată și NAT (Network Address Translation). Această soluție, la rândul său, creează mai multe dezavantaje, cum ar fi lipsa conectivității de la un capăt la altul și creșterea complexității rețelei.

IPv6 oferă următoarele îmbunătățiri:

- Spațiul de adresare extins bazat pe adrese de 128 de biți;
- Manipularea pachetelor îmbunătățită datorită antetului simplificat cu mai puține câmpuri;

- Elimină necesitatea de NAT prin eliminarea necesității de adrese private.

Antetul pachetului este prezentat în Figura 7.2:

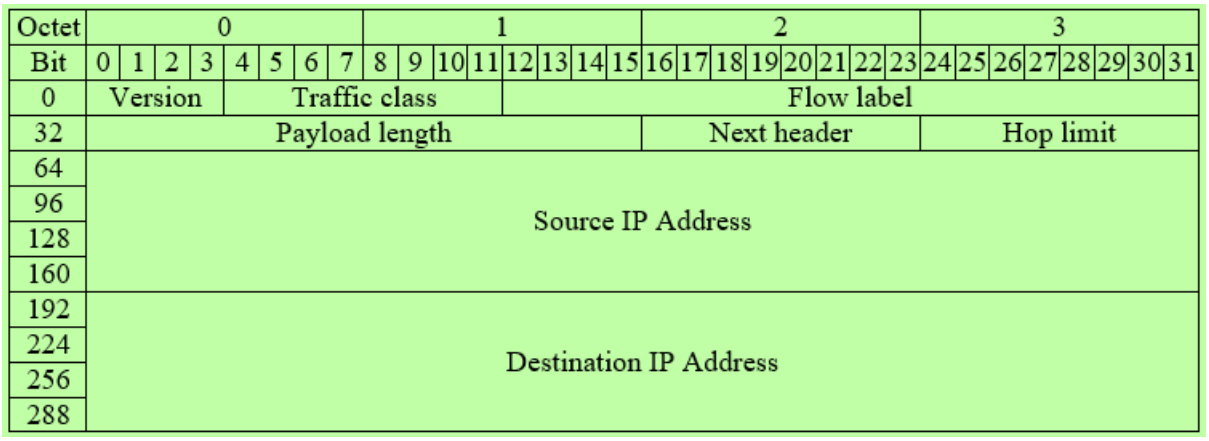


Figura 7.2 *Antetul pachetului IPv6*

- Version / Versiune - campul de versiune, egal cu 6;
- Traffic class / Clasa de trafic - echivalentul pentru DiffServ - câmpul DS;
- Payload length / Lungime încărcătură utilă – indică lungimea pachetului IPv6 (excluzând antetul);
- Next header / Antet următor – definește protocolul nivelului următor;
- Hop limit / Limita de salt – înlocuiește câmpul Time to live de la IPv4;
- Source address / Adresa sursă – adresa IPv4 a expeditorului pachetului;
- Destination address / Adresa destinație – adresa IPv4 a destinatarului pachetului;

Pachetul IPv6 poate conține antete de extensie, plasate între antetul IPv6 și datele utile, furnizând informații opționale la nivel de rețea. Ruterele nu fragmentează pachetele IPv6.

Adresele IPv6 au o lungime de 128 de biți. Formatul preferat pentru scrierea unei adrese IPv6 este x:x:x:x:x:x:x:x, fiecare "x" constând din patru valori hexadecimale, 4 biți fiind reprezentați de o cifră hexazecimală. "Hextet" este un termen neoficial, care se referă la un segment de 16 biți (4 valori în hexazecimal). Figura 7.3 arată un exemplu de adrese IPv6 în formatul preferat:

Tip	**Format**
Preferat	2001:0b20:0000:00d7:0000:0000:0000:0012

Figura 7.3 *Formatul adresei IPv6 pentru scriere - preferat*

Există două reguli pentru a reduce sau comprima reprezentarea IPv6. Prima regulă este să se omitetă zerourile care se află la începutul fiecărui hextet - zero-uri inițiale. (Figura 7.4).

Tip	**Format**
Preferat	2001:0b20:0000:00d7:0000:0000:0000:0012
Fără zerouri inițiale	2001:b20:0:d7:0:0:0:12

Figura 7.4 *Formatul adresei IPv6 pentru scriere - fără zerouri inițiale*

Regula a doua este să se omită segmentele (hextetele) care conțin toți biții 0 și să fie înlocuite cu :: . Această înlocuire poate fi făcută doar o singură dată într-o adresa IPv6. (Figura 7.5).

Tip	**Format**
Preferat	2001:0b20:0000:00d7:0000:0000:0000:0012
Fără zerouri inițiale	2001:b20:0:d7:0:0:0:12
Comprimat	2001:b20:0:d7::12
sau	
Comprimat	2001:b20::d7:0:0:0:12

Figura 7.4 *IPv6 address format for writing – compressed*

Tipuri de adrese IPv6:

- Unicast
  - Identifică în mod unic o interfață
  - Adresa sursă trebuie să fie de tip unicast
- Multicast
  - Este folosit pentru a trimite un singur pachet IPv6 către mai multe destinații
  - IPv6 nu are o adresă de difuzare (broadcast), dar există o adresă de multicasting care oferă același rezultat
  - Adrese multiscat bine cunoscute
    - ff02 :: 1: All IPv6 devices / Toate dispozitivele IPv6
    - ff02 :: 2: All IPv6 routers / Toate routerele IPv6
    - ff02 :: 5: All OSPFv3 routers / Toate routerele OSPFv3
    - ff02 :: a: All EIGRP (IPv6) routers / Toate routerele EIGRP (IPv6)
- Anycast
  - Orice adresă unicast care poate fi asignată la mai multe dispozitive
  - Un pachet trimis către o adresă anycast este rutat către dispozitivul cel mai apropiat cu acea adresă

Lungimea prefixului IPv6 indică porțiunea de rețea a unei adrese IPv6. Este reprezentată în notația cu bară oblică și poate varia între 0 și 128. Lungimea prefixului IPv6 recomandată pentru rețelele LAN este /64. Figura 7.5 prezintă un exemplu de adresă IPv6 și lungime a prefixului: 2001:b20:0:d7::12/64.

Prefix (64 biți)	**ID interfață (64 biți)**
2001:0b20:0000:00d7	0000:0000:0000:0012

Figura 7.5 *Exemplu de adresă IPv6 și lungime a prefixului*

Tipuri de adrese unicat (Figura 7.6):

- Global Unicast Address (GUA) / Adresă Globală Unicast
  - Unică la nivel global
  - Rutabilă pe Internet
  - Similara cu adresa IPv4 publică
- Link-local Address (LLA) / Adresă locală de legătură
  - Necesar pentru fiecare dispozitiv activat pentru IPv6
  - Creată chiar dacă dispozitivul nu a primit o adresă globală unicast

- Pentru comunicare cu alte dispozitive de pe aceeași legătură locală
- Permite dispozitivelor să comunice doar pe aceeași legătură
- Unice doar în cadrul legăturii locale
- Nu sunt rutabile pe internet
- Ele se află în intervalul FE80::/10
- Adresa locală a legăturii routerului este de obicei folosită ca gateway implicit

- Unique Local Address (ULA) / Adresă Locală Unică
  - Adresare locală în cadrul unui site sau între un număr limitat de site-uri.

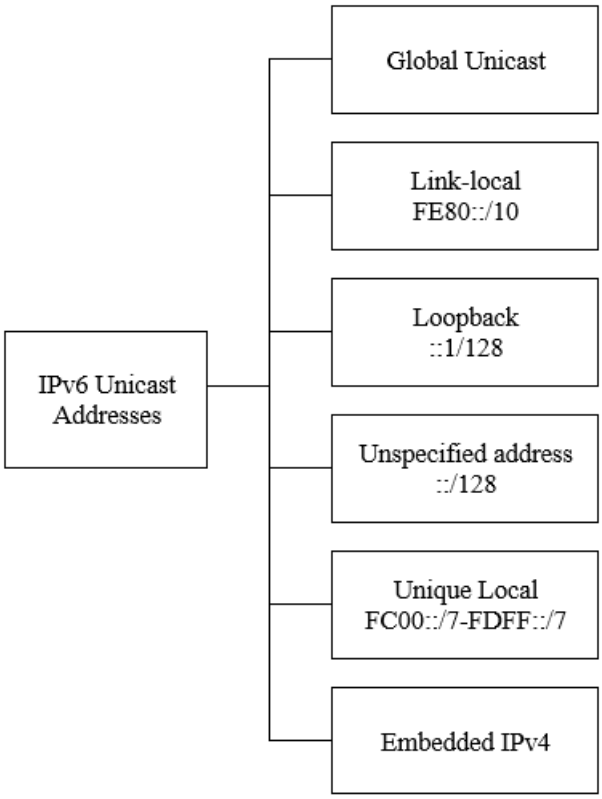


Figura 7.6 *Tipuri de adrese unicast*

- Structura adreselor unicast globale (GUA):
  - Prefixul global de rutare
    - Rețea
    - Porțiunea de adresă atribuită de furnizor
    - Tipic /48
  - ID Subnet
    - Pentru subnetare într-o organizație
    - Tipic, 16 biți
  - ID Interfață
    - Echivalentul porțiunii gazdă a unei adrese IPv4
    - Tipic, 64 biți

Figura 7.7 arată un exemplu de adresă IPv6 globală unică: 2001:b20:0:d7::12/64

Prefixul global de rutare	ID Subnet	ID Interfață
2001:0b20:0000	00d7	0000:0000:0000:0012

Figura 7.7 *Exemplu de adresă globală unicast IPv6*

2.2 Configurarea dispozitivelor gazdă

Metode posibile:

- Static
  - Configurare manuală a adresei IPv6
- Dinamic
  - Autoconfigurare fără stare a adreselor (SLAAC)
  - DHCPv6 cu stare

Un dispozitiv obține informațiile de adresare IPv6 dinamic, prin intermediul mesajelor Internet Control Message Protocol version 6 (ICMPv6). Ruterele IPv6 trimit periodic mesaje ICMPv6 de Anunțare a Ruterului (Router Advertisement - RA) către toate dispozitivele activate pentru IPv6 din rețea. Un mesaj RA va fi, de asemenea, trimis în răspuns la un dispozitiv care trimite un mesaj ICMPv6 de solicitare a ruterului (Router Solicitation- RS), care este o cerere pentru un mesaj RA.

Mesajul ICMPv6 RA este o sugestie către dispozitive cu privire la modul de obținere a informațiilor de adresare IPv6. Mesajul ICMPv6 RA include următoarele:

- Prefixul rețelei și lungimea prefixului
- Adresa gateway-ului implicit
- Adresele și numele de domeniu DNS

Există trei metode pentru mesajele RA:

- Metoda 1: SLAAC - prefix, lungimea prefixului și adresa gateway implicită
- Metoda 2: SLAAC cu un server DHCPv6 fără stare - informații parțiale, restul informațiilor, cum ar fi adresele DNS, trebuie să fie obținute de la un server DHCPv6 fără stare
- Metoda 3: DHCPv6 cu stare (fără SLAAC) - adresa gateway implicită, restul informațiilor trebuie să fie obținute de la un server DHCPv6 cu stare

Decizia privind modul în care un client va obține informații despre adresarea IPv6 depinde de setările din mesajul RA. Un mesaj ICMPv6 RA include trei indicatoare pentru a identifica opțiunile dinamice disponibile pentru un dispozitiv gazdă, după cum urmează::

- Indicator A - Indicator de configurare automată a adresei. Utilizează Configurarea Automată a Adresei fără Stare (SLAAC) pentru a crea o adresă IPv6 GUA.
- Indicator O – Indicator de configurare Other. Alte informații sunt disponibile de la un server DHCPv6 fără stare.
- Indicator M- Indicator de configurare a adreselor gestionate (Managed). Utilizează un server DHCPv6 cu stare pentru a obține o adresă IPv6 GUA.

- Metoda 1 – SLAAC (Figura 7.8)

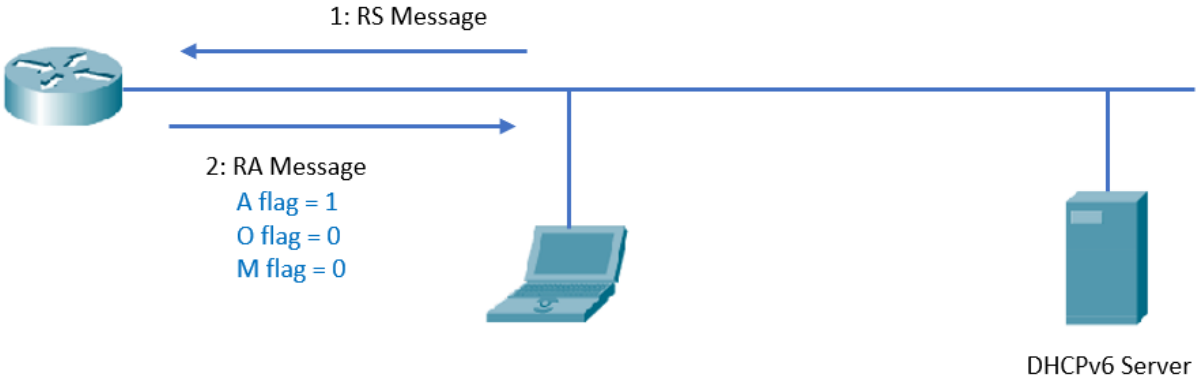


Figura 7.8 Proces *SLAAC*

- Metoda 2 - SLAAC cu un server DHCPv6 fără stare (Figura 7.9)

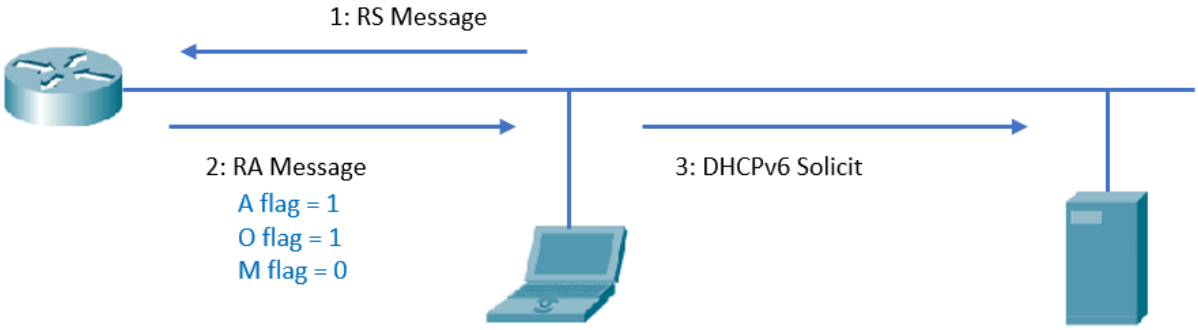


Figura 7.9 *Proces* SLAAC cu server DHCPv6 fără stare

- Metoda 3 - DHCPv6 cu stare (fără SLAAC) (Figura 7.10)

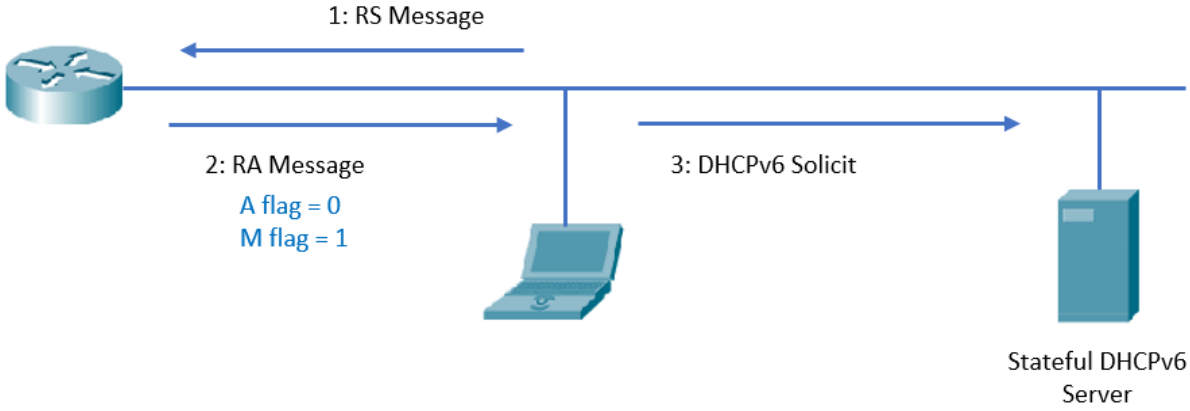


Figura 7.10 *Proces DHCPv6 cu stare*

3. Desfăşurarea lucrării practice

3.1 Discutați aspectele teoretice.

3.2 Considerați topologia rețelei de mai jos (Figura 7.11):

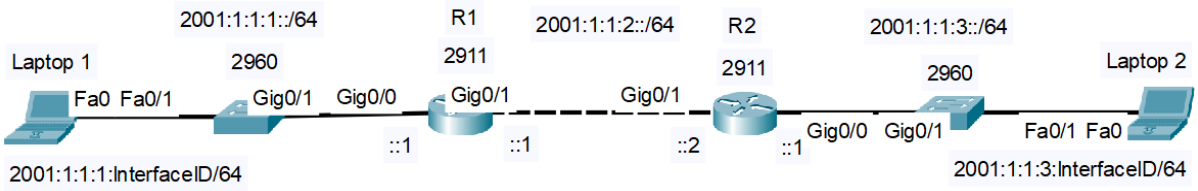


Figura 7.11 *Topologia rețelei de test*

Pas 1: Înainte de configurarea dispozitivelor de rețea, discutați asignarea adreselor IPv6 în Tabelul 7.1:

Tabel 7.1 *Adresele IPv6 pentru rețeaua de test*

Dispozitiv	Interfață	Adresă IPv6
Laptop 1	Fa0	DHCPv6
Laptop 2	Fa0	DHCPv6
R1	Gig0/0	2001:1:1:1::1/64 fe80::1 link-local
R1	Gig0/1	2001:1:1:2::1/64
R2	Gig0/1	2001:1:1:2::2/64 fe80::2 link-local
R2	Gig0/0	2001:1:1:3::1/64

Observație*: acordați atenție numelor interfețelor routerului pe care îl utilizați, deoarece unele routere ar putea avea doar interfețe FastEthernet.

Pas 2: Atribuiți nume routerului, activați rutarea IPv6 și atribuiți adrese IPv6 statice interfețelor routerului.

Example:

R1>enable
R1#conFigura terminal
Router(config)#hostname R1
R1(config)#ipv6 unicast-routing

R1(config)# interface gigabitEthernet 0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#ipv6 address 2001:1:1:1::1/64
R1(config-if)#no shutdown

Utilizați următoarea comandă pentru a afișa adresele IPv6 configurate pe router:

R1#show ipv6 interface brief

Pas 3: Configurați o rută statică pe fiecare router îndreptată către adresa IPv6 a interfeței Gig0/1 de pe celălalt router. Pentru routerul R1, specificați adresa LLA pentru următorul hop, iar pentru routerul R2 specificați adresa GUA pentru următorul hop. Discutați diferențele!

R1(config)#ipv6 route 2001:1:1:3::/64 GigabitEthernet0/1 FE80::2
R2(config)# ipv6 route 2001:1:1:1::/64 2001:1:1:2::1

Utilizați următoarea comandă pentru a afișa tabele de rutare IPv6:

Router#show ipv6 route

Pas 4: Verificați asignările de adrese prin SLAAC (Figura 7.12 și 7.13).

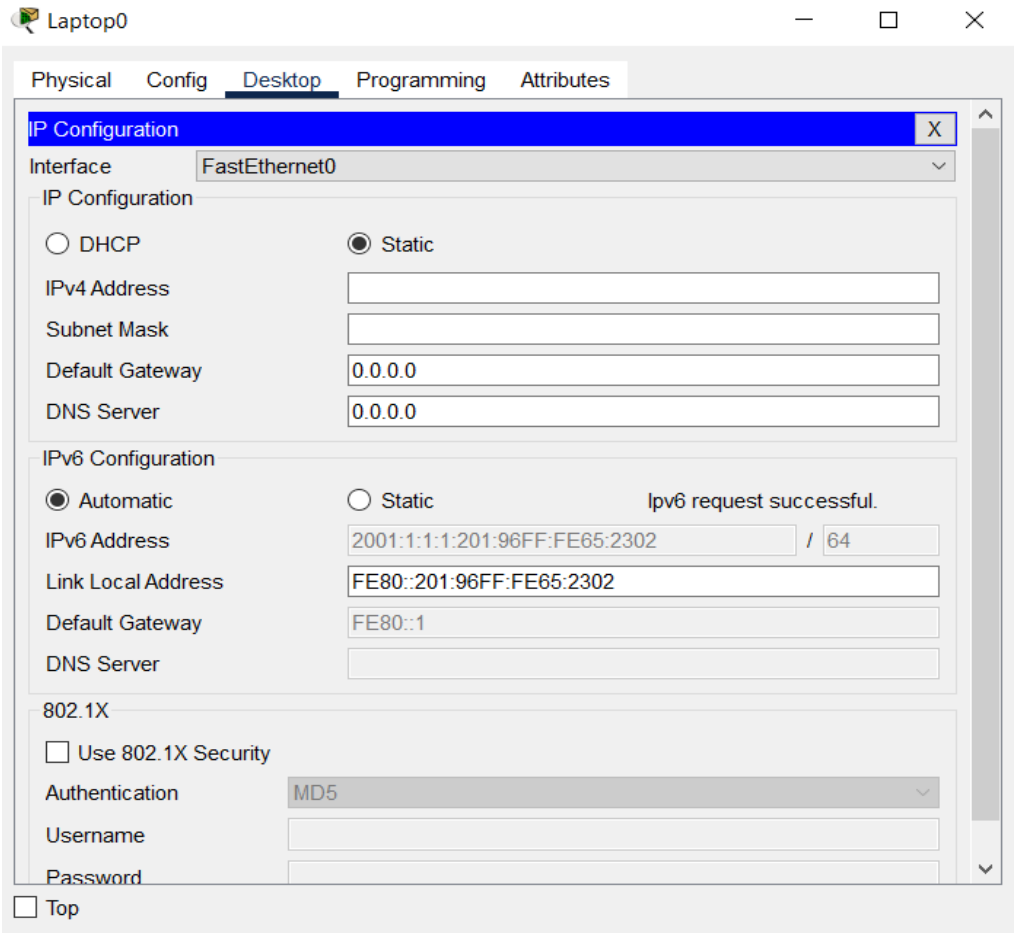


Figura 7.12 *Vizualizare configurație IP - GUI*

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0001.9665.2302
   Link-local IPv6 Address.........: FE80::201:96FF:FE65:2302
   IPv6 Address....................: 2001:1:1:1:201:96FF:FE65:2302
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: FE80::1
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-23-BA-17-8B-00-01-96-65-23-02
   DNS Servers.....................: ::
                                     0.0.0.0
```

Figura 7.13 *Vizualizare configurație IP - CLI*

Pas 5: Testați conectivitatea între dispozitive din rețele opuse. (Figura 7.14).

a. *ping <target IP>*
b. *tracert <target IP>*

```
C:\>ping 2001:1:1:3:2D0:BAFF:FE66:228A

Pinging 2001:1:1:3:2D0:BAFF:FE66:228A with 32 bytes of data:

Reply from 2001:1:1:3:2D0:BAFF:FE66:228A: bytes=32 time<1ms TTL=126
Reply from 2001:1:1:3:2D0:BAFF:FE66:228A: bytes=32 time<1ms TTL=126
Reply from 2001:1:1:3:2D0:BAFF:FE66:228A: bytes=32 time<1ms TTL=126
Reply from 2001:1:1:3:2D0:BAFF:FE66:228A: bytes=32 time<1ms TTL=126

Ping statistics for 2001:1:1:3:2D0:BAFF:FE66:228A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>tracert 2001:1:1:3:2D0:BAFF:FE66:228A

Tracing route to 2001:1:1:3:2D0:BAFF:FE66:228A over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      2001:1:1:1::1
  2    0 ms      0 ms      0 ms      2001:1:1:2::2
  3    0 ms      10 ms     0 ms      2001:1:1:3:2D0:BAFF:FE66:228A

Trace complete.
```

Figura 7.14 *Comenzi de testare a conectivității*

Pas 6: Înlocuiți rutele statice configurate cu rute implicite și testați conectivitatea între dispozitivele de la capetele opuse ale rețelelor. În IPv6, ruta implicită este ::/0.

R1(config)#no ipv6 route 2001:1:1:3::/64 GigabitEthernet0/1 FE80::2
R2(config)#no ipv6 route 2001:1:1:1::/64 2001:1:1:2::1

R1(config)#ipv6 route ::/0 _____
R2(config)#ipv6 route ::/0 _____

Pas 7: Configurați routerul R1 pentru a oferi DHCPv6 fără stare pentru Laptopul 1.

R1(config)#ipv6 dhcp pool R1_NET1
R1(config-dhcpv6)#dns-server 2001:1:1:1::F
R1(config-dhcpv6)#domain-name NET1.com
R1(config-dhcpv6)#exit
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ipv6 nd other-config-flag
R1(config-if)#ipv6 dhcp server R1_NET1

Pas 8: Verificați atribuirea adreselor prin DHCPv6 fără stare (Figura 7.15 și 7.16).

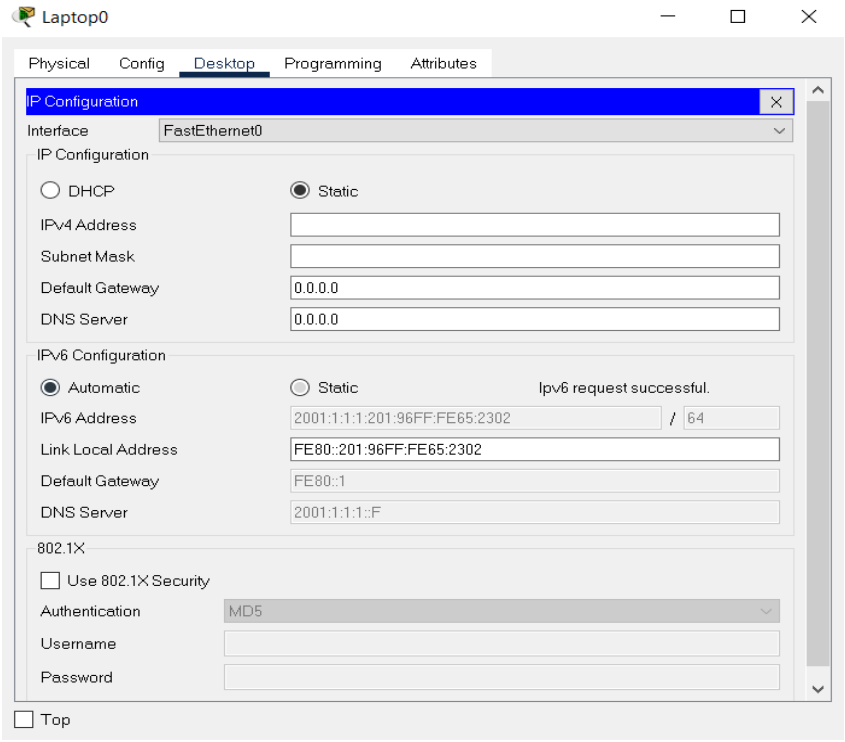


Figura 7.15 *Vizualizare configurație IP - GUI*

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: NET1.com
   Physical Address................: 0001.9665.2302
   Link-local IPv6 Address.........: FE80::201:96FF:FE65:2302
   IPv6 Address....................: 2001:1:1:1:201:96FF:FE65:2302
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: FE80::1
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................: 2061700019
   DHCPv6 Client DUID..............: 00-01-00-01-23-BA-17-8B-00-01-96-65-23-02
   DNS Servers.....................: 2001:1:1:1::F
                                     0.0.0.0
```

Figura 7.16 *Vizualizare configurație IP - CLI*

Pas 9: Configurați routerul R2 pentru a oferi DHCPv6 cu stare pentru Laptopul 2.

R2(config)#ipv6 dhcp pool R2_NET3
R2(config-dhcpv6)# address prefix 2001:1:1:3::/64
R2(config-dhcpv6)#dns-server 2001:1:1:3::A
R2(config-dhcpv6)#domain-name NET3.com
R2(config-dhcpv6)#exit
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ipv6 nd managed-config-flag
R2(config-if)#ipv6 dhcp server R2_NET3

Pas 10: Verificați atribuirea adreselor prin DHCPv6 cu stare (Figura 7.17 și 7.18).

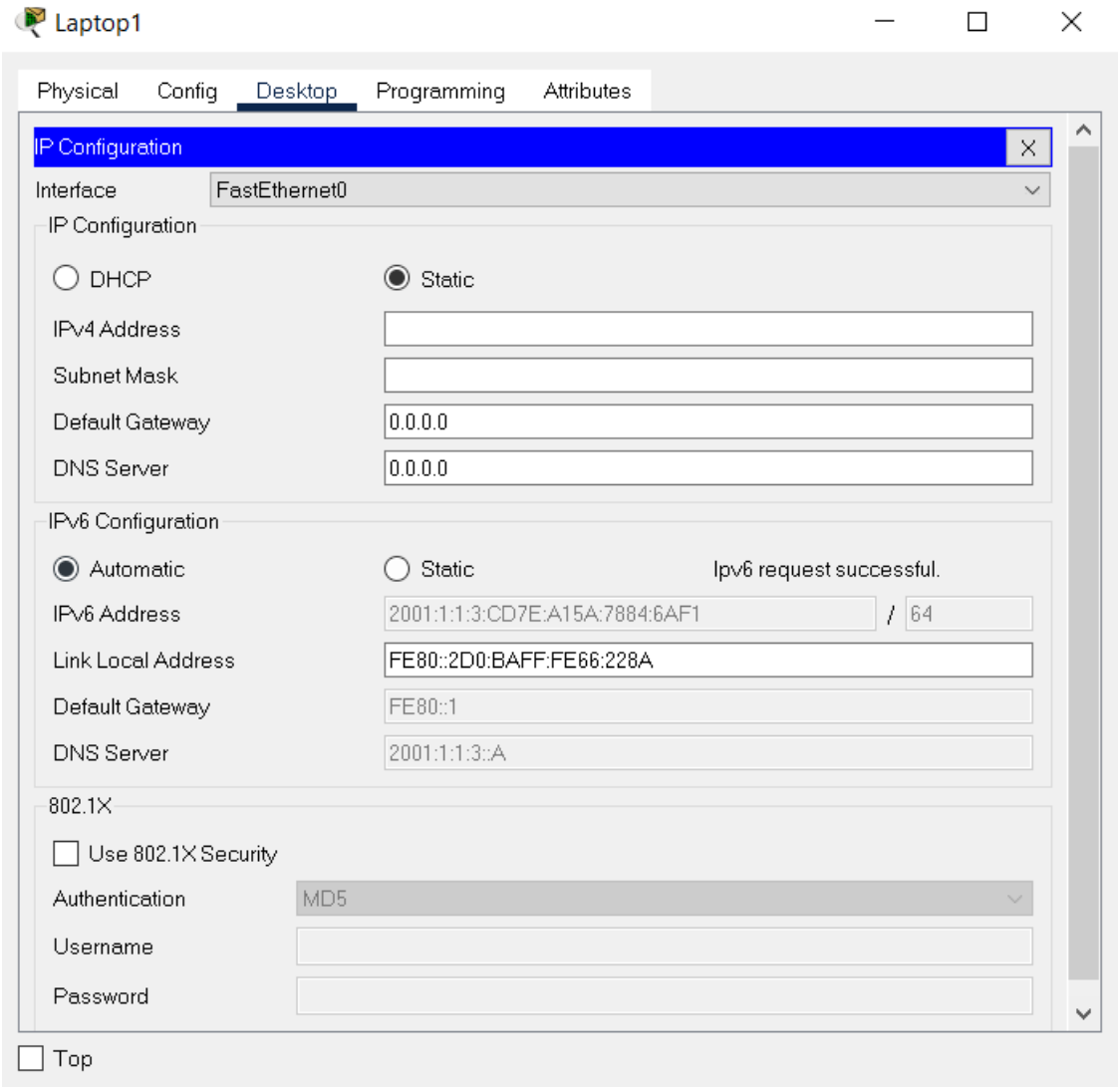


Figura 7.17 *Vizualizare configurație IP - GUI*

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: NET3.com
   Physical Address................: 00D0.BA66.228A
   Link-local IPv6 Address.........: FE80::2D0:BAFF:FE66:228A
   IPv6 Address....................: 2001:1:1:3:CD7E:A15A:7884:6AF1
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: FE80::1
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................: 1998122365
   DHCPv6 Client DUID..............: 00-01-00-01-40-4C-51-2B-00-D0-BA-66-22-8A
   DNS Servers.....................: 2001:1:1:3::A
                                     0.0.0.0
```

Figura 7.18 *Vizualizare configurație IP - CLI*

Pas 11: Testați conectivitatea dintre dispozitivele din rețele opuse.

a. *ping <target IP>*

b. *tracert <target IP>*

CAPITOLUL 8: NIVELUL APLICAȚIE: PROGRAMARE ÎN REȚEA UTILIZÂND SOCKET-URI

1. Obiective

Precondiție: Utilizați un mediu de lucru funcțional pentru limbajul de programare preferat (Java, C#, Python, C/C++, etc.)

La finalul activității, cititorii vor putea să scrie software pentru aplicații de socket-uri și să depaneze aplicații de rețea folosind Wireshark.

2. Considerații teoretice

Lucrările practice curente se concentrează pe nivelurile de Transport și de Aplicație ale stivei de protocoale ISO/OSI. (Figura 8.1).

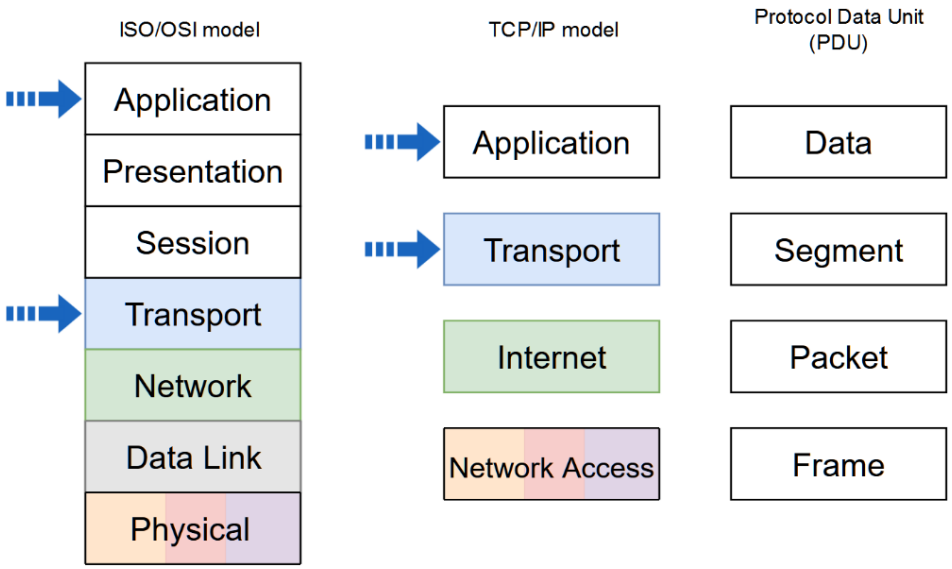


Figura 8.1 *Modelele de stivă de rețea și denumirea PDU (Protocol Data Unit - Unitate de Date la nivelul Protocolului) în fiecare nivel. Săgețile indică nivelurile adresate în activitatea curentă*

Această activitate practică abordează partea de programare din ingineria software și a comunicațiilor prin utilizarea socket-urilor de rețea într-un mediu desktop. Programarea socket-urilor este disponibilă în orice limbaj de programare de nivel înalt, iar socket-urile transmit informații la Nivelul Aplicației. Socket-urile sunt utilizate în diferite tipuri de aplicații, precum: Client-Server, sisteme peer-2-peer, comunicare inter-proces (pe aceeași mașină).

Socket-urile de rețea pot fi construite pentru a folosi atât adrese IPv4, cât și IPv6. Un socket este combinația unei adrese IP și a unui număr de port și se utilizează într-o aplicație de rețea. O aplicație de rețea furnizează conectivitate între diferite dispozitive de rețea. Nu este posibil să legați un socket la un port care este deja folosit de către o altă aplicație, totuși același port poate fi folosit concurent de protocoalele de nivel transport TCP și UDP. Adresele IP identifică

dispozitivul de rețea, dar numărul portului identifică în mod unic fiecare aplicație în executare pe dispozitivul de rețea curent.

Operațiile pe care o aplicație le poate efectua pe un socket sunt următoarele:

- **Create** - Crearea unui obiect de tip socket
- **Bind** - Configurarea obiectului de tip socket pentru a folosi o pereche locală de adresă IP și număr de port pentru a accepta conexiuni
- **Listen** - Programarea socket-ului pentru a aștepta conexiuni de intrare
- **Accept** - Acceptarea conexiunii de intrare
- **Connect** - Această operație este folosită de un client care dorește să se conecteze la un server
- **Send** - Folosit pentru a trimite date prin socket către destinația remote
- **Receive** - Folosit pentru a primi date trimise dintr-o locație remote
- **Close** - Închiderea conexiunii între cele două socket-uri

2.1. Lucrul cu socket-uri pe mașina locală

- Pentru a simula o rețea pe mașina locală, întregul interval disponibil de IP de tip loopback (127.0.0.0 - 127.255.255.255) poate fi folosit. Interfața de rețea loopback este disponibilă doar pe dispozitivul gazdă local și este folosită în principal pentru diagnosticare și aplicații de rețea independente. Prin urmare, o rețea locală simulată poate folosi aceste adrese IP pentru comunicare. Pentru a testa și confirma că acest interval poate fi folosit, poate fi rulată o comandă ping de la terminalul local pentru a verifica conectivitatea la aceste adrese IP (Figura 8.2):

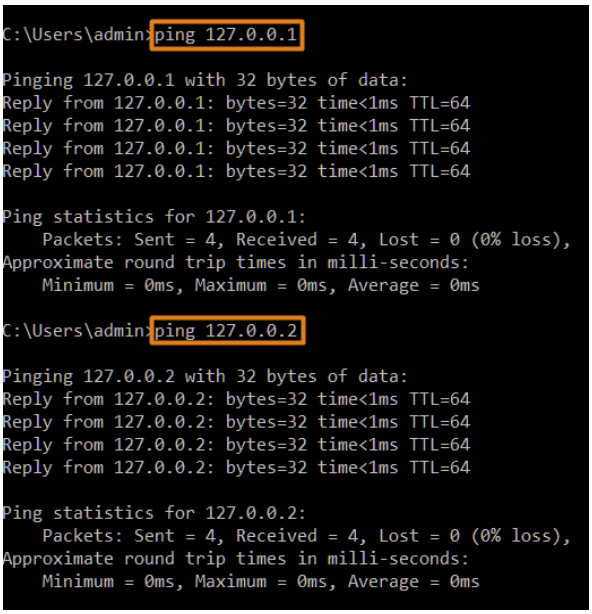


Figura 8.2 *Testarea adresării loopback*

- De asemenea, este posibil să atribuiți mai multe adrese IP valide pe interfața locală, dar acest lucru trebuie făcut manual prin alocarea statică a adreselor IP interfeței. În acest

caz, rularea comenzii **ipconfig** arată toate adresele IP atribuite aceleiași interfețe. Vezi un exemplu mai jos (Figura 8.3):

```
Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fce4:5011:a37b:f929%22
   IPv4 Address. . . . . . . . . . . : 10.0.0.1
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   IPv4 Address. . . . . . . . . . . : 10.0.0.2
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   IPv4 Address. . . . . . . . . . . : 20.0.0.1
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   IPv4 Address. . . . . . . . . . . : 20.0.0.2
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   IPv4 Address. . . . . . . . . . . : 30.0.0.1
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   IPv4 Address. . . . . . . . . . . : 30.0.0.2
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   IPv4 Address. . . . . . . . . . . : 172.16.0.1
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   IPv4 Address. . . . . . . . . . . : 172.16.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   IPv4 Address. . . . . . . . . . . : 172.16.0.3
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   IPv4 Address. . . . . . . . . . . : 192.168.0.35
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::8f3:92ff:fe9b:5d34%22
```

Figura 8.3 *Vizualizarea configurației IP - CLI*

- După ce au fost atribuite adresele IP, acum pot fi create socket-uri pentru a utiliza aceste adrese IP.

2.2. Socket-uri TCP

- Socket-urile TCP (Transmission Control Protocol) sunt orientate pe conexiune și reprezintă un mecanism de transmitere a datelor fiabil care permite ca datele să fie primite și procesate în aceeași ordine în care au fost transmise.

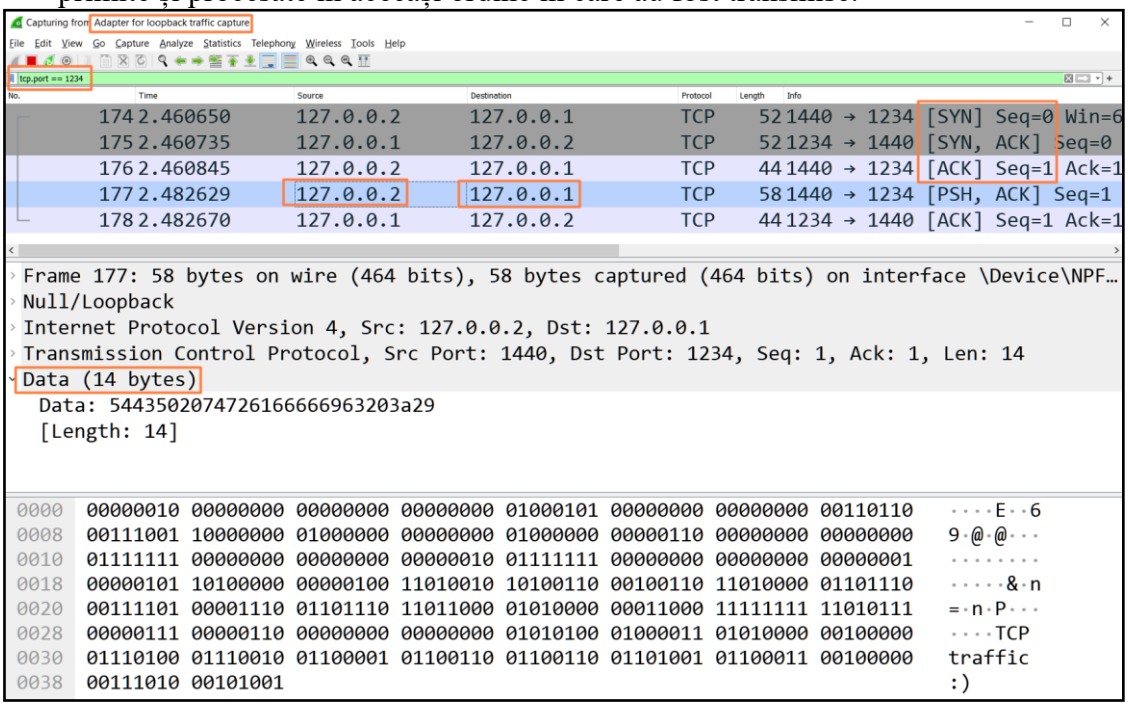


Figura 8.4 *Captura Wireshark pentru comunicație prin socket-uri TCP*

- Figura 8.4 arată o captură de trafic Wireshark pe interfața pentru capturarea traficului pe interfața de rețea loopback. Captura de ecran arată o comunicare client-server prin socket-uri folosind adresele loopback. Filtrul aplicat este **tcp.port == 1234**. Serverul este legat de adresa 127.0.0.1 și așteaptă conexiuni pe portul 1234, în timp ce clientul este legat de adresa 127.0.0.2, trimitând 14 octeți de date către server.
- Captura de ecran evidențiază mecanismul TCP reprezentat de pachetele de confirmare (ACK). Primele trei schimburi de pachete (Figura 8.4) reprezintă strângerea de mână în trei pași (3-way handshake), necesară pentru stabilirea conexiunii pentru orice conexiune TCP (Figura 8.5), iar mai apoi este vizibil pachetul care trimite datele - încărcătura utilă. Această strângere de mână asigură că ambele gazde doresc să comunice și recunosc intenția celeilalte gazde de a comunica.

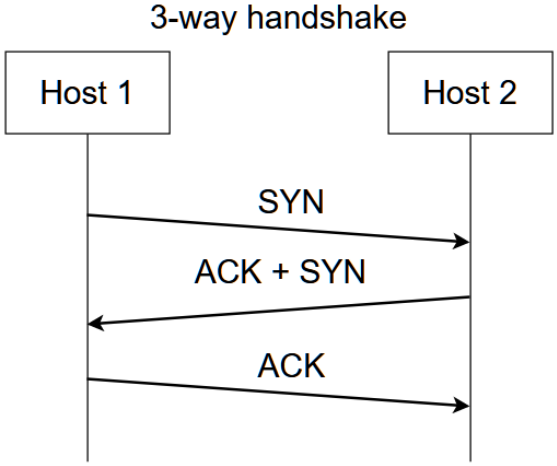


Figura 8.5 *TCP 3-way handshake*

- Imaginea Wireshark arată o comunicare socket care rămâne deschisă.
    - Răspundeți la următoarea întrebare în timp ce lucrați la activitatea practică: Dacă conexiunea socket-ului este închisă, care sunt indicatoarele TCP (TCP flags) care sunt setate pentru a închide conexiunea?

2.3. Socket-uri UDP

- În contrast cu socket-urile TCP, socket-urile UDP (User Datagram Protocol) nu sunt orientate spre conexiune și nu furnizează comunicare fiabilă. Acest lucru înseamnă că nu garantează că pachetele de rețea sunt livrate la destinație. Figura 8.6 reprezintă o captură Wireshark (din nou, capturarea traficului pe interfața de rețea loopback) a unei comunicări UDP între două gazde. Filtrul aplicat este **udp.port == 1234**. După cum se poate observa, nu există o metodă de stabilire a conexiunii și nu sunt transmise niciun fel de pachete ACK.

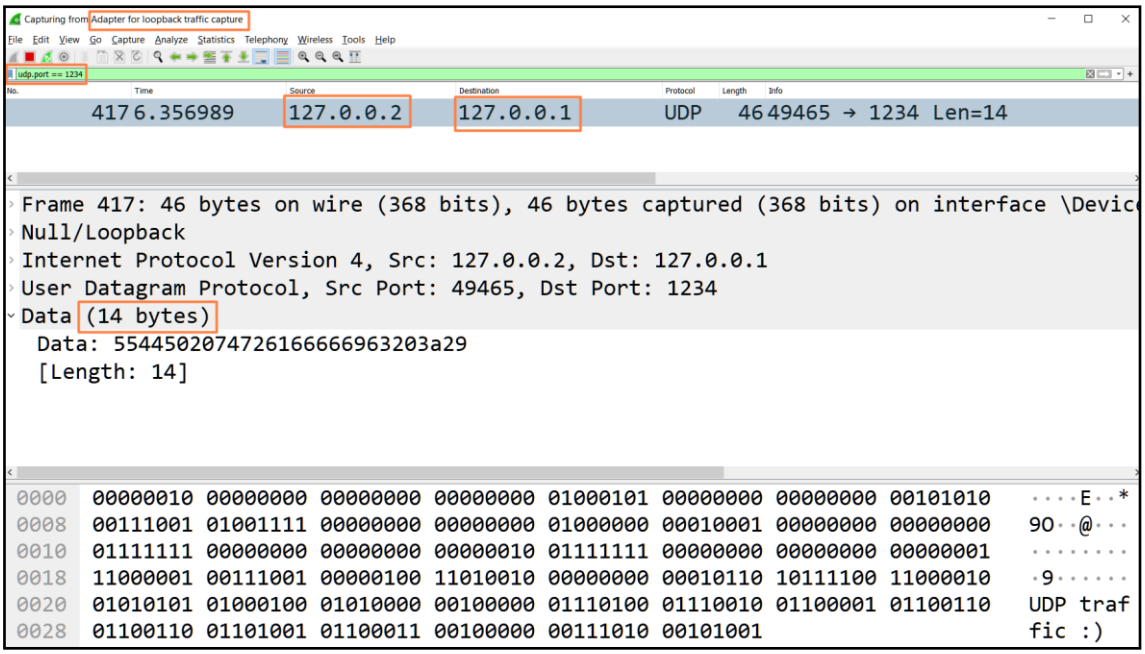
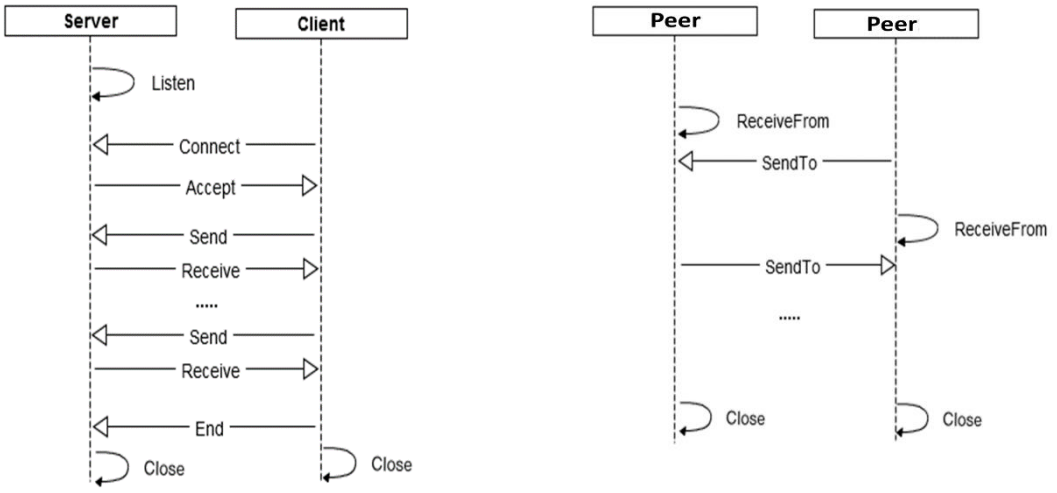


Figura 8.6 *Captura Wireshark pentru comunicație prin socket-uri UDP*

Comunicația prin socket-uri TCP și UDP sunt prezentate în Figura 8.7 a și b.



a. Comunicație prin socket TCP b. Comunicație prin socket UDP

Figura 8.7 *Comunicare prin socket-uri*

1. Șablon de implementare

- Un dispozitiv de rețea poate funcționa în 3 moduri:
  - **Server:** Dispozitiv care recepționează
  - **Client:** Dispozitiv care trimite
  - **Releu (Relay):** Acționând ca un nod intermediar în comunicare și acționează atât ca dispozitiv de trimitere, cât și de recepție. Acest tip de nod de rețea poate fi întâlnit în Rețelele de Senzori Fără Fir (WSN) unde nu toate nodurile senzor

sunt în raza wireless a dispozitivului colector, prin urmare unele noduri trebuie să transmită informațiile către nodul destinatar (nodul colector).

- Acest subcapitol oferă un șablon pentru implementarea nodului de comunicare releu folosind concepte OOP (șablonul este scris în pseudocod, nu într-un limbaj de programare anume). Aceasta nu este singura posibilitate de organizare a codului, cititorii pot alege orice metodologie de proiectare a software-ului cu care se simt confortabili.

Relay node implementation template

```
class RelayNode {
public:
   RelayNode(IPAddress, serverPortNr) {
      m_server.listen(IPAddress, serverPortNr);
      m_client.bind(IPAddress);

      m_server.onReceive() => {
         ByteArray receivedData = m_server.readData();
         m_client.connectToHost(m_nextHopIpAddress, m_nextHopPortNr);
         m_client.sendData(receivedData);
         m_client.close();
      }
   }
   void setNextHopInformation(nextHopIPAddress, nextHopServerPortNr) {
      m_nextHopIpAddress = nextHopIPAddress;
      m_nextHopPortNr= nextHopServerPortNr;
   }

private:
   Server m_server; // server instance accepting connections
   Client m_client; // client instance sending data to the next hop
   IPAddress m_nextHopIpAddress; // next hop address used by the client instance
   int m_nextHopPortNr; // next hop port nr used by the client instance
}
void main() {
   RelayNode relay(127.0.0.1, 1234);
   relay.setNextHopInformation(127.0.0.2, 2345)
   …
   // run application event loop
}
```

3. Desfăşurarea lucrării practice

- Fiecare student îi va fi asignată una dintre topologiile de mai jos și scenariul de simulare trebuie implementat în software.
- În afară de constrângerile impuse de fiecare scenariu de simulare, sarcinile comune pentru fiecare implementare sunt următoarele:
    - Folosiți un limbaj de programare la alegere pentru a implementa simularea rețelei

- Folosiți intervalul de adrese pentru buclă locală (loopback) pentru adresare: 127.0.0.0 – 127.255.255.255
- Testați implementarea folosind Wireshark
- Livrați implementarea (codul sursă sau link către un depozit de cod versiune online - code versioning repository)
- Prezentați o captură Wireshark pentru a dovedi comunicarea între diferitele adrese IP
- Inspectați raportul dintre totalul încărcăturii livrate comparativ cu traficul de nivel de aplicație relevant / raportul dintre lungimea totală a pachetului (antete și date) în comparație cu lungimea datelor trimise (folosiți statistici Wireshark sau inspecție manuală a pachetelor)
- În funcție de simularea implementată, cercetați antetele pentru protocoalele TCP și/sau UDP. Utilizând Wireshark, identificați elementele antetului în traficul capturat.

3.1 Comunicare în Inel (Ring Comunication)

- Trei calculatoare comunică într-o singură direcție creând o buclă (Figura 8.8)
- Unul dintre calculatoare inițiază comunicarea trimițând valoarea '1'
- La primire, fiecare dispozitiv de rețea incrementează valoarea primită și o trimite către dispozitivul următor
- Comunicarea se încheie când încărcătura livrată atinge valoarea '100'
- Sugestii de implementare:
    - Implementați o singură clasă care este instanțiată de 3 ori cu diferiți parametri de comunicare (reutilizați codul și nu-l duplicați pentru fiecare instanță)
    - Toată comunicarea folosește socket-uri TCP (opțional)

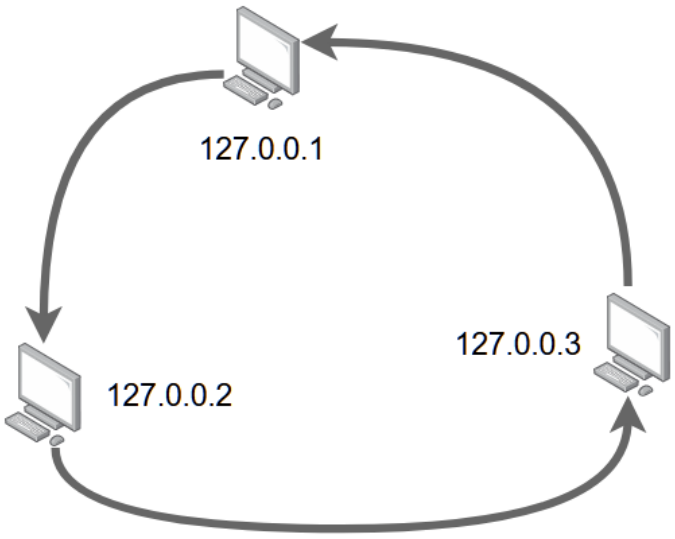


Figura 8.8 *Topologia rețelei pentru comunicație în inel*

3.2 Selector de noduri (Node selector)

- Există trei noduri în topologie: N1, N2, N3 (Figura 8.9)
- N1 crește o valoare de 100 de ori și după fiecare incrementare trimite valoarea fie către N2 sau către N3, noduri care sunt selectate aleatoriu pentru transmitere
- Când N2 primește o valoare întreagă care este un multiplu de 3, va trimite înapoi un pachet ACK către N1
- Când N3 primește o valoare întreagă care este un multiplu de 5, va trimite înapoi un pachet ACK către N1
- Sugestii de implementare:
    - Implementați o singură clasă pentru N2 și N3 care este instanțiată cu diferiți parametri de comunicare (reutilizați codul și nu-l duplicați pentru fiecare instanță)
    - Toată comunicarea folosește socket-uri UDP (opțional)

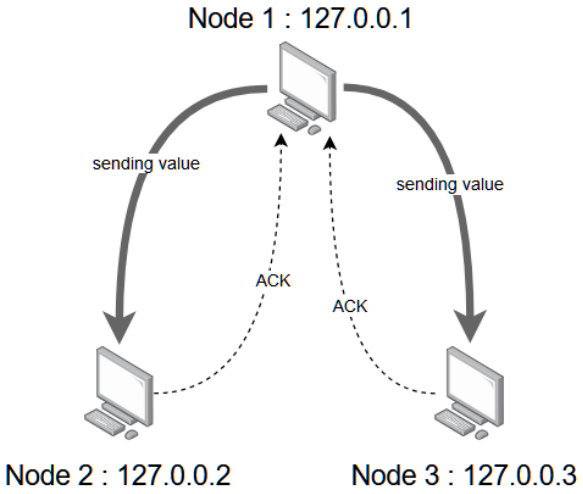


Figura 8.9 *Topologia rețelei pentru selector de noduri*

3.3 Noduri Releu (Relay Nodes)

- În topologie există patru noduri (Figura 8.10): Expeditorul și trei destinații posibile (D1, D2 și D3).
- Nodul Expeditor transmite 100 de pachete, conținând un număr întreg aleator, către una dintre cele 3 destinații posibile (D1, D2 sau D3).
- După fiecare transmitere a pachetului, numărul întreg este incrementat.

  Fiecare nod poate trimite date doar către următorul hop la care este conectat, prin urmare, un pachet de la Expeditor către D3 trebuie să treacă prin D1 și D2.

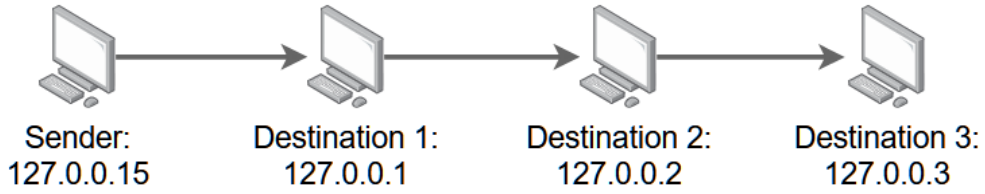


Figura 8.10 *Topologia rețelei pentru noduri releu*

- Sugestii de implementare:
  - Datele utile care sunt transmise prin socket trebuie să conțină adresa IP destinație, astfel că datele au următorul format (Figura 8.11):

Adresa IP țintă	**Valoare**

Figura 8.11 *Formatul datelor utile transmise*

  - De fiecare dată când un nod primește un pachet, acesta verifică dacă adresa IP destinație a datelor utile primite este aceeași cu adresa IP curentă a nodului. Dacă este identică, comunicarea se oprește aici, în caz contrar datele sunt trimise mai departe la următorul salt.
  - Implementați o singură clasă pentru D1, D2 și D3, care este instanțiată cu diferiți parametri de comunicare (reutilizați codul și nu-l duplicați pentru fiecare instanță).

CAPITOLUL 9: ETHERNET, ARP ȘI NDP

1. Obiective

Obiectivele acestei activități practice constau în înțelegerea structurii cadrului Ethernet și a tehnicilor utilizate pentru descoperirea altor dispozitive într-o rețea bazată pe Ethernet. În plus, este explorat modul de simulare al instrumentului Cisco Packet Tracer.

2. Considerații teoretice

Această activitate practică se concentrează pe operațiunile de nivel 2 efectuate pe switch-uri. Nivelul 2 se referă la stratul Data Link din modelul ISO/OSI, care corespunde stratului de acces la rețea (Network Access Layer) din modelul TCP/IP.

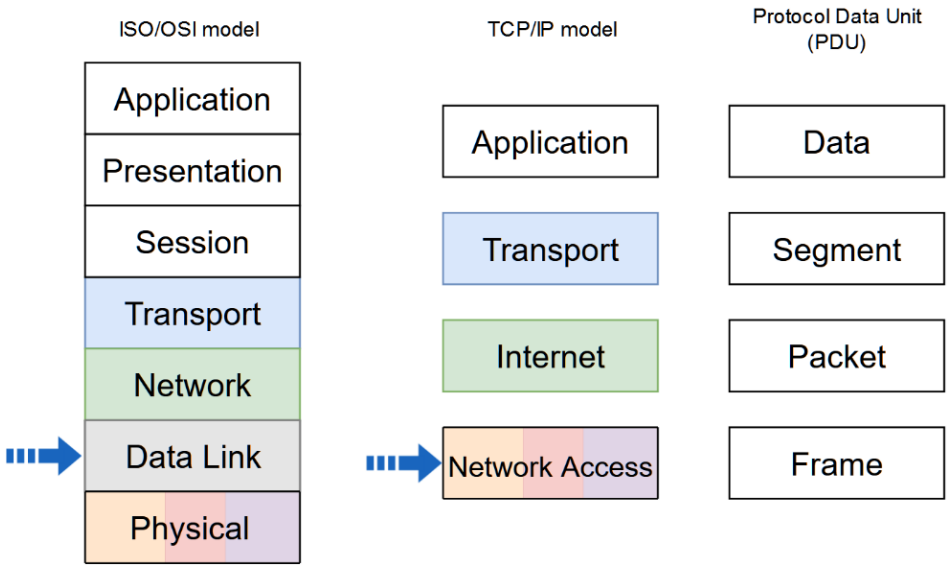


Figura 9.1 *Modelele stivei de rețea și denumirea PDU la fiecare nivel. Săgețile indică nivelurile abordate în activitatea curentă*

Pentru ca un switch să poată redirecționa un pachet pe un port specific, acesta menține o tabelă de comutare care conține o corespondență între o adresă MAC de destinație și numărul portului switch-ului. Adresele MAC utilizate pentru comunicare se găsesc în antetul cadrului Ethernet (Nivelul 2) și un switch nu decapsulează cadrul mai departe atunci când manipulează conținutul pachetului (Figura 9.2). Această activitate practică continuă cu furnizarea de mai multe detalii despre operațiunile de Nivel 2.

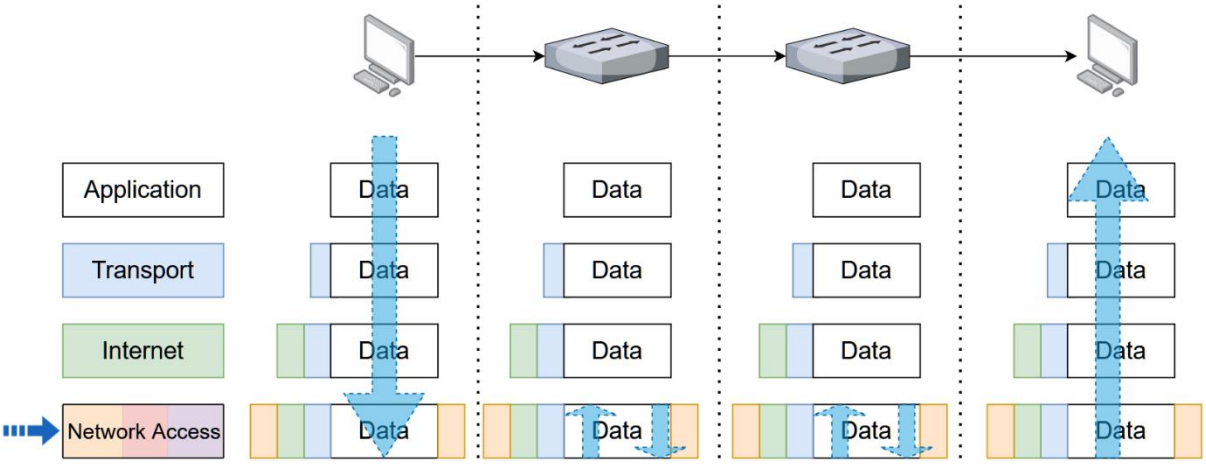


Figura 9.2 *Operațiunea de comutare, care arată serializarea/deserializarea cadrelor în nivelului de Acces la Rețea (Network Access Layer).*

2.1 Ethernet, Ethernet II și IEEE 802.3

Ethernet, Ethernet II și IEEE 802.3 sunt termeni adesea folosiți interschimbabil. Deși acești termeni se referă la standarde foarte similare, ele sunt ușor diferite, atât din punct de vedere istoric, cât și tehnic. În 1981, un consorțiu format din Digital Equipment Corporation, Intel și Xerox (abreviat DIX) a dezvoltat standardul Ethernet (denumit și DIX 1.0 sau Ethernet I). Acesta a fost înlocuit cu DIX 2.0, mult mai cunoscut sub numele de Ethernet II, în 1982. În 1983, IEEE a introdus standardul 802.3 în încercarea de a standardiza protocolul dincolo de consorțiul DIX. În prezent, Ethernet II este, în general, abordarea mai populară, din motive care vor fi descrise în curând.

Există două diferențe principale între Ethernet II și IEEE 802.3. Prima este că Ethernet II folosește un câmp de tip (denumit și EtherType), care specifică protocolul încapsulat în payload, în timp ce 802.3 folosește acel câmp pentru a specifica lungimea payload-ului. A doua diferență este că, pentru a rula 802.3 într-o stivă TCP/IP, este nevoie de informații suplimentare (bazate pe formatul SNAP și 802.2 – care depășesc sfera acestei activități practice) și, ca atare, sunt preluate din câmpul de date (Data field). Acest lucru totalizează 8 octeți pe care 802.3 îi folosește din câmpul de date, reducând acest câmp la o gamă de 38 până la 1492 octeți. Totuși, istoric vorbind, câmpul de lungime a fost considerat inutil, iar rețelele funcționează la fel de bine și fără el – acesta este motivul pentru care Ethernet II este standardul mai frecvent utilizat. Toate sistemele de operare moderne funcționează însă atât cu 802.3, cât și cu Ethernet II.

Rețineți că, atunci când majoritatea inginerilor se referă la Ethernet, se referă în general la Ethernet II sau, mai rar, la standardul IEEE 802.3. Această activitate practică va folosi termenii Ethernet și Ethernet II interschimbabil, deoarece Ethernet I nu mai este utilizat.

2.2 Structura cadrului Ethernet II

Figura 9.3 prezintă structura cadrului Ethernet II/IEEE 802.3 și numărul de octeți alocați pentru fiecare câmp. Secțiunea următoare descrie semnificația fiecărui câmp dintr-un cadru Ethernet.

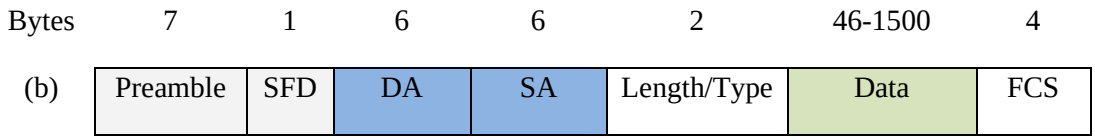


Figura 9.3 *Strucutra cadrului Ethernet II / IEEE 802.3*

Deoarece Ethernet definește protocoale atât pentru părțile stratului Fizic, cât și pentru stratul Data Link dintr-o stivă de rețea, unele câmpuri sunt gestionate de stratul Fizic (Preambul și SFD), în timp ce altele sunt gestionate de stratul Data Link (celelalte câmpuri).

Câmpul Preambul este o serie de 56 de biți alternanți de „0” și „1”. Aceștia sunt utilizați pentru ca dispozitivele implicate în comunicare să își poată sincroniza ceasurile respective și, astfel, să ajusteze rata de eșantionare corespunzător pentru recepția corectă a cadrului. Conceptul de utilizare a unui preambul nu impune o lungime fixă, ci este ajustat în funcție de protocolul individual, chiar dacă Ethernet folosește o lungime fixă de 56 de biți. Utilizarea mai multor biți permite mai mult timp pentru ca dispozitivele de comunicație să se sincronizeze, dar crește sarcina de comunicație, în timp ce reducerea lungimii preambulului are efecte opuse.

Câmpul Start Frame Delimiter (SFD) este un octet folosit pentru a întrerupe modelul de biți din Preambul și pentru a marca începutul restului cadrului Ethernet. În mod specific, acesta este „10101011” sau 0xD5 (din nou, acest lucru este specific pentru Ethernet; alte protocoale ar putea folosi valori diferite pentru SFD). Rețineți că biții sunt transmiși de la stânga la dreapta și interpretați în ordine LSB (Least Significant Bit).

Adresa MAC de destinație (DA) și Adresa MAC sursă (SA) sunt identificatori atribuiți în mod unic controlerului de interfață de rețea (NIC) al fiecărui dispozitiv. Este important de menționat că un dispozitiv poate avea multiple NIC-uri și, prin urmare, mai multe adrese MAC corespunzătoare. Rolul DA și SA va fi discutat mai detaliat în secțiunile următoare.

Câmpul Type este utilizat pentru a indica tipul de mesaj încapsulat în cadru. Tabelul 9.1 indică unele valori specifice pentru câmpul Type.

Tabel 9.1 Exemple EtherType

Valoare Hex	Tip Protocol
0x0000-0x05DC	Length field for IEEE 802.3
0x0600	Xerox
0x0800	IPv4
0x0801	X.75
0x0806	ARP
0x86DD	IPv6

Rețineți că, din cauza cerinței minime de 46 de octeți folosiți pentru transmiterea datelor, dacă lungimea datelor este mai mică decât această valoare, stratul Data Link adaugă octeți de umplere (padding) în câmpul Data. Valoarea de 46 de octeți se bazează pe mecanismul

CSMA/CD (prezentat în timpul cursului) și depășește sfera acestei activități. Alternativ, acest câmp este considerat a reprezenta Lungimea (Length) pentru 802.3, atunci când valoarea sa este mai mică decât 0x05DC.

Câmpul Data corespunde sarcinii utile (payload) care este încapsulată în cadru. Aceasta este de obicei data protocolului de nivel superior.

Câmpul Frame Check Sequence (FCS) este folosit pentru a verifica integritatea mesajului. Este un control de redundanță ciclică (CRC) de patru octeți. Este o valoare numerică calculată pe baza tuturor datelor din cadrul, cu excepția FCS-ului propriu-zis (și, evident, a Preambulului și a SFD-ului). La recepție, această valoare este recalculată și comparată cu FCS-ul original. Dacă cele două valori sunt diferite, atunci cadrul conține erori și este eliminat.

2.3 Protocolul ARP (Address Resolution Protocol)

Protocolul Address Resolution Protocol (ARP) este un protocol foarte important în rețelistică. Așa cum s-a discutat în timpul cursurilor și activităților anterioare, adresarea este gestionată separat de nivelurile stivei OSI (sau TCP/IP). Nivelului Data Link (DLL) îi revine gestionarea adreselor MAC (deși uneori sunt denumite adrese fizice și depind de placa de rețea, nivelul Fizic nu gestionează în mod general adresele MAC), nivelul de rețea gestionează adresele IP, iar nivelul Transport gestionează numerele de port. Nivelului Transport nu i se acordă atenție în această activitate practică. Într-un scenariu tipic de rețelistică, atunci când un dispozitiv intenționează să trimită un mesaj către o destinație, acesta știe deja adresa IP a destinației de la un server DNS. Cu toate acestea, pentru a asambla corect un cadru, nivelul Data Link trebuie să cunoască adresa MAC, care nu este gestionată de serverele DNS, iar gestionarea manuală este extrem de impracticabilă. Astfel, ARP oferă un mecanism simplu pentru a determina adresa MAC pentru o adresă IP cunoscută, un proces cunoscut sub numele de *Rezoluția Adresei (Address Resolution).*

Fiecare dispozitiv conține o structură de date internă, cunoscută sub numele de cache ARP, care stochează corelațiile dintre adresele IP și adresele MAC într-o rețea. ARP este utilizat pentru a popula acest cache. Figura 9.4 ilustrează conținutul cache-ului prin rularea comenzii *arp -a* în consola Windows.

```
C:\Users\admin>arp -a

Interface: 192.168.0.103 --- 0x12
  Internet Address      Physical Address      Type
  192.168.0.1           c4-6e-1f-37-70-61     dynamic
  192.168.0.101         9c-2e-a1-ed-55-ab     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
```

Figura 9.4 *Cache ARP*

Pentru a realiza acest lucru, sunt necesare, în general, două cadre ARP: un cadru ARP Request și un cadru ARP Reply. Să considerăm două dispozitive într-o rețea: dispozitivul A intenționează să transmită un mesaj către dispozitivul B. Algoritmul ARP este următorul:

1. Dispozitivul A își verifică cache-ul ARP. Dacă există o intrare cu adresa IP a dispozitivului B, va sări direct la pasul 5.
2. Dispozitivul A transmite un ARP Request prin broadcast, conținând adresa IP a țintei. Toate dispozitivele primesc acest broadcast, deoarece A nu cunoaște încă adresa MAC a dispozitivului B.
3. Dacă dispozitivul B se află în rețea, acesta va răspunde cu un ARP Response care conține propria sa adresă MAC. Toate celelalte dispozitive vor ignora în tăcere (adică fără a trimite un mesaj care să anunțe acest lucru) cererea.
4. Dispozitivul A își va actualiza cache-ul ARP.
5. Dispozitivul A va trimite mesajul dorit ca unicast către B.

Cache-urile ARP conțin două tipuri de intrări: statice și dinamice. Intrările statice sunt introduse de utilizator și sunt păstrate permanent în cache, cu excepția cazului în care sunt eliminate în mod specific. Intrările dinamice sunt introduse de ARP și sunt șterse periodic. Fiecare intrare ARP poate fi ștearsă după perioade de la câteva secunde până la câteva ore, în funcție de rețea, tipul dispozitivului, caracteristicile sistemului de operare și configurațiile individuale. Ștergerea intrărilor dinamice este un proces automat (dar care poate fi inițiat manual) și este utilă deoarece unele intrări ARP ar putea să nu mai fie necesare. Câteva exemple ale acestei situații sunt:

- Un dispozitiv își schimbă adresa IP (mai ales dacă utilizează DHCP).
- Un dispozitiv este eliminat din rețea, astfel încât intrarea ar putea să nu mai fie necesară.
- Un dispozitiv își schimbă NIC-ul și, implicit, adresa MAC corespunzătoare din rețea.

Motivul pentru eliminarea periodică a intrărilor din cache este de a înlătura orice intrări inutile sau neutilizate (mai ales că cache-ul are o dimensiune fixă, ceea ce poate duce la anumite strategii de atacuri cibernetice). Doar mesajele ARP actualizează cache-urile ARP, astfel încât un dispozitiv va actualiza o intrare fie atunci când primește o cerere ARP, fie când primește un răspuns ARP ca parte a procesului de rezoluție sau când primește un broadcast ARP (acest scenariu final doar actualizează intrările ARP, nu adaugă unele noi – de asemenea, este utilizat pentru a evita suprasolicitarea cache-ului).

Intrările statice ar trebui, în general, să fie utilizate doar atunci când un dispozitiv este destinat să rămână în rețea pentru o perioadă lungă de timp (de exemplu, un router). Cu excepția unor forme de atacuri cibernetice, ARP nu generează mult overhead.

Alte cazuri de utilizare ARP sunt: utilizarea Proxy ARP, care implică un dispozitiv care răspunde la o cerere ARP în numele altui dispozitiv, și utilizarea unui ARP gratuit (gratuitous ARP), care implică trimiterea unui broadcast ARP astfel încât alte gazde să își poată actualiza intrările respective. Aceste cazuri de utilizare depășesc sfera acestei activități.

2.4 Protocolul NDP (Neighbor Discovery Protocol)

Protocolul Neighbor Discovery Protocol (NDP sau simplu ND) este un protocol utilizat cu IPv6 și are multiple roluri. Acesta definește cinci tipuri de pachete ICMPv6, dintre care unele au fost deja prezentate. Acestea sunt: Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisement (NA) și pachetele Redirect.

NDP îndeplinește mai multe roluri, dintre care activitatea curentă prezintă doar pe scurt rezoluția adreselor MAC și IPv6.

În IPv6, mesajele NS și NA sunt utilizate pentru a înlocui ARP și sunt, într-o anumită măsură, echivalente cu mesajele ARP Request și ARP Reply. La fel ca și cache-ul ARP, dispozitivele compatibile cu IPv6 folosesc o Tabelă de Vecini IPv6 sau un Cache de Descoperire a Vecinilor IPv6. Cu toate acestea, există anumite optimizări aduse de NDP.

O optimizare semnificativă este adusă de utilizarea adreselor multicast: în loc de a trimite o cerere ARP prin broadcast, NDP implică trimiterea unui NS la adresa multicast a dispozitivului țintă, ceea ce reduce suprasolicitarea rețelei.

O altă optimizare este adusă de utilizarea a cinci stări care descriu o intrare în Cache-ul de Descoperire a Vecinilor IPv6 (IPv6 ND Cache):

- Incomplete (NS a fost trimis, dar NA nu a fost încă primit)
- Reachable (NS a fost trimis și NA a fost primit sau intrarea ND a fost utilizată cu succes de un protocol de nivel superior)
- Stale (Intervalul de timeout a expirat)
- Delay (Intervalul de timeout a expirat, dar un pachet recent a fost trimis către țintă, starea se schimbă în Probe după trimiterea unui NS)
- Probe (NS a fost trimis din starea Delay, așteptând NA)

IPv6 ND se bazează pe ARP, dar are multiple funcții și este mult mai complex decât simpla rezoluție a adreselor MAC în adrese IP.

3. Desfăşurarea lucrării practice

În activitatea următoare, veți utiliza Wireshark pentru a analiza protocolul ARP. Utilizarea cache-ului ARP local pe dispozitiv necesită privilegii de administrator. Instrucțiunile curente sunt pentru sistemele bazate pe Windows. Pe sistemele bazate pe Unix, comanda `sudo` poate fi necesară pentru a manipula cache-ul ARP local. Activitatea are două părți:

1. Utilizarea dispozitivului local
   a. Golirea cache-ului ARP local
   b. Examinarea unei cereri ARP
   c. Examinarea unui răspuns ARP

2. Utilizarea simulatorului Packet Tracer
   a. Modul de simulare ARP
   b. Modul de simulare NDP

3.1 Utilizarea dispozitivului local

Pasul 1: Mai întâi, va trebui să deschideți o linie de comandă sau PowerShell cu privilegii de administrator. Pentru a face acest lucru, faceți clic dreapta pe programul corespunzător și selectați „Run as Administrator”. Introduceți parola atunci când vi se solicită. Utilizați comanda `ipconfig /all` și notați-vă adresa IPv4, adresa MAC corespunzătoare și adresa IPv4 a gateway-ului implicit.

Pasul 2: Deschideți o captură Wireshark pe interfața corespunzătoare. Pentru a goli cache-ul ARP, trebuie să utilizați comanda `arp -d`. Pentru a vizualiza cache-ul ARP, se folosește comanda `arp -a`. Deoarece cache-ul ARP este actualizat continuu, pentru a vă asigura că este golit, puteți combina cele două instrucțiuni folosind caracterul `&`, astfel: `arp -d & arp -a` (opțional, dacă `arp -d` nu funcționează, utilizați una dintre următoarele comenzi: `arp -ad` sau `netsh interface ip delete arpcache`). Pentru a vă asigura că adresa MAC a gateway-ului implicit este reintrodusă în cache, trimiteți un ping la adresa IPv4 a gateway-ului implicit. Opriți capturarea în Wireshark. Puteți folosi din nou comanda `arp -a` pentru a verifica că acum cache-ul conține intrarea corespunzătoare gateway-ului implicit.

Pasul 3: Utilizați filtrul ARP în Wireshark pentru a vizualiza doar cadrele ARP. Selectați primul mesaj de tip broadcast. Acesta este un mesaj de cerere ARP. Observați că tipul este Ethernet II (cu excepția cazului în care utilizați în mod specific un alt protocol). Extindeți fila corespunzătoare Ethernet II în Wireshark. Verificați că mesajul provine de la dispozitivul dvs. fie folosind adresa MAC sursă, fie adresa IP sursă (pot exista alte mesaje de cerere pe rețea). Dacă prima cerere nu este a dvs., continuați și navigați până când găsiți cererea proprie.

Pasul 4: Acum că ați identificat corect mesajul de cerere ARP, continuați și analizați-l (Figura 9.5). Observați că câmpul DA este *FF:FF:FF:FF:FF* . Aceasta este o adresă de broadcast. Observați că câmpul de tip este 0x0806, ceea ce indică corect un cadru ARP. Rețineți că adresele din cazul dvs. vor fi diferite.

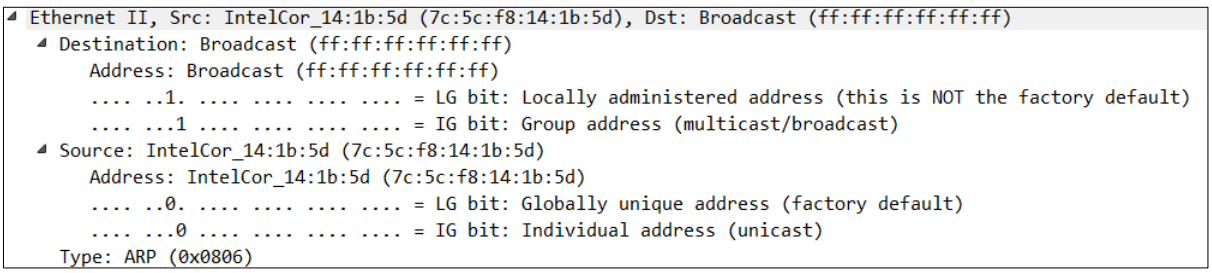


Figura 9.5 *Captură Wireshark a unui cadru detaliat de cerere ARP (ARP Request)*

Pasul 5: Să investigăm conținutul real al ARP. Extindeți selecția corespunzătoare, așa cum se vede în Figura 9.6.

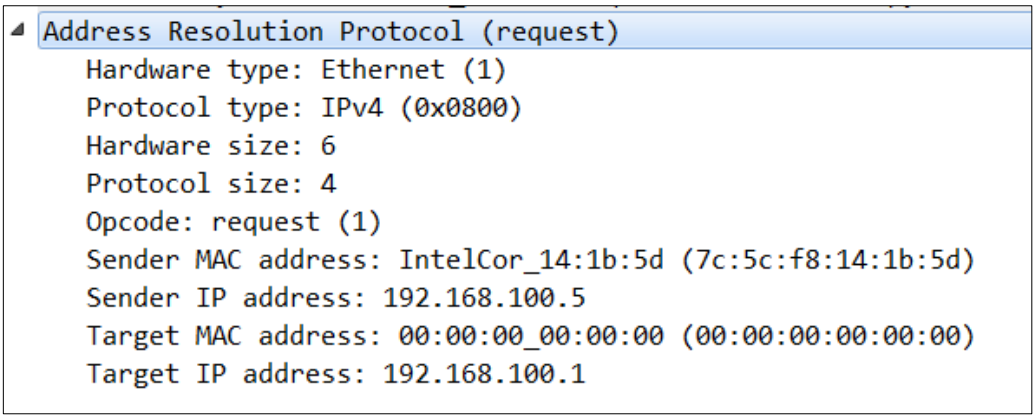


Figura 9.6 *Captură Wireshark a unui cadru ARP Request (cerere ARP)*

Să analizăm fiecare câmp și să înțelegem scopul și semnificația lor respectivă. Hardware type și Protocol type se referă la ce tipuri de adrese sunt mapate între ele. În acest caz, o adresă MAC este mapată la o adresă IPv4 cunoscută (rețineți că acesta este scopul ARP). Următoarele două câmpuri se referă la dimensiunea fiecărei adrese: o adresă MAC are 6 octeți, în timp ce o adresă IPv4 are 4 octeți. Opcode este, în cazul ARP, una dintre două opțiuni: „1” reprezintă o cerere, iar „2” reprezintă un răspuns. Adresele MAC și IP ale expeditorului sunt evident ale dvs. (includerea adresei MAC a expeditorului în cerere asigură că răspunsul poate fi trimis ca unicast către solicitant). Un aspect de remarcat este faptul că protocolul include adresele MAC și IP ale țintei. O distincție **foarte importantă** este utilizarea termenului „Target” în loc de „Destination”. Chiar dacă destinația este un broadcast, așa cum s-a văzut anterior, ținta reprezintă dispozitivul a cărui adresă MAC este rezolvată. Prin urmare, există o distincție între destinație și țintă. Adresa IP este clar gateway-ul implicit și, deoarece adresa MAC a țintei nu a fost încă rezolvată, acest câmp este lăsat necompletat.

Pasul 6: Să analizăm răspunsul ARP corespunzător (Figura 9.7). Mai întâi, trebuie să găsiți răspunsul corect – acesta ar trebui să fie de la gateway-ul implicit către dispozitivul dvs. În funcție de cât timp a rulat capturarea, este posibil să existe mai multe cereri și răspunsuri – acest lucru se datorează ratei de reîmprospătare a cache-ului ARP.

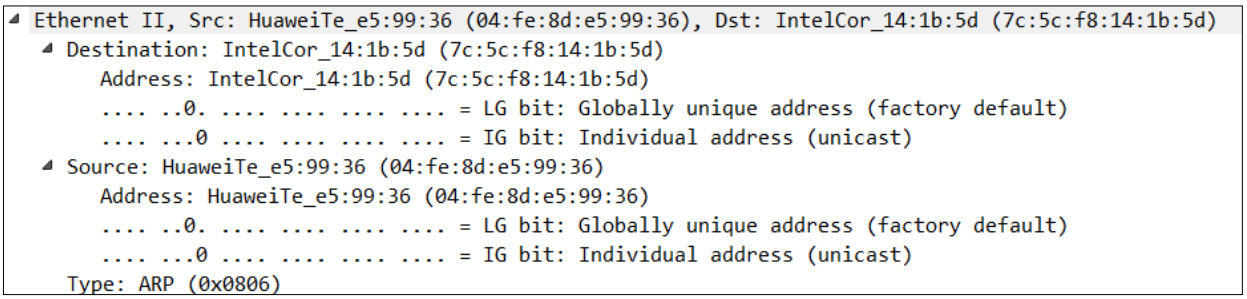


Figura 9.7 *Captură Wireshark a unui cadru ARP Reply (răspuns ARP)*

Se poate observa că acesta este un mesaj unicast de la o adresă MAC din rețea (verificați că este gateway-ul implicit pe baza celor notate anterior).

Pasul 7: Să analizăm conținutul protocolului (Figura 9.8).

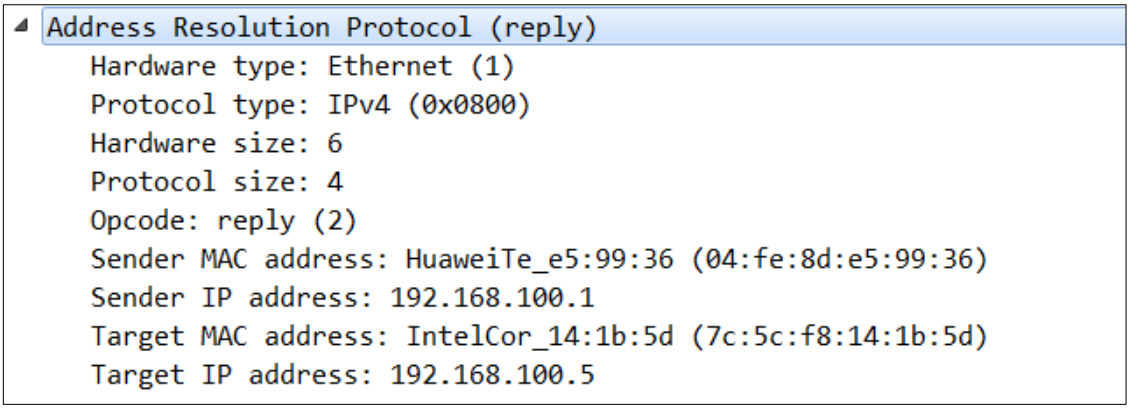


Figura 9.8 *Captură Wireshark a unui cadru ARP Reply (răspuns ARP)*

Observați că Opcode a fost schimbat și că adresa MAC a expeditorului este acum vizibilă (în timpul cererii, aceasta corespundea adresei MAC a țintei necunoscute). În concluzie, dispozitivul nostru primește acest răspuns de la gateway-ul implicit și astfel își poate popula cache-ul ARP cu adresa MAC corespunzătoare. Comunicarea poate continua acum fără schimbul de mesaje ARP suplimentare, cu excepția cazului în care intrarea este ștearsă după expirarea unui timeout.

3.2 Utilizarea simulatorului Packet Tracer

a. Mod simulare ARP

Această parte a activității practice utilizează modul de simulare al instrumentului Cisco Packet Tracer pentru a verifica modul în care pachetele de rețea circulă într-o rețea. Aceasta va clarifica, de asemenea, de ce prima cerere de ecou a unei comenzi **ping** poate fi uneori un timeout nereușit (așa cum probabil ați observat în activitățile anterioare).

Pasul 1: Lansați Packet Tracer, creați o topologie de rețea care conține doar switch-uri și dispozitive finale, și navigați la modul de simulare, așa cum este indicat de săgeata din Figura 9.9.

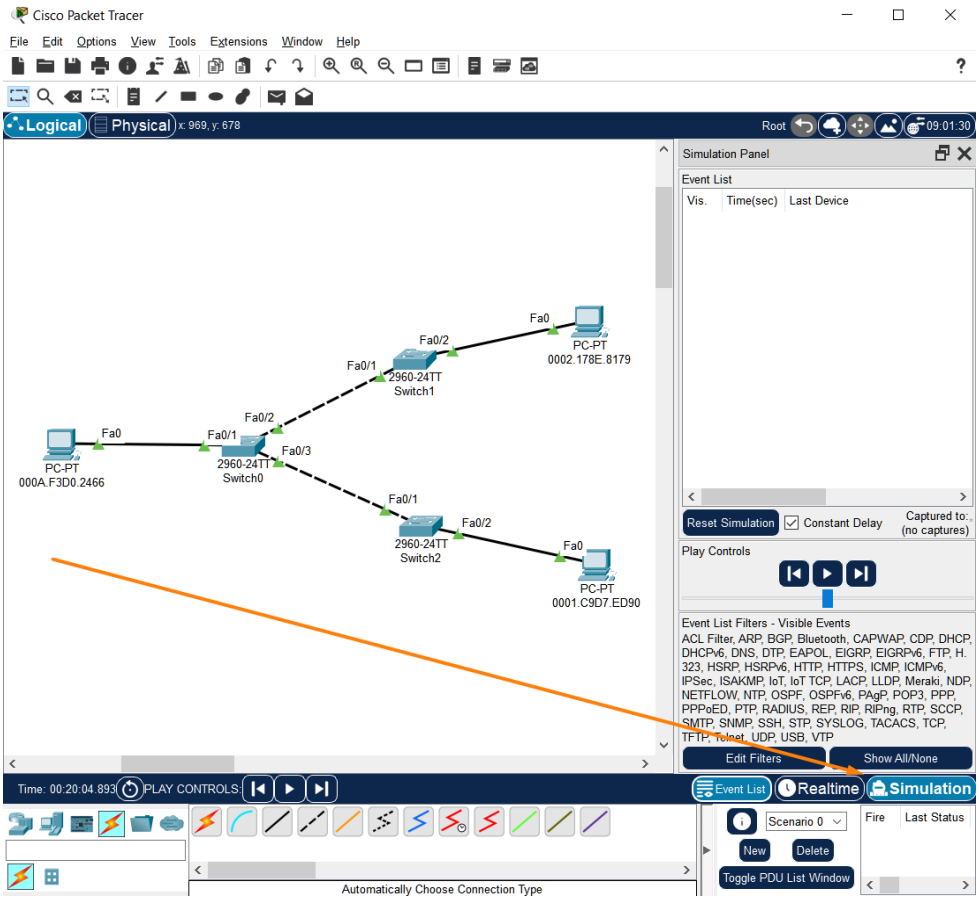


Figura 9.9 *Modul de simulare PacketTracer*

Pasul 2: În fereastra de simulare, faceți clic pe butonul „Show All/None” pentru a șterge toate filtrele, apoi faceți clic pe butonul „Edit Filters” și selectați doar ARP și ICMP (Figura 9.10).

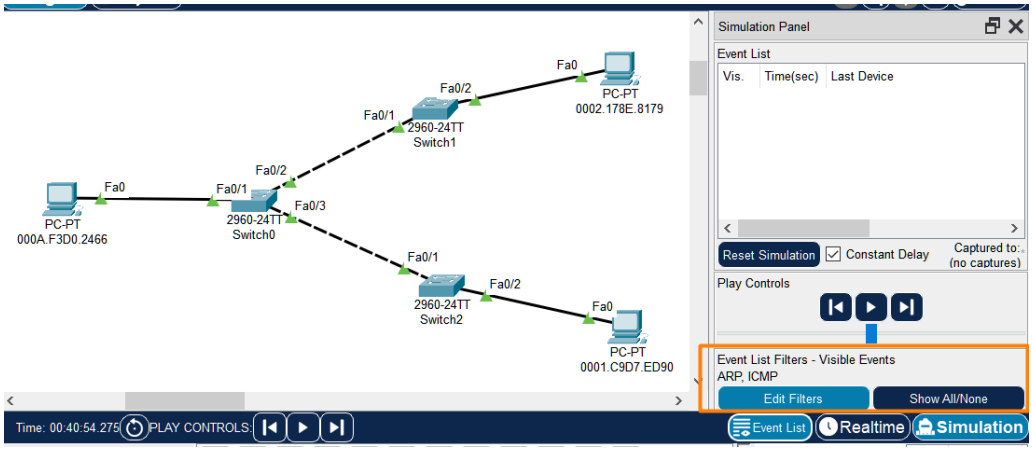


Figura 9.10 *Filtre de Simulare în PacketTracer*

Pasul 3: Redenumiți numele PC-urilor cu propriile lor adrese MAC; acestea pot fi găsite în meniul PC -> tab Config -> interfața FastEthernet0.

Pasul 4: Atribuiți fiecărui PC o adresă IP din aceeași rețea (de exemplu, 10.0.0.1, 10.0.0.2 și 10.0.0.3, toate /8 – puteți folosi o altă rețea/subrețea dacă doriți).

Pasul 5: Deschideți linia de comandă pe unul dintre PC-uri și verificați că cache-ul ARP este gol. Dacă nu este gol, rulați comanda `arp -d` pentru a-l goli.

Pasul 6: Trimiteți un ping către adresa IP a altui PC și inspectați simularea. În acest moment, cache-ul ARP al PC-ului este gol, așa că nu poate completa întregul pachet (în mod specific, nu poate completa câmpul DA al cadrului Ethernet), prin urmare lansează o cerere ARP prin broadcast în rețea – reamintiți-vă că aceasta este prima etapă a protocolului ARP. Analiza traficului pas cu pas (Figura 9.11, Figura 9.12 și Figura 9.13) arată calea pe care o parcurge cererea; observați că doar dispozitivul țintă răspunde la cererea difuzată, iar toate celelalte dispozitive elimină pachetul în tăcere.

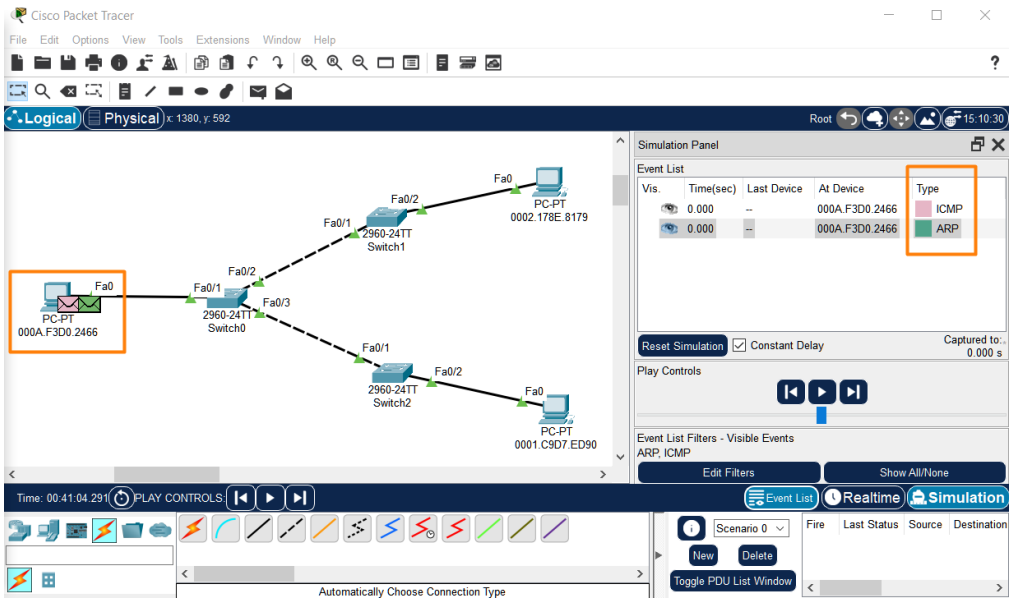


Figura 9.11 *Cerere ARP (ARP request)*

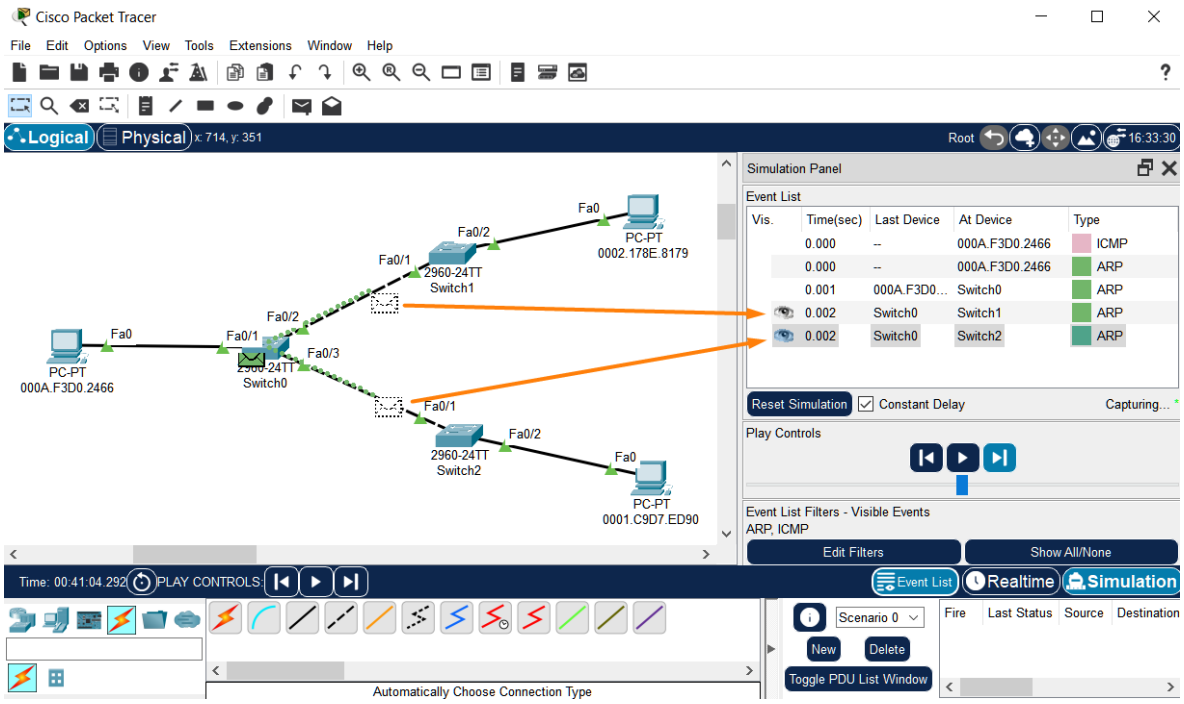


Figura 9.12 *Broadcast ARP*

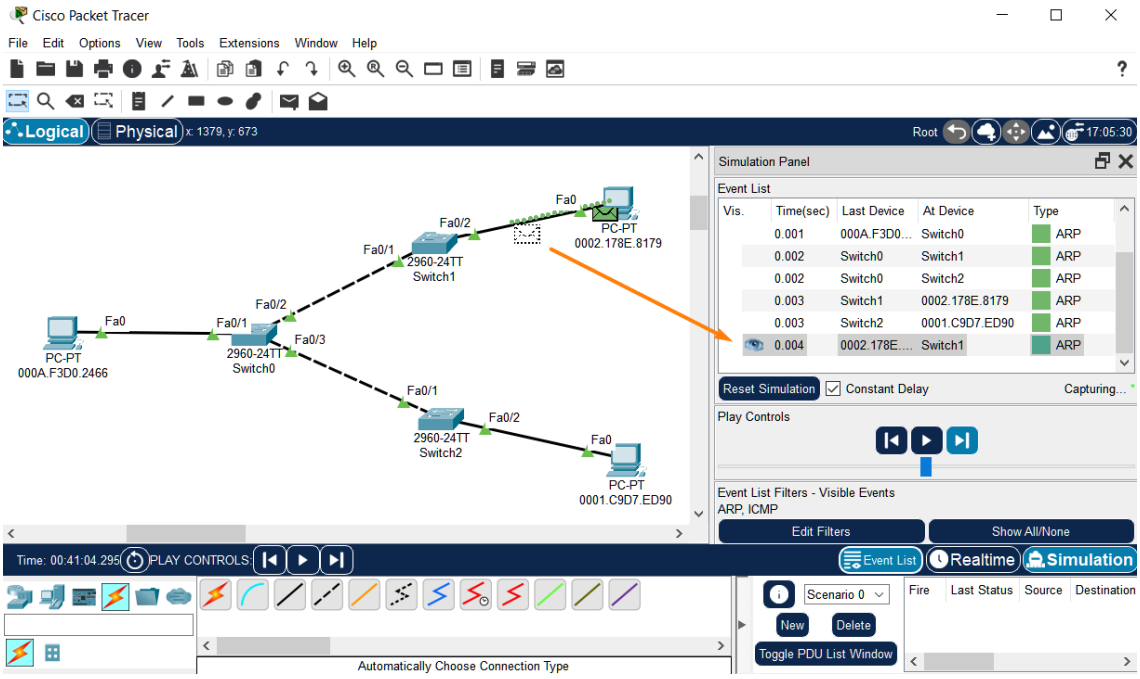


Figura 9.13 *Răspuns ARP (ARP reply)*

Pasul 7: Conținutul pachetului poate fi explorat făcând dublu clic pe pachetul din lista de evenimente (Event List) (Figura 9.14). Aici se poate vedea aceeași informație care a fost descoperită în prima parte a activității practice (informații la toate cele 7 straturi ale modelului OSI, la fel ca în Wireshark).

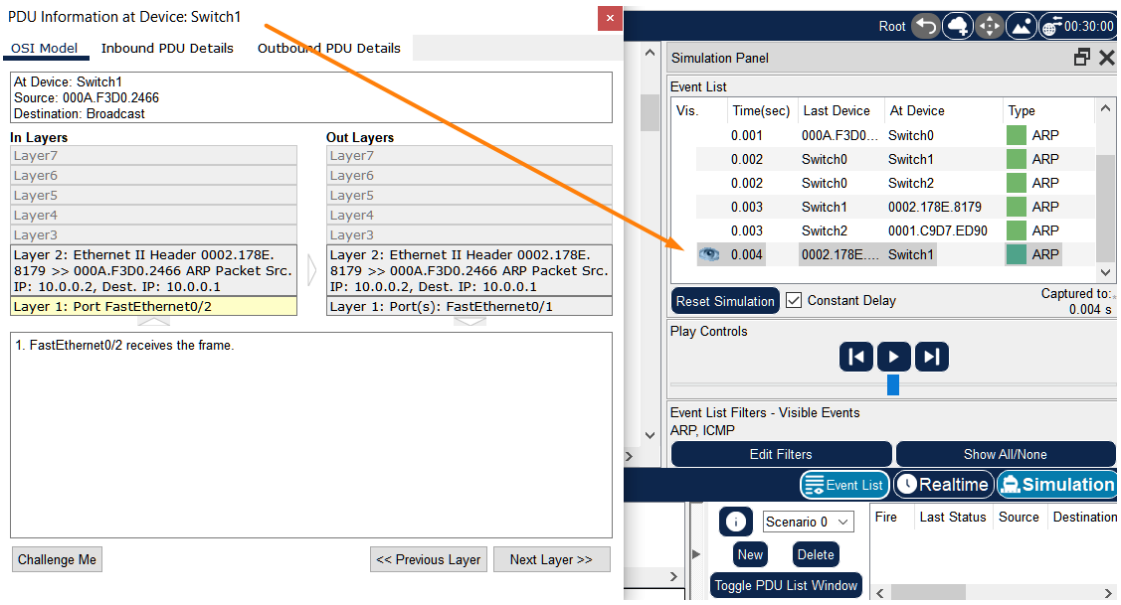


Figura 9.14 *Inspectarea conținutului cadrului în PacketTracer*

Pasul 8: Reluați fluxul pachetului în rețea și inspectați consola PC-ului care rulează comanda **ping**. Dacă răspunsul ARP durează prea mult să fie returnat, atunci primul mesaj ICMP de răspuns la ecou ar putea să nu ajungă la PC la timp, rezultând într-un timeout al cererii (reamintiți-vă că utilitarul **ping** folosește cereri și răspunsuri de ecou ICMP). Acest lucru explică de ce probabil ați observat în activitățile anterioare din Packet Tracer că, mai ales într-o rețea nou formată, unele mesaje se termină cu timeout (Figura 9.15).

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes

Request timed out.
Request timed out.
Reply from 10.0.0.2: bytes=32
```

Figura 9.15 *Timeout-ul la ping exemplificat în PacketTracer*

Pasul 9: Utilizați următoarele comenzi pe componentele switch-ului pentru a inspecta tabelele de adrese MAC și pentru a vedea cum se populează acestea atunci când primele cereri/răspunsuri ARP circulă prin rețea.
Switch>enable
Switch#show mac address-table
Switch#clear mac address-table

b. Mod simulare NDP

Folosind fișierul .pkt pentru IPv6, care a fost creat într-o activitate anterioară pentru funcționalitatea de rutare statică, aplicați filtrul de pachete NDP în fereastra Edit Filters și inspectați traficul conform descrierii din textul activității. Găsiți pachetele RS, RA, NS și ND utilizând modul de simulare.

CAPITOLUL 10: VLAN-URI, TRUNKING ȘI RUTARE INTER-VLAN

1. Obiective

La finalul activității practice, cititorii vor fi capabili să definească și să clasifice rețelele Virtual Local Area Networks (VLAN-uri), să explice scopul trunking-ului și al rutării inter-VLAN și să configureze rețele bazate pe VLAN-uri într-un mediu cu mai multe switch-uri.

2. Consideraţii teoretice

Lucrarea practică actuală se concentrează asupra nivelurilor Data Link și Network ale stivei ISO/OSI (Figura 10.1).

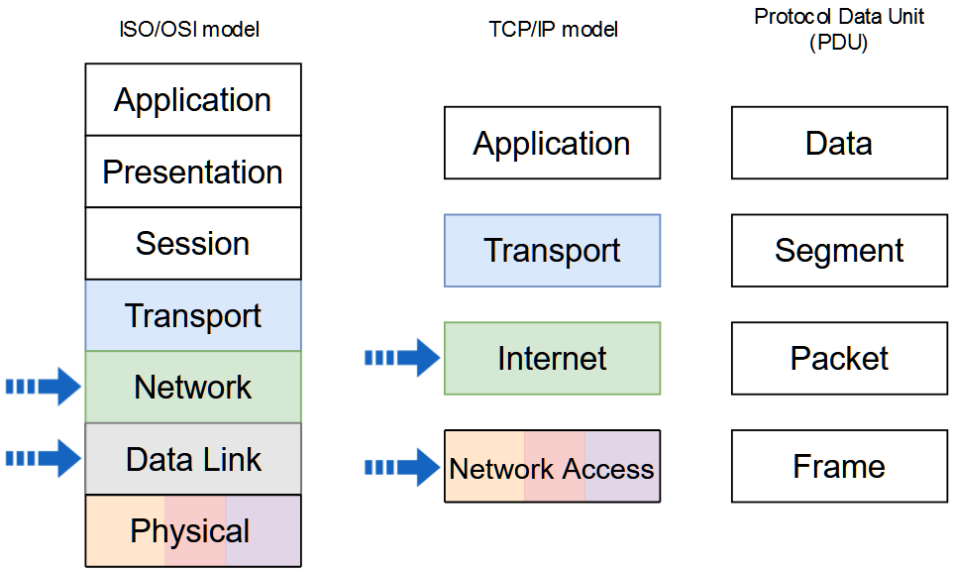


Figura 10.1 *Modelele stivei de rețea și denumirea PDU la fiecare nivel. Săgețile indică nivelurile vizate în activitatea curentă*

2.1 VLAN-uri

Un VLAN este o partiționare a setului de dispozitive conectate la rețeaua locală. Gruparea în VLAN-uri poate fi realizată conform unor criterii diferite, cum ar fi rolul utilizatorilor sau tipul de trafic. Această grupare poate fi făcută indiferent de locația fizică a dispozitivelor sau utilizatorilor (Figura 10.2). VLAN-urile funcționează prin segmentarea logică a rețelei în domenii de broadcast, fiecare VLAN reprezentând un domeniu de broadcast diferit. Switch-ul menține o tabelă de bridging diferită pentru fiecare VLAN. Dispozitivele dintr-un VLAN sunt restricționate la comunicarea doar cu dispozitivele din același VLAN. Conectivitatea între VLAN-uri este facilitată de routere.

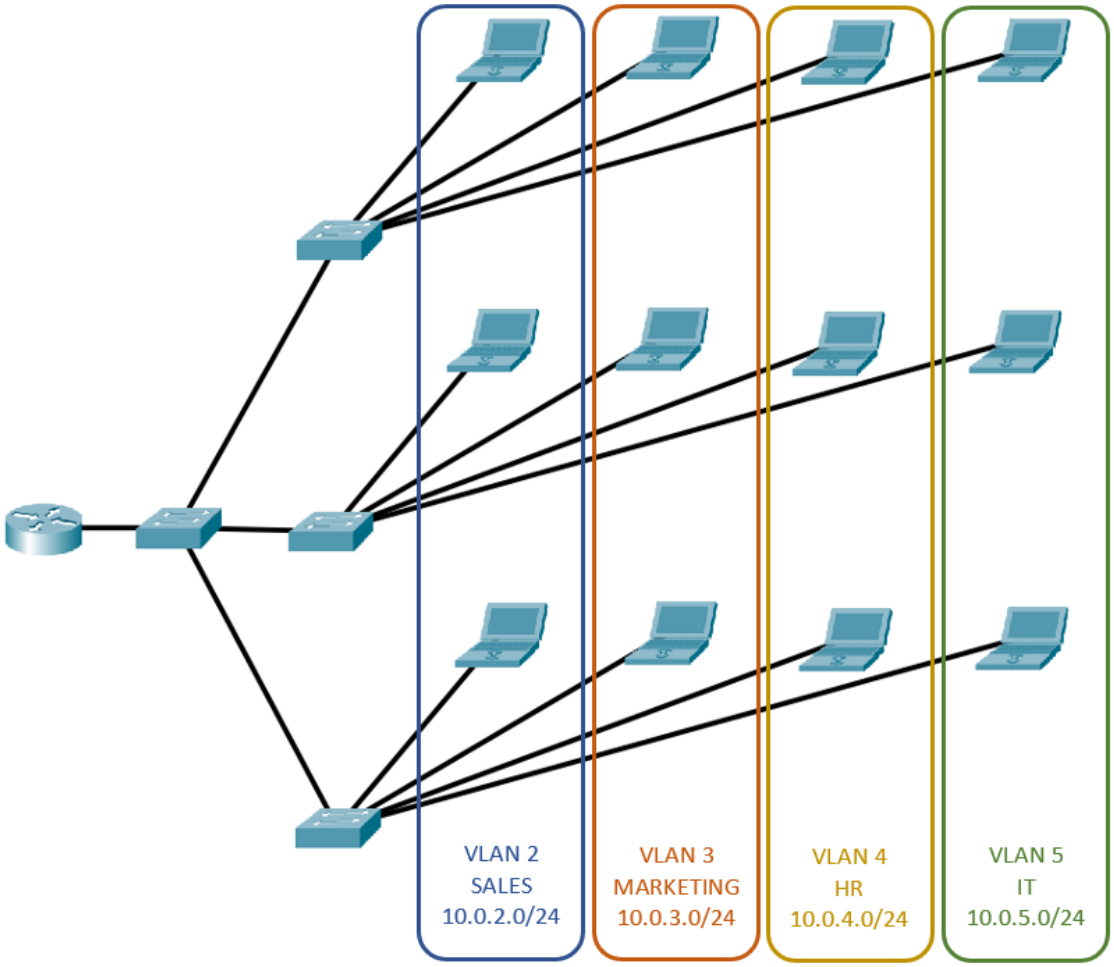


Figura 10.2 *VLAN-urile într-un mediu cu mai multe switch-uri*

Principalele beneficii ale VLAN-urilor sunt:

- domenii de broadcast mai mici;
- costuri reduse;
- performanță crescută a rețelei;
- scalabilitate crescută;
- securitate sporită;
- management îmbunătățit.

Tipuri comune de VLAN-uri:

- VLAN implicit (Default VLAN) – De asemenea cunoscut sub numele de VLAN 1, nu poate fi șters sau redenumit. Toate porturile switch-ului sunt membre ale VLAN-ului 1 în mod implicit;
- VLAN de date (Data VLAN) – VLAN-urile de date sunt de obicei create pentru grupuri specifice de utilizatori sau dispozitive. Ele transportă trafic generat de utilizatori;
- VLAN de voce (Voice VLAN) – VLAN-ul de voce este creat deoarece acest tip de trafic necesită o lățime de bandă garantată și o întârziere mai mică de 150 ms de la sursă la destinație;
- VLAN nativ (Native VLAN) – Acesta este VLAN-ul care transportă tot traficul netaguit. Acest trafic nu provine de la un port VLAN;

- VLAN de management (Management VLAN) – Acesta este un VLAN creat pentru a transporta trafic de management al rețelei, inclusiv SSH, SNMP, Syslog și altele.

2.2 Trunking

Un trunk este o legătură punct-la-punct între două dispozitive de rețea care nu aparține unui VLAN specific și transportă mai multe VLAN-uri. Acesta extinde VLAN-urile pe întreaga rețea și permite dispozitivelor conectate la switch-uri diferite, dar care aparțin aceluiași VLAN, să comunice prin rețeaua comutată.

Porturile atribuite VLAN-urilor sunt configurate în modul acces și utilizează anteturi standard ale cadrelor Ethernet. Acest antet nu conține informații despre VLAN-ul căruia îi aparține cadrul. Când cadrele sunt transmise între switch-uri pe linii de trunk, informațiile despre apartenența la VLAN trebuie să fie transmise împreună cu cadrele. Prin urmare, atunci când cadrele Ethernet sunt plasate pe trunk, informațiile despre apartenența la VLAN sunt adăugate, cadrele folosind anteturi 802.1Q în loc de anteturi Ethernet. Adăugarea informațiilor despre VLAN-uri se numește etichetare (tagging), iar anteturile 802.1Q adaugă și alte informații în cadrul cadrelor, pe lângă apartenența la VLAN.

Figura 10.3 prezintă structura cadrului Ethernet II/IEEE 802.3 utilizată în porturile configurate în modul acces și structura cadrului IEEE 802.1Q utilizată în porturile configurate în modul trunk. Secțiunea următoare descrie semnificația câmpurilor de control ale etichetelor (Tag control information).

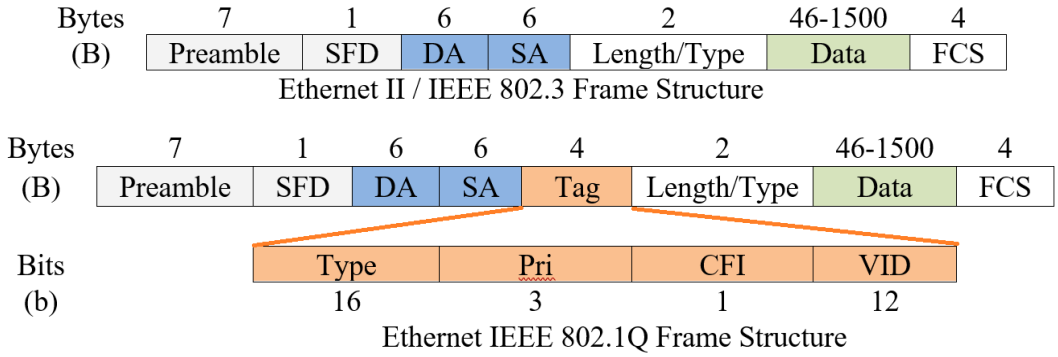


Figura 10.3 *Cadre Ethernet II/IEEE 802.3 și IEEE 802.1Q*

Câmpul de control al etichetei VLAN (VLAN tag control information field) constă din următoarele elemente:

- Type - Valoarea ID-ului protocolului de etichetare (Tag Protocol ID - TPID). Pentru Ethernet, aceasta este setată la valoarea hexadecimală 0x8100.
- User priority - Suportă implementarea nivelului sau serviciului.
- Canonical Format Identifier (CFI) - Permite transportul cadrelor Token Ring pe legături Ethernet.
- VLAN ID (VID) - Numărul de identificare VLAN, suportă până la 4096 ID-uri VLAN.

În exemplul de mai jos (Figura 10.4), Laptop1 conectat la switch-ul S2 pe portul de acces Fa0/6 în VLAN 10 comunică cu Laptop2 conectat la un alt switch, S3, pe portul de acces Fa0/7 în

același VLAN, VLAN 10. Porturile dintre switch-uri sunt configurate în modul trunk. Laptop1 trimite un pachet către Laptop2. Când pachetul intră în switch-ul S2 pe portul de acces Fa0/6, pachetul este encapsulat într-un cadru Ethernet II/IEEE 802.3. Switch-ul S2 transmite pachetul pe portul trunk Fa0/1, encapsulând pachetul într-un cadru Ethernet 802.1Q. Numărul VLAN este setat la 0x00a (VLAN 10).

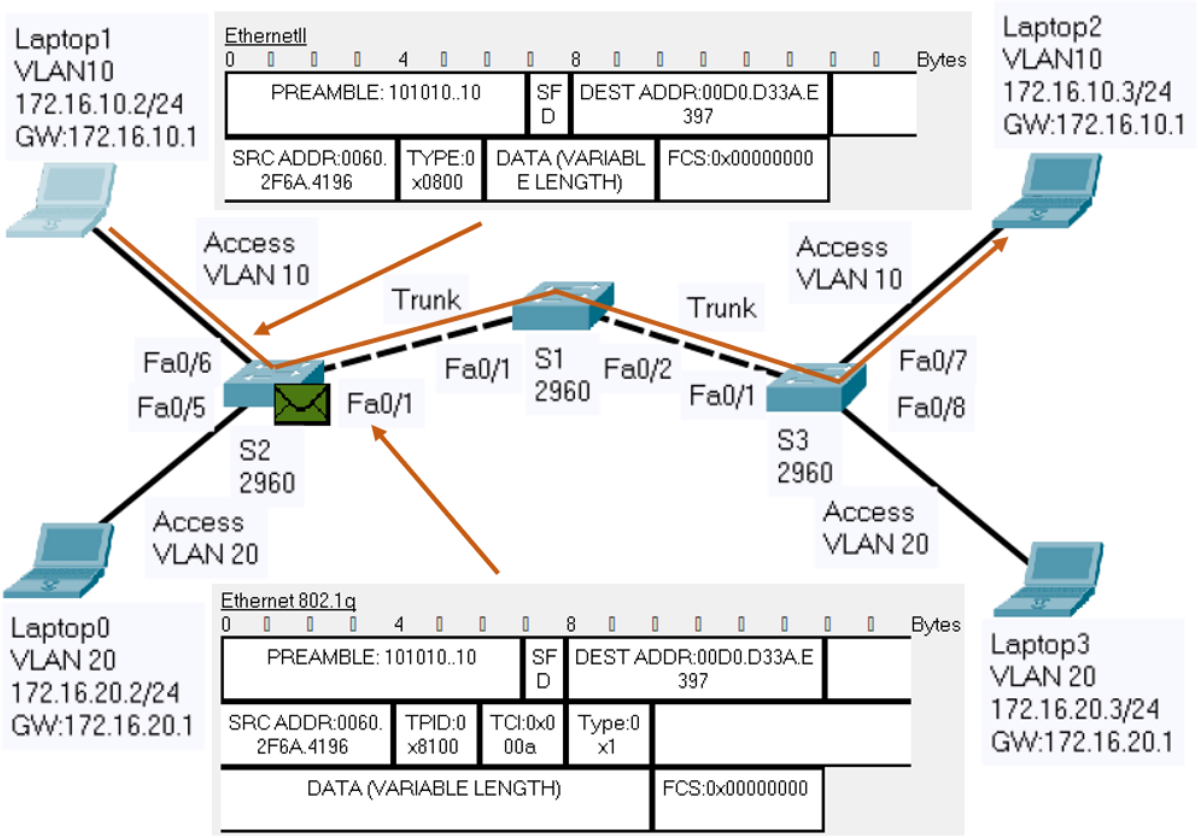


Figura 10.4 *Comunicare în același VLAN*

2.3 Rutare Inter-VLAN

Switch-urile de nivel 2 (Layer 2) nu redirecționează traficul de la un VLAN la altul. Traficul între VLAN-uri este redirecționat folosind dispozitive de nivel 3 (Layer 3), precum routere sau switch-uri de nivel 3, procesul fiind numit rutare inter-VLAN. Există trei opțiuni pentru rutarea inter-VLAN:

- Rutare inter-VLAN de tip legacy (veche);
- Router-on-a-Stick;
- Comutare de nivel 3 folosind SVIs (Switch Virtual Interfaces)

Abordarea router-on-a-stick (vezi Figura 10.5) utilizează una dintre interfețele fizice ale routerului pentru rutarea inter-VLAN.

- Subinterfețe logice sunt create pe interfața fizică; o subinterfață pentru fiecare VLAN; subinterfețele folosesc încapsularea 802.1Q pentru a procesa etichetele VLAN;
- Fiecărui VLAN i se atribuie o adresă de rețea/subrețea diferită;

- Fiecare subinterfață este configurată într-un VLAN cu o adresă IP din VLAN-ul pe care îl reprezintă;
- Gazdele VLAN-ului sunt alocate adrese IP din VLAN-urile lor corespunzătoare; fiecare gazdă este configurată să utilizeze ca gateway implicit subinterfața care reprezintă VLAN-ul său.
- Când o gazdă într-un VLAN comunică cu o gazdă dintr-un alt VLAN, trimite pachetele către propriul gateway, în propriul VLAN; routerul rutează intern între VLAN-uri folosind subinterfețe, deoarece rețelele VLAN-urilor sunt prezente în tabela de rutare ca fiind conectate; routerul primește pachetele pe subinterfața VLAN-ului sursă și redirecționează traficul rutat ca fiind etichetat cu VLAN pentru VLAN-ul de destinație, prin legătura trunk.

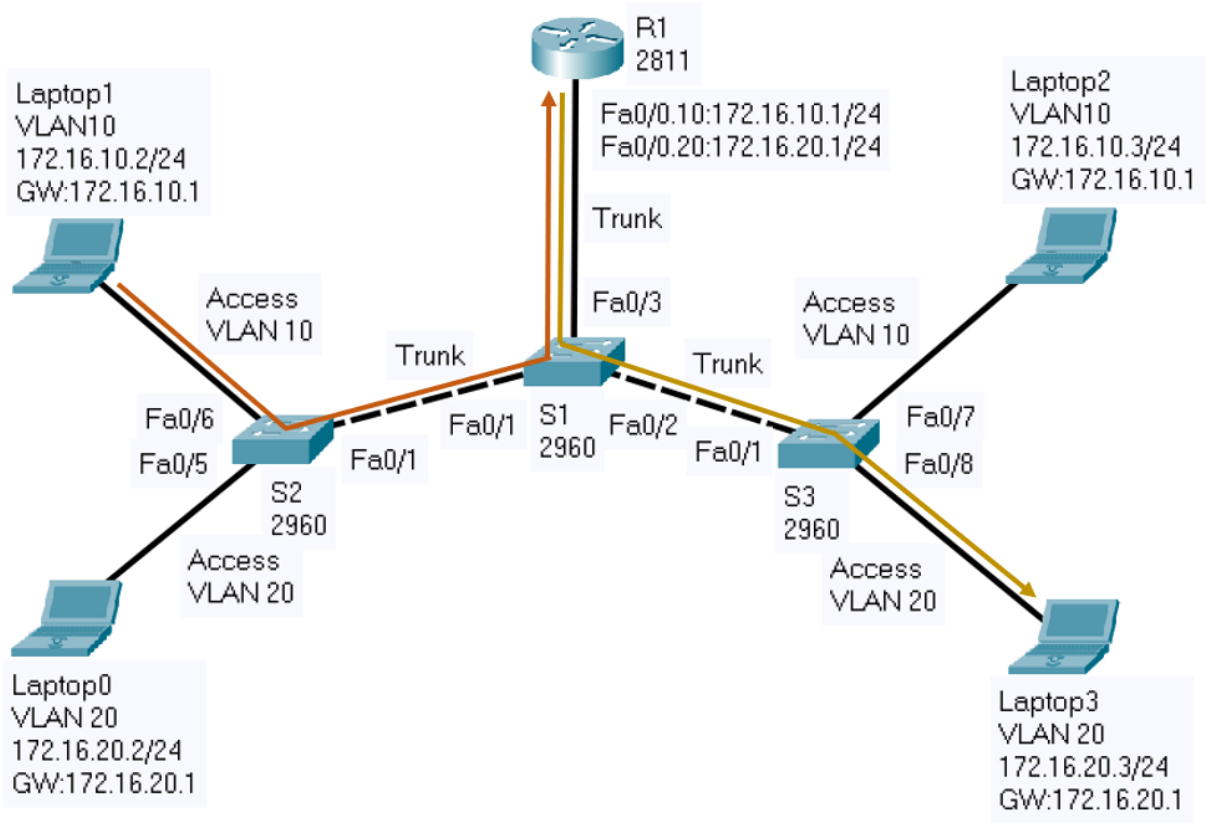


Figura 10.5 *Opțiunea Router-on-a-Stick pentru rutarea inter-VLAN*

3. Desfășurarea lucrării practice

3.1 Discutați aspectele teoretice.

3.2 Luați în considerare topologia rețelei din Figura 10.6:

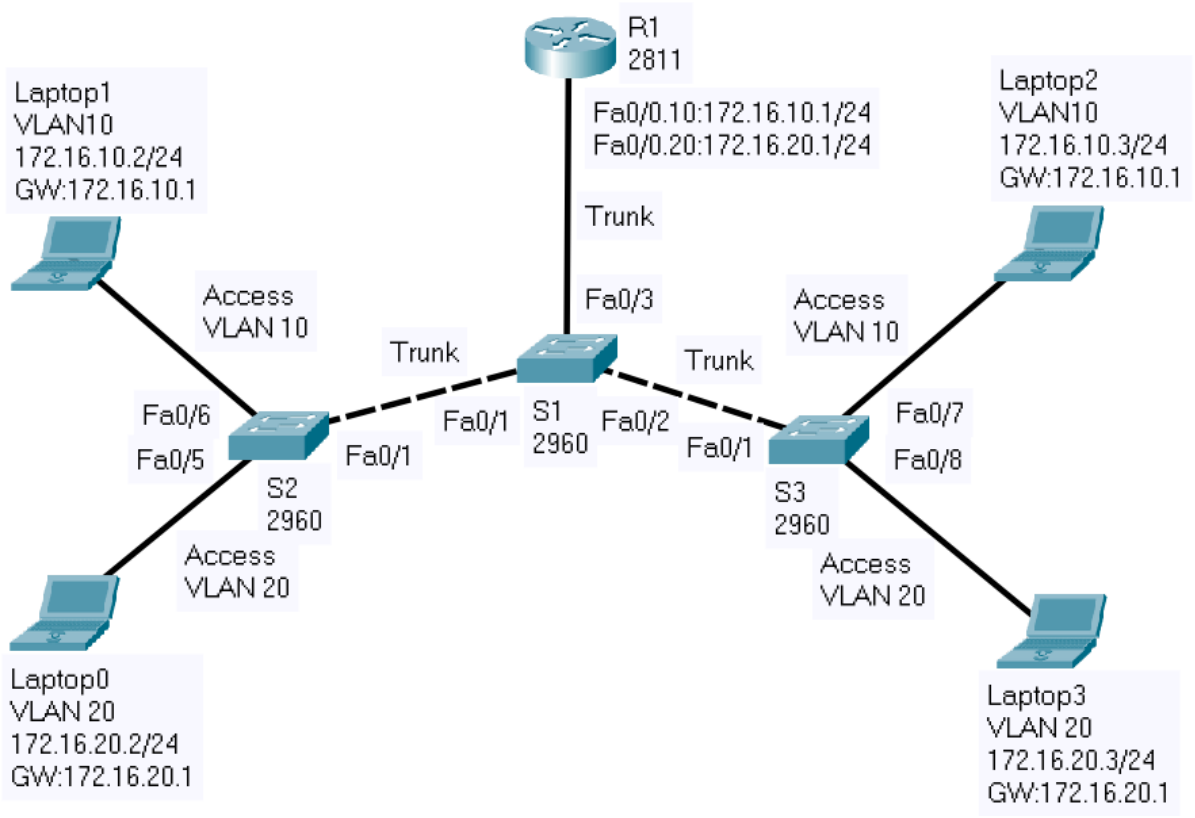


Figura 10.6 *Topologia rețelei de test*

Pas 1: Înainte de a configura dispozitivele de rețea, discutați despre atribuirea adreselor IPv4 din Tabelul 10.1:

Tabel 10.1 *IPv4 addresses for the test network*

Dispozitiv	Interfața	Adresa IP	Netmask	Gateway
Laptop 0	Fa0	172.16.20.2	255.255.255.0	172.16.20.1
Laptop 1	Fa0	172.16.10.2	255.255.255.0	172.16.10.1
Laptop 2	Fa0	172.16.10.3	255.255.255.0	172.16.10.1
Laptop 3	Fa0	172.16.20.3	255.255.255.0	172.16.20.1
R1	Fa0/0.10	172.16.10.1	255.255.255.0	-
R1	Fa0/0.20	172.16.20.1	255.255.255.0	-

Pas 2: Specificați numele gazdă pentru dispozitivele de rețea (router și switch-uri).

Sintaxă generală:

Switch(config)#hostname host-name

Descriere: Specifică sau modifică numele gazdă

Exemplu:

Switch(config)#hostname S2

Pas 3: Creați VLAN 10 și 20 pe toate switch-urile și verificați informațiile VLAN

Sintaxă generală:

Switch(config)#vlan vlan_id

Descriere: Comandă de configurare globală care creează VLAN-ul cu vlan_id specificat

Switch(config-vlan)#name vlan_name

Descriere: Atribuiți un nume VLAN-ului

Exemplu:

S2(config)#vlan 10
S2(config-vlan)#name Vlan10
S2(config-vlan)#exit
S2(config)#vlan 20
S2(config-vlan)#name Vlan20

Sintaxă generală:

Switch#show vlan
Switch#show vlan brief

Descriere: Afișați informațiile VLAN-urilor (conținutul fișierului vlan.dat)

Pas 4: Atribuiți porturile la VLAN-uri și verificați configurația

Sintaxă generală:

Switch(config)#interface interface_id

Descriere: Intrați în modul de configurare a interfeței

Switch(config-if)#switchport mode access

Descriere: Setați portul în modul access

Switch(config-if)#switchport access vlan vlan_id

Descriere: Atribuiți portul unui VLAN

Exemplu:

S2(config)#interface fastEthernet 0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#interface fastEthernet 0/5
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20

Sintaxă generală:

Switch#show vlan
Switch#show vlan brief

Descriere: Afișați informațiile VLAN-urilor (conținutul fișierului vlan.dat)

Pas 5: Setați porturile switch-ului conectate la alte dispozitive de rețea în modul trunk și verificați configurația.

Sintaxă generală:

Switch(config)#interface interface_id

Descriere: Intrați în modul de configurare a interfeței

Switch(config-if)#switchport mode trunk

Descriere: Forțați legătura să fie o legătură de tip trunk.

Exemplu:

S2(config)#interface fastEthernet 0/1
S2(config-if)#switchport mode trunk

Sintaxă generală:

Switch#show interfaces trunk

Descriere: Afișați informațiile despre trunking pentru switch.

Pas 6: Configurați gazdele cu informațiile de adresare IP din figură (adresă IP, mască de rețea și gateway) și testați conectivitatea între ele.

a. ping <target IP>

b. tracert <target IP>

Pas 7: Configurați rutarea inter-VLAN și testați conectivitatea între gazdele din VLAN-uri diferite

Sintaxă generală:

Router(config)#interface interface_id

Descriere: Intrați în modul de configurare a interfeței

Router(config-if)#no shutdown

Descriere: Activează interfața

Router(config-if)#exit

Descriere: Reveniți la modul de configurare globală

Router(config)#interface interface_id.subinterface_id

Descriere: Creați o subinterfață pe o interfață

Router(config-subif)#encapsulation dot1Q vlan_id

Descriere: Specificați IEEE 802.1Q ca metodă de etichetare VLAN pentru VLAN-ul cu ID-ul vlan_id pe această subinterfață

Router(config-subif)#ip address ip_address netmask

Descriere: Adăugați o adresă IP și o mască de rețea pe această subinterfață

Router(config-subif)#end

Descriere: Reveniți la modul Privileged EXEC

Router#show ip route

Descriere: Afișează tabela de rutare.

Exemplu:

R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.16.10.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 172.16.20.1 255.255.255.0
R1(config-subif)#end

R1#show ip route

Test the connectivity using:

a. ping <target IP>
b. tracert <target IP>

Pas 8: În modul de simulare, folosind comanda *ping*, analizați comunicarea între gazdele din același VLAN și între gazdele din VLAN-uri diferite.

CAPITOLUL 11: REȚELE DE NIVEL 2, PROTOCOLUL SPANNING TREE, AGREGAREA LEGĂTURILOR ȘI ETHERCHANNEL

1. Obiective

La finalul capitolului, cititorii vor putea explica funcțiile switch-urilor, funcționarea protocoalelor spanning-tree și EtherChannel, precum și să configureze rețele de Nivel 2.

2. Considerații teoretice

Capitolul curent se concentrează pe nivelul de Legătură de Date al stivei ISO/OSI (Figura 11.1).

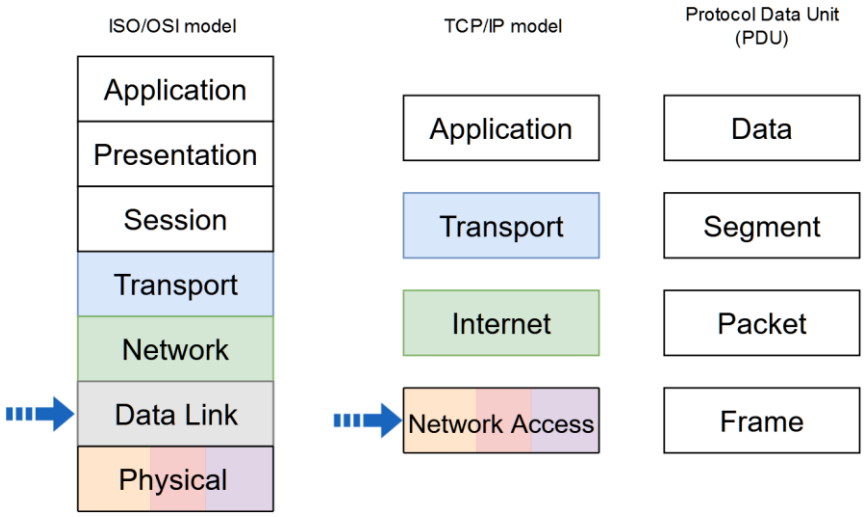


Figura 11.1 *Modele de stivă de rețea și denumire PDU în fiecare nivel. Săgețile indică nivelurile adresate în activitatea curentă*

2.1 Switch-uri și bridge-uri

Switch-urile și bridge-urile sunt dispozitive de nivel 2 care sunt utilizate pentru a crește lățimea de bandă disponibilă și pentru a reduce congestionarea rețelei. Switch-urile și bridge-urile efectuează două operațiuni de bază: comutarea cadrelor de date și menținerea operațiunilor de comutare. Acestea segmentează rețeaua LAN, creând domenii de coliziune mai mici. Fiecare port creează un segment, care este un domeniu de coliziune, deoarece switch-ul sau podul învață adresele MAC ale dispozitivelor conectate la fiecare port, introduce aceste informații într-un tabel de comutare sau bridging și redirecționează sau blochează traficul pe baza acelui tabel (figura 11.2). Segmentarea permite reducerea semnificativă a congestionării rețelei în cadrul fiecărui segment. Dispozitivele din cadrul acelui segment împart lățimea de bandă total disponibilă. Dacă switch-ul sau bridge-ul nu știe unde să trimită cadrul, acesta difuzează cadrul către toate porturile (operațiune de broadcast). Când este returnat un răspuns, switch-ul sau bridge-ul înregistrează noua adresă în tabelul de comutare sau bridging. Un alt avantaj al

conexiunii prin switch este că permite Ethernet full-duplex, ceea ce permite transmiterea unui pachet și recepționarea unui alt pachet în același timp. Dezavantajul dispozitivelor de nivel 2 este că acestea redirecționează cadrele de difuzare (broadcast) către toate dispozitivele conectate la rețea, astfel încât toate gazdele conectate la switch sau bridge fac parte în continuare din același domeniu de difuzare.

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0cd6.28a1    DYNAMIC     Fa0/2
   1    0002.4ab1.e29a    DYNAMIC     Fa0/9
   1    00d0.97a3.d6b5    DYNAMIC     Fa0/7
```

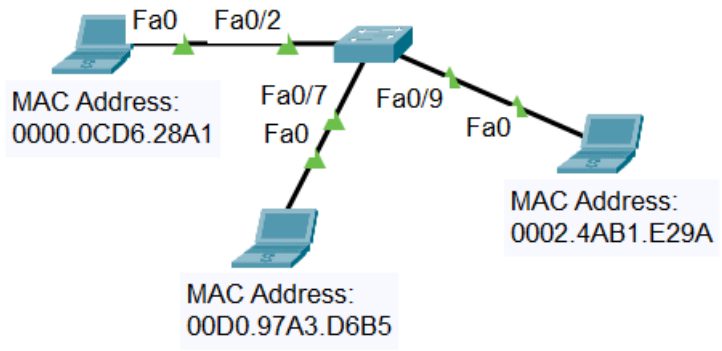


Figura 11.2 *Tabela de comutare*

Comutarea este clasificată ca fiind simetrică sau asimetrică. Comutarea simetrică oferă conexiuni comutate între porturi cu aceeași lățime de bandă. Comutarea asimetrică oferă conexiuni comutate între porturi cu lățimi de bandă diferite. Comutarea asimetrică permite alocarea unei lățimi de bandă mai mari portului de switch al serverului, pentru a preveni apariția unui blocaj (bottleneck).

Modurile de comutare sunt clasificate ca *store-and-forward (stocare și redirecționare)* sau *cut-through (redirecționare directă)*, fiecare mod reprezentând un compromis între latență și detectarea erorilor. În modul de comutare store-and-forward, întregul cadru este recepționat înainte de a începe orice redirecționare. Acest mod de comutare crește latența transmiterii și permite o detectare mai mare a erorilor. În modul de comutare cut-through, cadrul este redirecționat prin switch înainte ca întregul cadru să fie recepționat. Cel puțin adresa de destinație a cadrului trebuie citită înainte ca acesta să fie redirecționat. Acest mod de comutare scade latența transmiterii și permite o detectare mai redusă a erorilor. Modul de comutare cut-through are două forme: fast-forward și fragment-free. Comutarea fast-forward redirecționează pachetul după citirea adresei de destinație. Acest mod de comutare are cel mai scăzut nivel de latență și detectare a erorilor. Comutarea fragment-free redirecționează pachetul după citirea primilor 64 de octeți ai cadrului. Deoarece fragmentele rezultate din coliziuni sunt mai mici de 64 de octeți, modul de comutare fragment-free filtrează acest tip de eroare, care reprezintă și majoritatea erorilor de pachete. Acest mod de comutare are un nivel mai mare de latență și detectare a erorilor decât modul fast-forward.

2.2 Protocolul Spanning-Tree

Topologiile de rețea redundante cresc fiabilitatea rețelei prin introducerea de legături redundante. Aceste conexiuni introduc bucle fizice în rețea. Deoarece nivelul 2 nu are un mecanism pentru a elimina cadrele pierdute, acestea pot circula la nesfârșit într-o topologie de nivel 2 cu bucle, cauzând apariția a două tipuri de probleme: furtuna de difuzare (broadcast storm) și instabilitatea tabelei de comutare sau bridging. Furtuna de difuzare este creată de cadrele de difuzare care sunt trimise la nesfârșit către toate porturile switch-urilor sau podurilor, risipind lățimea de bandă sau făcând rețeaua inutilizabilă. Instabilitatea tabelei de comutare sau bridging apare atunci când mai multe copii ale unui cadru ajung la porturi diferite ale unui switch sau bridge, cauzând instabilitatea înregistrărilor MAC în tabelul de comutare sau bridging. Protocolul IEEE 802.1d Spanning-Tree utilizează algoritmul spanning-tree pentru a crea o topologie logică fără bucle și cu cea mai scurtă cale într-o topologie de nivel 2 cu bucle. Protocolul IEEE 802.1w Rapid Spanning-Tree utilizează un algoritm rapid de spanning-tree pentru a îndeplini aceeași funcție ca algoritmul spanning-tree, dar cu un timp de convergență mai scurt.

Protocolul Spanning-Tree utilizează mesaje multicast de nivel 2 Bridge Protocol Data Unit (BPDU) care sunt trimise de dispozitivele din rețea la fiecare două secunde, implicit. Structura acestor mesaje este prezentată în figura 11.3.

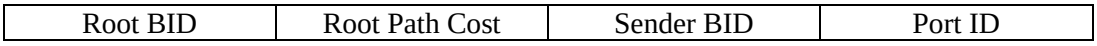


Figura 11.3 *Structura mesajului BPDU*

BID-ul este un câmp de 8 octeți. Cei doi octeți de ordin superior reprezintă prioritatea bridge-ului sau a switch-ului, care este implicit 32768, iar cei șase octeți de ordin inferior sunt adresa MAC a podului sau a switch-ului. Structura BID-ului este prezentată în figura 11.4.

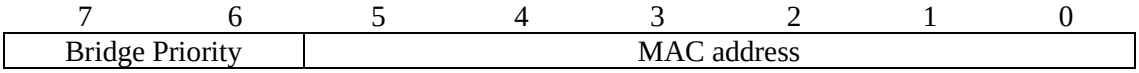


Figura 11.4 *Structura BID*

Protocolul Spanning-Tree calculează cea mai scurtă cale în rețea pe baza costurilor cumulative ale legăturilor. Costurile legăturilor sunt determinate în funcție de viteza legăturii. Unele dintre costurile pentru legături care depășesc 1 Gbps, specificate în standardul IEEE 802.1d, sunt prezentate mai jos, în Tabelul 11.1.

Tabelul 11.1 *Costurile de legătură definite de standardul IEEE 802.1D*

Viteza Legăturii	Cost
4Mbps	250
10Mbps	100
16Mbps	62
100Mbps	19
1Gbps	4
10Gbps	2

Unele dintre costurile pentru legături de 10 Gbps sau mai mari, specificate în standardul IEEE 802.1d, sunt prezentate Tabelul 11.2.

Tabelul 11.2 *Costurile de legătură definite de standardul IEEE 802.1w*

Viteza Legăturii	Cost
10Mbps	2000000
100Mbps	200000
1Gbps	20000
10Gbps	2000
1Tbps	20
10Tbps	2

Port ID-ul este un câmp de 2 octeți. Octetul de ordin superior reprezintă prioritatea portului, care este implicit 128, iar octetul de ordin inferior este numărul portului. Structura Port ID-ului este prezentată în figura 11.4.

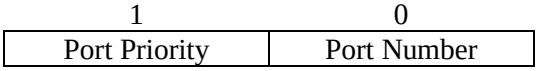


Figura 11.5 *Structura Port ID*

Protocolul Spanning-Tree stabilește un singur nod rădăcină, numit bridge rădăcină (root bridge), și construiește o topologie care are un singur traseu pentru a ajunge la fiecare nod din rețea. Arborele rezultat pornește de la bridge-ul rădăcină. Bridge-urile și switch-urile calculează cel mai scurt traseu de la ele însele până la podul rădăcină. Prima decizie pe care o iau toate bridge-urile sau switch-urile din rețea este identificarea bridge-ului rădăcină, care se face prin mesajele BPDU primite de toate bridge-urile și switch-urile. Toate celelalte decizii din rețea sunt luate în raport cu acest bridge rădăcină. Când un bridge sau un switch este pornit pentru prima dată, acesta presupune că este bridge-ul rădăcină și trimite mesaje BPDU care conțin adresa MAC a bridge-ului sau switch-ului atât în BID-ul rădăcină, cât și în BID-ul expeditorului. Dacă un bridge sau un switch primește un BPDU cu un BID rădăcină mai mic, acesta setează acest BID rădăcină în BPDU-urile care sunt trimise mai departe. Bridge-ul sau switch-ul cu cea mai mică valoare BID va fi bridge-ul rădăcină. Setarea priorității bridge-ului sau switch-ului la o valoare mai mică decât valoarea implicită va face ca BID-ul să fie mai mic și va influența identificarea bridge-ului rădăcină. Pentru fiecare segment LAN, Protocolul Spanning-Tree stabilește un switch desemnat ca fiind cel mai apropiat de bridge-ul rădăcină, care gestionează toate comunicațiile din acel LAN către bridge-ul rădăcină. Pentru fiecare bridge non-rădăcină, se alege un port rădăcină, care oferă cea mai bună cale către bridge-ul rădăcină. Astfel, portul cu cel mai mic cost al traseului către bridge-ul rădăcină este ales ca port rădăcină. Dacă mai multe porturi au același cost al traseului către bridge-ul rădăcină, portul cu cel mai mic Port ID este selectat ca port rădăcină. Protocolul Spanning-Tree selectează, de asemenea, porturile desemnate care fac parte din arborele cu cea mai scurtă cale. Astfel, portul cu cel mai mic cost al traseului către bridge-ul rădăcină este selectat ca port desemnat. Dacă mai multe porturi din segment au același cost al traseului, portul pe care bridge-ul sau switch-ul are cel mai mic ID de bridge sau switch este selectat ca port desemnat. Pe bridge-ul rădăcină, toate porturile sale sunt porturi desemnate. Legăturile redundante care nu fac parte din arborele cu cea mai scurtă cale sunt blocate, iar cadrele de date primite pe legăturile blocate sunt eliminate.

Fiecare port de pe un bridge sau switch care folosește Protocolul Spanning-Tree are unul dintre următoarele cinci stări: blocare (blocking), ascultare (listening), învățare (learning), redirecționare (forwarding) și dezactivat (disabled). În starea de blocare, porturile pot doar să primească BPDU-uri, cadrele de date sunt eliminate și nu pot fi învățate adrese. Poate dura până la 20 de secunde pentru a trece din această stare. Porturile trec de la starea de blocare la

starea de ascultare. În această stare, switch-urile sau bridge-urile determină dacă există alte căi către bridge-ul rădăcină. Calea care nu este cea mai eficientă către bridge-ul rădăcină revine la starea de blocare. În starea de ascultare, BPDU-urile sunt procesate, datele utilizatorului nu sunt redirecționate și adresele MAC nu sunt învățate. Perioada de ascultare este numită întârziere de redirecționare și durează 15 secunde. Porturile trec din starea de ascultare în starea de învățare. În această stare, BPDU-urile sunt procesate, datele utilizatorului nu sunt redirecționate, dar adresele MAC sunt învățate din orice trafic detectat. Starea de învățare este, de asemenea, numită întârziere de redirecționare și durează 15 secunde. Un port trece din starea de învățare în starea de redirecționare. În această stare, BPDU-urile sunt procesate, datele utilizatorului sunt redirecționate și adresele MAC continuă să fie învățate. Portul poate fi în starea dezactivată atunci când este oprit administrativ sau eșuează. Valorile de timp date pentru fiecare stare sunt valorile implicite. Aceste valori au fost calculate pe baza presupunerii că vor exista maximum șapte switch-uri în orice ramură a arborelui spanning-tree de la bridge-ul rădăcină. Când topologia rețelei se schimbă, switch-urile și bridge-urile recalculează arborele Spanning-Tree. Convergența către o nouă topologie spanning-tree folosind standardul IEEE 802.1D poate dura până la 50 de secunde.

2.3 EtherChannel

Agregarea legăturilor (Link aggregation) este capacitatea de a crea o legătură logică folosind mai multe legături fizice între două dispozitive. EtherChannel este o formă de agregare a legăturilor utilizată în rețelele cu switch-uri (figura 11.6). Aceasta permite redundanță și lățime de bandă mai mare prin partajarea sarcinii între legăturile fizice. EtherChannel creează o relație de tip unu-la-unu; adică, o legătură EtherChannel conectează doar două dispozitive. O legătură EtherChannel poate fi creată între două switch-uri sau o legătură EtherChannel poate fi creată între un server compatibil cu EtherChannel și un switch.

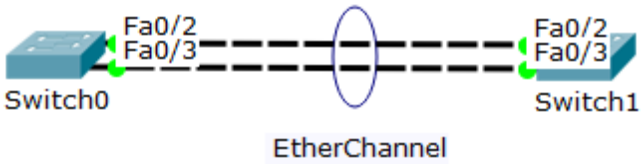


Figura 11.6 *EtherChannel*

Tehnologia EtherChannel a fost dezvoltată inițial de Cisco ca o tehnică de grupare a mai multor porturi fizice într-un singur canal logic pentru conexiuni între switch-uri LAN. Atunci când un EtherChannel este configurat, interfața virtuală rezultată se numește port channel. Interfețele fizice sunt grupate împreună într-o interfață de tip port channel (Figura 11.7). Majoritatea sarcinilor de configurare pot fi realizate pe interfața EtherChannel în loc de fiecare port individual, asigurând astfel consistența configurării pe toate legăturile.

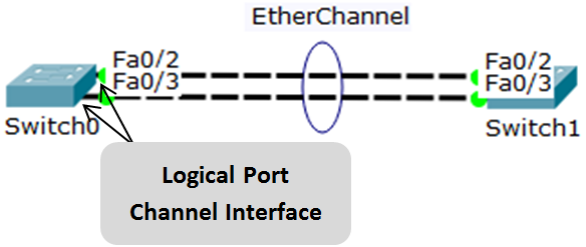


Figura 11.7 *Interfață Port channel*

EtherChannel se bazează pe porturile existente ale switch-ului. Nu este necesară actualizarea legăturii la o conexiune mai rapidă și mai scumpă pentru a obține o lățime de bandă mai mare. Echilibrarea sarcinii (load balancing) are loc între legăturile care fac parte din același EtherChannel. În funcție de platforma hardware, pot fi implementate una sau mai multe metode de echilibrare a sarcinii. Aceste metode includ echilibrarea sarcinii de la MAC-ul sursă la MAC-ul destinație sau de la IP-ul sursă la IP-ul destinație, pe legăturile fizice.

EtherChannel creează o agregare care este percepută ca o singură legătură logică. Atunci când există o singură legătură EtherChannel, toate legăturile fizice din EtherChannel sunt active deoarece STP (Spanning Tree Protocol) vede doar o singură legătură logică.

EtherChannel oferă redundanță deoarece legătura totală este percepută ca o singură conexiune logică. În plus, pierderea unei legături fizice din cadrul canalului nu generează o schimbare în topologie; prin urmare, nu este necesară o recalculare a arborelui spanning-tree. Atâta timp cât există cel puțin o legătură fizică prezentă, EtherChannel rămâne funcțional, chiar dacă debitul general scade din cauza unei legături pierdute în cadrul EtherChannel-ului. Costul spanning-tree este calculat pe baza numărului de porturi alocate port-channel-ului și nu se schimbă dinamic atunci când legăturile cad sau sunt reactivitate în cadrul port-channel-ului. Protocolul Spanning-Tree calculează cea mai scurtă cale în rețea pe baza costurilor cumulative ale legăturilor. Costurile legăturilor sunt determinate în funcție de viteza legăturii. Unele dintre costurile pentru legături specificate în standardul IEEE 802.1d sunt prezentate în tabelul 11.3.

Tabelul 11.3 *Costurile de legătură definite de standardul IEEE 802.1D*

Viteza legăturii	Cost (Short mode – 16bit)
10Mbps	100
100Mbps	19
Two-port * 100Mbps EtherChannel	9
Three-port * 100Mbps EtherChannel	8
Four-port * 100Mbps EtherChannel	7
Five-port * 100Mbps EtherChannel	6
Six-port * 100Mbps EtherChannel	5
Seven-port * 100Mbps EtherChannel	5
Eight-port * 100Mbps EtherChannel	5
1Gbps	4
Two-port * 1Gbps EtherChannel	3
Three-port * 1Gbps EtherChannel	2
Four-port * 1Gbps EtherChannel	2
Five-port * 1Gbps EtherChannel	2
Six-port * 1Gbps EtherChannel	2
Seven-port * 1Gbps EtherChannel	2
Eight-port * 1Gbps EtherChannel	1
10Gbps	2
Two-port * 10Gbps EtherChannel	1

Tipurile de interfețe nu pot fi amestecate; acestea trebuie să fie porturi Ethernet configurate compatibil. Configurația fiecărui port membru al grupului EtherChannel trebuie să fie consistentă pe ambele dispozitive. Dacă porturile fizice de pe o parte sunt configurate ca trunchiuri (trunks), porturile fizice de pe cealaltă parte trebuie, de asemenea, să fie configurate ca trunchiuri în cadrul aceluiași VLAN nativ. În plus, toate porturile din fiecare legătură EtherChannel trebuie să fie configurate ca porturi de Nivel 2. Fiecare EtherChannel are o interfață logică de tip port channel. O configurație aplicată interfeței port channel afectează

toate interfețele fizice care sunt atribuite acelei interfețe. EtherChannel-urile de Nivel 3 pot fi configurate pe switch-urile Cisco Catalyst multilayer. Un EtherChannel de Nivel 3 are o singură adresă IP asociată cu agregarea logică a porturilor switch-ului din EtherChannel.

Numărul maxim de porturi fizice într-o legătură EtherChannel depinde de platforma hardware a switch-ului și de versiunea IOS. De obicei, fiecare EtherChannel poate consta din până la 8 porturi Ethernet configurate compatibil.

Numărul maxim de EtherChannel-uri suportate de un switch depinde de platforma hardware și de versiunea IOS. Un switch Cisco IOS poate suporta, de obicei, 6 EtherChannel-uri.

EtherChannel poate fi configurat static, necondiționat sau poate fi format prin negociere folosind unul dintre cele două protocoale: Protocolul de Agregare a Porturilor (PAgP) sau Protocolul de Control al Agregării Legăturilor (LACP). Aceste protocoale permit porturilor cu caracteristici similare să formeze un canal prin negociere dinamică cu switch-urile adiacente.

PAgP este un protocol proprietar Cisco care ajută la crearea automată și gestionarea legăturilor EtherChannel. Există trei moduri pentru PAgP: on, desirable și auto. Modul on forțează interfața să formeze un canal fără PAgP. Modul desirable plasează o interfață într-o stare activă de negociere, în care interfața inițiază negocieri cu alte interfețe prin trimiterea de pachete PAgP. Modul auto plasează o interfață într-o stare pasivă de negociere, în care interfața răspunde pachetelor PAgP pe care le primește, dar nu inițiază negocierea PAgP. Figura 11.8 prezintă stabilirea canalului atunci când porturile switch-urilor S1 și S2 sunt în moduri diferite pentru PAgP.

S1	**S2**	**Stabilirea canalului**
On	On	Da
Auto/Desirable	Desirable	Da
On/Auto/Desirable	Not Configured	Nu
On	Desirable	Nu
Auto/On	Auto	Nu

Figura 11.8 *Stabilirea canalului cu PAgP*

LACP face parte dintr-o specificație IEEE (802.3ad) care permite gruparea mai multor porturi fizice pentru a forma un singur canal logic. LACP este, de asemenea, definit în standardul IEEE 802.1AX pentru rețele locale și metropolitane. LACP permite unui switch să negocieze automat un grup trimițând pachete LACP către dispozitivul partener. Acesta îndeplinește o funcție similară cu PAgP. Deoarece LACP este un standard IEEE, acesta poate fi utilizat pentru a facilita EtherChannel-uri în medii cu mai mulți furnizori. Există trei moduri pentru LACP: on, active și passive. Modul on forțează interfața să formeze un canal fără LACP. Modul active plasează un port într-o stare activă de negociere, în care portul inițiază negocieri cu alte porturi trimițând pachete LACP. Modul passive plasează un port într-o stare pasivă de negociere, în care portul răspunde pachetelor LACP pe care le primește, dar nu inițiază negocierea pachetelor LACP.

Figura 11.9 prezintă stabilirea canalului atunci când porturile switch-urilor S1 și S2 sunt în moduri diferite pentru LACP.

S1	S2	Stabilirea canalului
On	On	Da
Active/Pasive	Active	Da
On/Active/Passive	Not Configured	Nu
On	Active	Nu
Passive/On	Passive	Nu

Figura 11.9 *Stabilirea canalului cu LACP*

3. Desfășurarea lucrării practice

3.1 Discutați aspectele teoretice.

3.2 Configurare switch-uri

Switch-urile și routerele Cisco utilizează o interfață de linie de comandă (CLI) foarte similară, care este folosită pentru configurare și verificare.

Comanda de ajutor este semnul întrebării (?) care afișează lista de comenzi disponibile pentru modul curent de comandă, lista de comenzi care încep cu o anumită secvență de caractere sau lista de cuvinte cheie sau argumente asociate cu o anumită comandă.

Switch-urile au mai multe moduri de comandă. Modul User EXEC are un set limitat de comenzi care pot schimba setările terminalului, efectua teste de bază sau afișa informații despre sistem. Comanda `enable` este folosită pentru a trece din modul User EXEC în modul Privileged EXEC. Modul Privileged EXEC are un set mai mare de comenzi, care include setul de comenzi din modul User EXEC și comanda `configure`, folosită pentru a trece din modul Privileged EXEC în modul de configurare globală. Modul de configurare globală permite accesul la alte moduri de comandă, care sunt folosite pentru a configura switch-ul. Comanda `exit` este folosită pentru a ieși dintr-un mod de comandă și a reveni la modul anterior.

Rulați comanda `show running-config` pentru a vizualiza fișierul de configurație curent al switch-ului.

Intrați în modul Privileged EXEC cu comanda `enable`.

Rulați comanda copy running-config startup-config pentru a copia fișierul de configurație curent în fișierul de backup al configurației.

Pentru a șterge complet configurația switch-ului, trebuie urmați pașii următori:

- Ștergeți fișierul bazei de date VLAN `vlan.dat` din directorul flash cu comanda `delete flash:vlan.dat`.
- Ștergeți fișierul de backup al configurației `startup-config` cu comanda `erase startup-config`.
- Reporniți switch-ul cu comanda `reload`.

Treciți din modul Privileged EXEC în modul de configurare globală cu comanda `configure terminal`.

Setați numele switch-ului cu comanda `hostname nume_host`.

Switch# enable
Switch# configure terminal
Switch(config)# hostname SWITCH_EXAMPLE

Configurați linia terminalului principal cu următoarele comenzi:

Switch(config)# line console 0
Switch(config-line)# password password
Switch(config-line)# login
Switch(config-line)# exit

Configurați terminalul virtual cu următoarele comenzi:

Switch(config)# line vty 0 4
Switch(config-line)# password secret_password
Switch(config-line)# login
Switch(config-line)# exit

Pentru a permite accesul la switch prin aplicații TCP/IP, trebuie setate adrese IP și un default gateway. Acest lucru permite configurarea switch-ului folosind o conexiune telnet sau ssh. Spre deosebire de routere, în cazul switch-urilor, adresele IP sunt configurate pe interfețele VLAN. Configurați adresele IP și default gateway cu următoarele comenzi:

Switch(config)# interface VLAN1
Switch(config-if)# ip address ip_address netmask
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway default_gateway_address

3.3 Spanning Tree

Pas 1: Configurați rețeaua prezentată în Figura 11.10. Dacă LED-ul portocaliu al portului din topologie nu este în aceeași poziție ca în imagine, mutați switch-urile astfel încât LED-ul portocaliu al portului să fie așa cum este în figură..

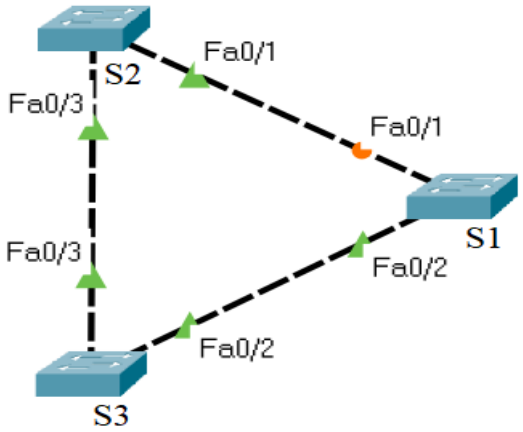


Figure 11.10 *Topologia rețelei de test*

1. Specificați numele gazdă pentru switch-uri
2. Examinați configurația Spanning Tree
   - LED-ul portului este de culoare verde dacă portul este în starea de forwarding, în timp ce LED-ul portului este de culoare portocalie dacă portul este în starea de blocare.
   - Consultați informațiile Spanning Tree pe fiecare switch, utilizând comanda corespunzătoare. Examinați și explicați rezultatul comenzii.

Sintaxa generală:
Switch# show spanning-tree

Descriere: Afișează informațiile Spanning Tree

3. Răspundeți la următoarele întrebări:
   - De ce această topologie este utilă și implementată în rețelele de calculatoare?
   - Care switch este root bridge și de ce?

Pas 2: La topologia anterioară, conectează utilizatorii la switch-urile S2 și S3 și adaugă routerul care conectează rețeaua la alte rețele, așa cum este ilustrat în Figura 11.11. În acest fel, se obține o topologie de tip stea extinsă cu o cale de backup.

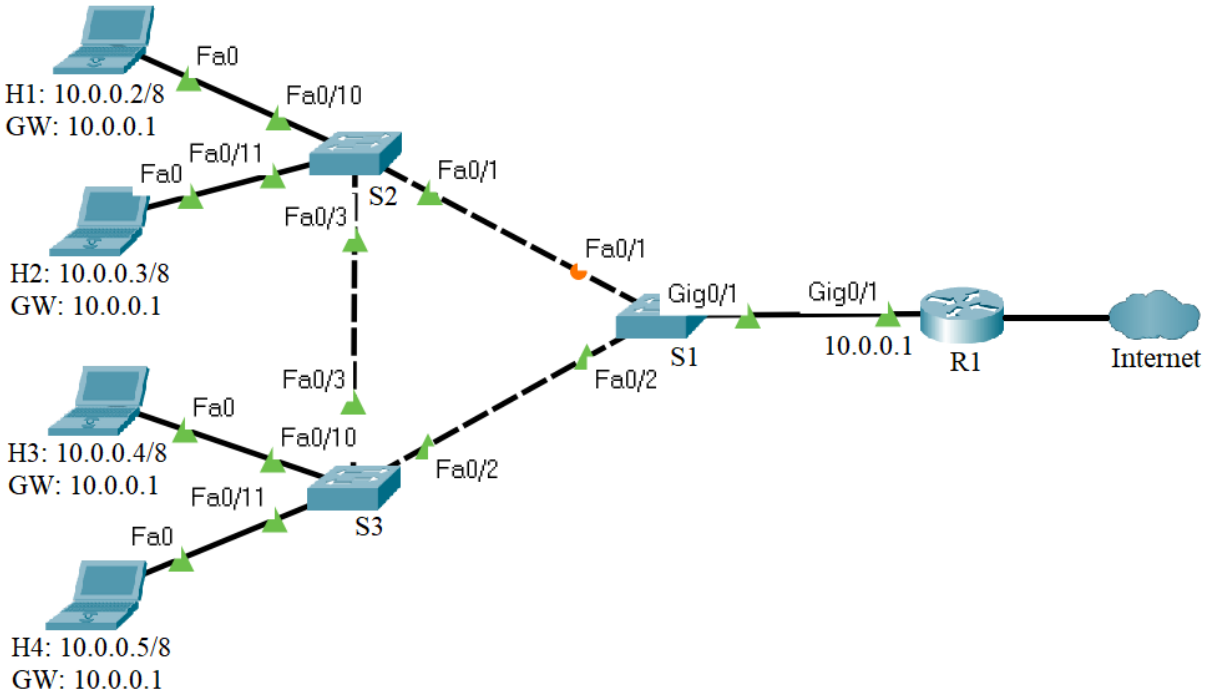


Figure 11.10 *Topologia rețelei de test*

Înainte de a configura dispozitivele de rețea, discutați despre atribuirea adreselor IPv4 în Tabelul 11.4:

Tabelul 11.4 *Adrese IPv4 pentru rețeaua de testare*

Dispozitiv	Interfață	Adresă IP	Netmask	Gateway
Laptop H1	Fa0	10.0.0.2	255.0.0.0	10.0.0.1
Laptop H2	Fa0	10.0.0.3	255.0.0.0	10.0.0.1
Laptop H3	Fa0	10.0.0.4	255.0.0.0	10.0.0.1
Laptop H4	Fa0	10.0.0.5	255.0.0.0	10.0.0.1
R1	Gig0/1	10.0.0.1	255.0.0.0	-

1. Specificați numele gazdă pentru router
2. Atribuiți informațiile IP gazdelor și routerului
3. Testați conectivitatea între gazde și router folosind comanda *ping*
4. Analizați rețeaua și răspundeți la următoarele întrebări:
   - Care cale ar trebui să fie calea de backup (legătura redundantă) și de ce?
   - Care switch ar trebui să fie root bridge pentru a obține căile optime în rețeaua de nivel 2?
   - Ce configurație ar trebui realizată pentru ca un anumit switch să devină root bridge, indiferent de adresele MAC ale switch-urilor din rețea?
5. Schimbați switch-ul root modificând prioritatea acestuia la o valoare mai mică decât valoarea implicită

Sintaxă generală:

Switch(config)# spanning-tree vlan vlan_number priority priority_number

Descriere: Schimbă prioritatea Spanning-tree a switch-ului

Considerați: switch *S1*, vlan *1* și priority *0*

6. Emiteți comanda *show spanning-tree* (Figura 11.12) de mai multe ori pentru a vizualiza informațiile Spanning Tree pe switch-ul S1

- Acordați atenție următoarelor aspecte:
  - Switch-ul S1 devine root bridge
  - Portul aflat în starea de blocare trece în starea de forwarding, trecând prin stările de listening și learning

```
S1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     00E0.F7B4.DDC2
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1  (priority 0 sys-id-ext 1)
              Address     00E0.F7B4.DDC2
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------------------------
Fa0/1            Desg LRN 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Gi0/1            Desg FWD 4         128.25   P2p
```

Figura 11.12 *Ieșirea comenzii show spanning-tree pentru S1*

➢ În topologia rețelei, LED-ul portului portocaliu devine verde, în timp ce un LED de port între switch-urile S2 și S3 devine portocaliu (Figura 11.13). Legătura dintre S1 și S2 transmite traficul, în timp ce legătura dintre S2 și S3 devine calea de backup, legătura redundantă. Emite comanda `show spanning-tree` (Figura 11.14) pentru a vizualiza informațiile Spanning Tree pe switch-ul care are LED-ul portului portocaliu.

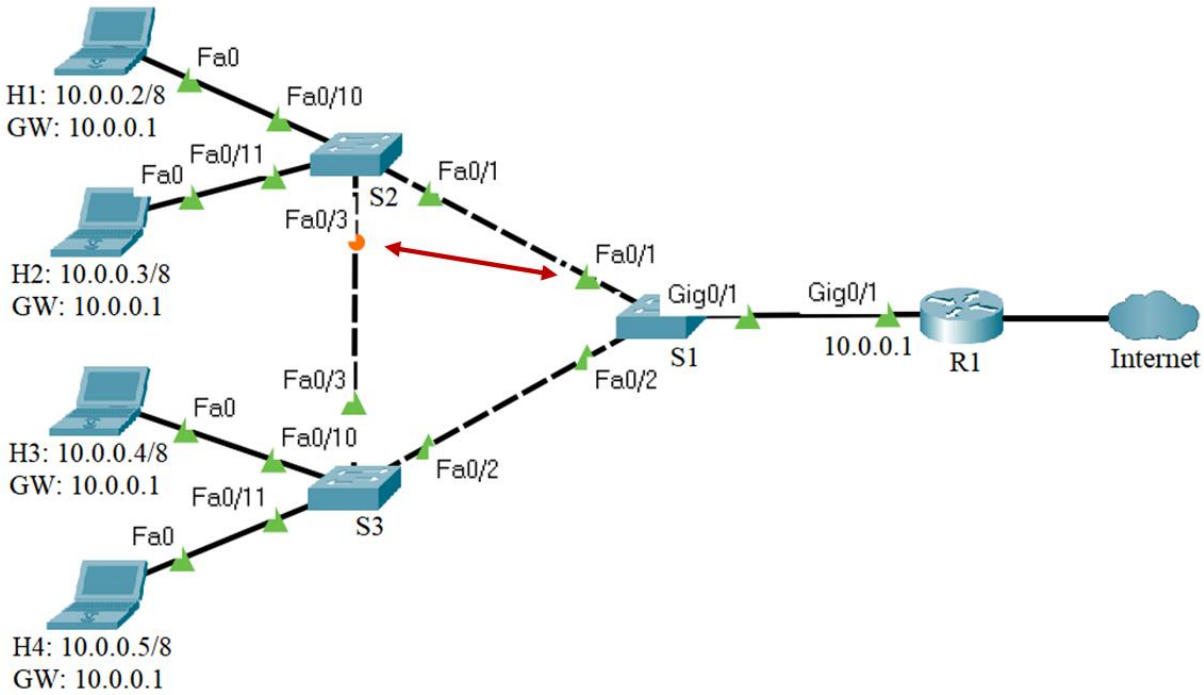


Figura 11.13 *STP schimbă starea porturilor*

```
S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     00E0.F7B4.DDC2
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.D349.4CEC
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
```

Figure 11.14 *Ieșirea comenzii Show spanning-tree pentru switchul care are LED-ul portului portocaliu*

7. Testați continuu conectivitatea între gazda H1 și router folosind comanda *ping* cu opțiunea *-t* (Figura 11.15).

```
C:\>ping
Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target

C:\>ping -t 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
```

Figura 11.15 *Test de conectivitate între gazda H1 și router*

8. În timp ce comanda *ping* testează conectivitatea între gazda H1 și router, deconectați legătura dintre switch-urile S1 și S2 (Figura 11.16).

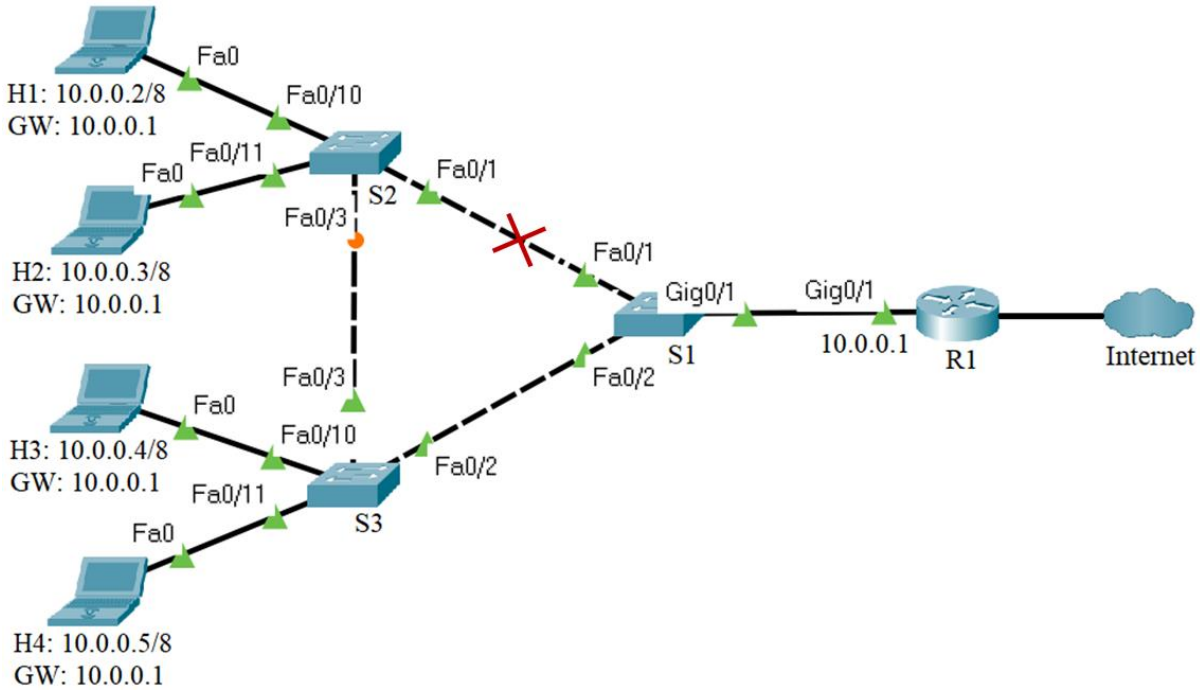


Figura 11.16 *Eliminarea legăturii dintre comutatoarele S1 și S2*

➢ Emiteți comanda *show spanning-tree* (Figura 11.17)de mai multe ori pentru a vizualiza informațiile Spanning Tree pe switch-ul S2; acordați atenție portului aflat în starea de blocare, acesta trece în starea de forwarding, trecând prin stările de listening și learning.

```
S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     00E0.F7B4.DDC2
              Cost        38
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.D349.4CEC
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/3            Root LSN 19        128.3    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
```

Figura 11.17 *Ieșirea comenzii show spanning-tree pentru S2*

➢ În topologia rețelei, LED-ul portului portocaliu devine verde (Figura 11.18), iar legătura dintre S2 și S3 transmite traficul.

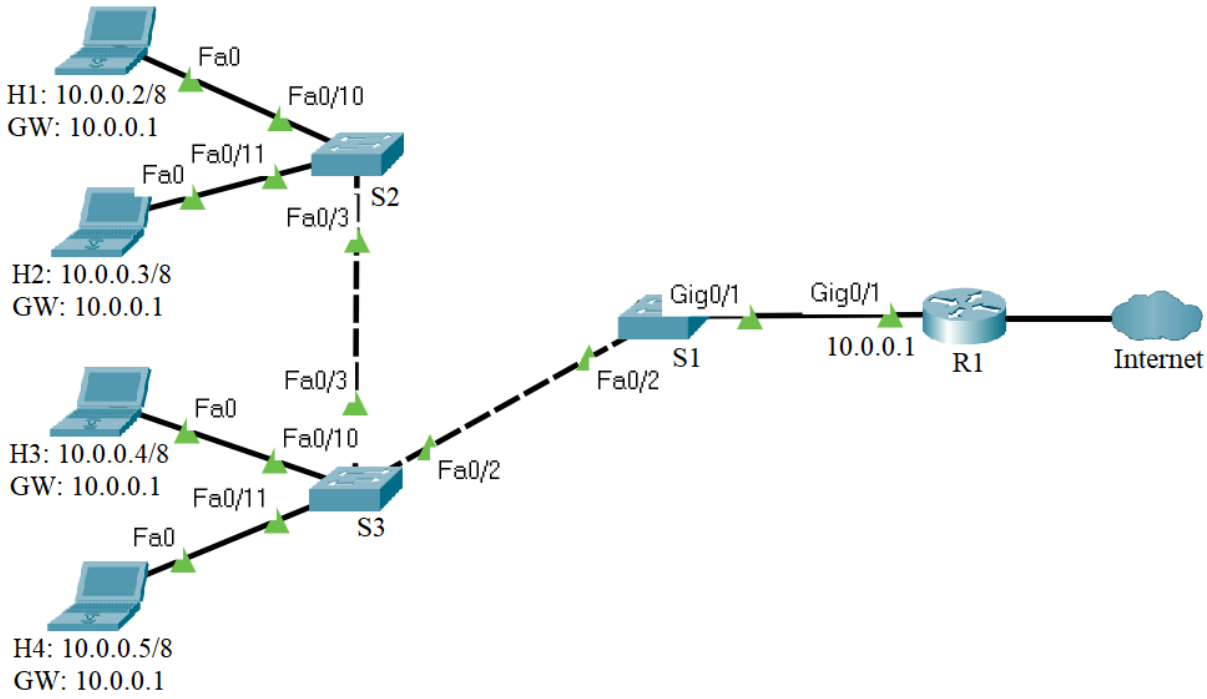


Figura 11.18 *STP schimbă starea porturilor*

➢ Protocolul Spanning Tree restabilește conectivitatea între gazda H1 și router prin legătura redundantă (Figura 11.19).

```
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.0.0.1: bytes=32 time=27ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
```

Figura 11.19 *Test de conectivitate între gazda H1 și router*

9. Restabiliți legătura dintre switch-urile S1 și S2 și observați cum protocolul Spanning Tree alege cele mai scurte căi către root bridge și blochează legăturile redundante (Figura 11.20).

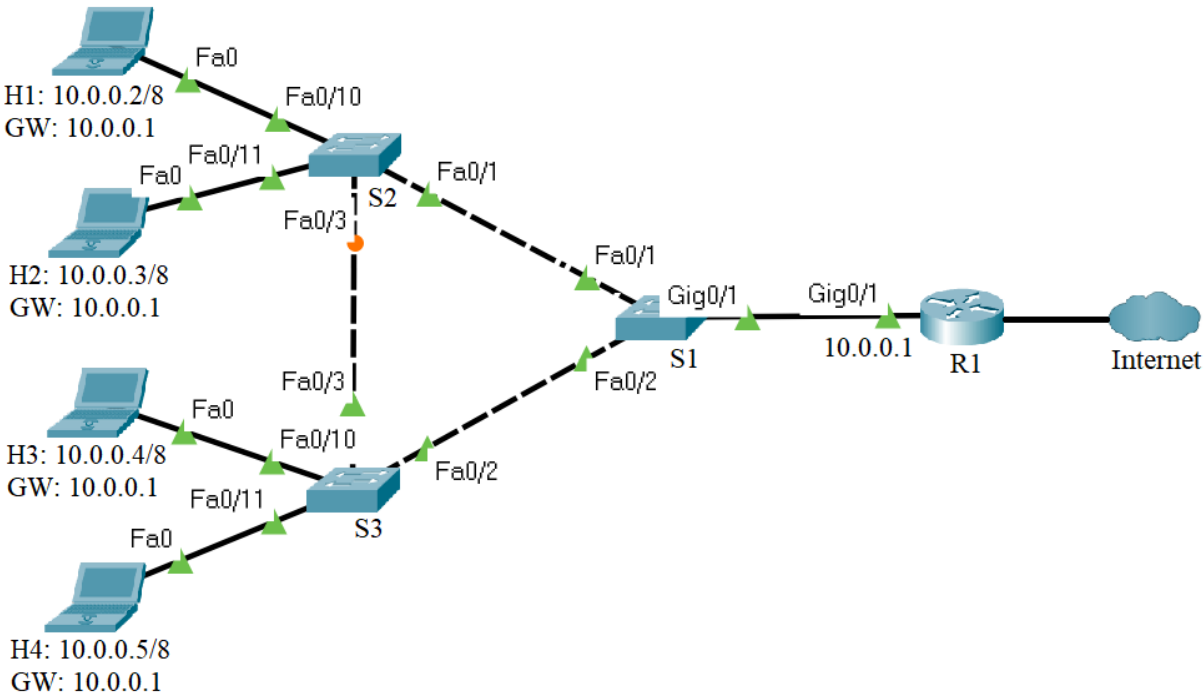


Figura 11.20 *Restabilirea legăturii dintre S1 și S2*

3.4 EtherChannel

Conectați cablurile conform rețelei prezentate în figura de mai jos.

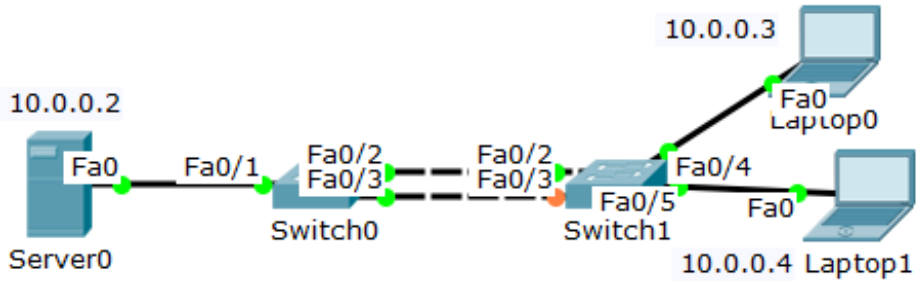


Figure 11.21 *Topologia rețelei de test*

Înainte de a configura dispozitivele de rețea, discutați despre atribuirea adreselor IPv4 în Tabelul 11.5:

Tabelul 11.5 *Adrese IPv4 pentru rețeaua de testare*

Dispozitiv	Intefață	Adresă IP	Netmask
Server0	Fa0	10.0.0.2	255.0.0.0
Laptop 0	Fa0	10.0.0.3	255.0.0.0
Laptop 1	Fa0	10.0.0.4	255.0.0.0

1. Configurați adresele IP pe gazde.
2. Verificați conectivitatea între laptopuri și Server0 folosind comanda `ping`.
3. Conectați-vă la Switch0 și intrați în modul Privileged EXEC. Vizualizați informațiile Spanning Tree cu comanda `show spanning-tree`. Examinați și explicați rezultatul acestei comenzi.

Switch0#show spanning-tree

4. Repetați pasul anterior și pentru Switch1.
5. Conectați-vă la Switch0 și specificați interfețele care compun grupul EtherChannel folosind comanda `interface range` în modul de configurare globală a interfeței. Creați interfața port channel cu comanda `channel-group identifier mode on` în modul de configurare a intervalului de interfețe. Identificatorul specifică numărul de grupului de canale.

Switch0(config)#interface range fastEthernet 0/2-3
Switch0(config-if-range)#channel-group 1 mode on

6. Repetați pasul anterior și pentru Switch1.

Conectați-vă la Switch0 și intrați în modul Privileged EXEC. Vizualizați fișierul running-config folosind comanda `show running-config`. Examinați și explicați rezultatul acestei comenzi. Vizualizați informațiile EtherChannel folosind comanda `show etherchannel summary`. Examinați și explicați rezultatul acestei comenzi. Vizualizați informațiile Spanning Tree folosind comanda `show spanning-tree`. Examinați și explicați rezultatul acestei comenzi.

Switch0#show running-config
Switch0#show etherchannel summary
Switch0#show spanning-tree

7. Repetați pasul anterior și pentru Switch1.
8. Conectați-vă la Switch0 și intrați în modul de configurare a interfeței port channel folosind comanda `interface port-channel`, urmată de identificatorul interfeței. Configurați EtherChannel ca interfață trunk folosind comanda `switchport mode trunk`.

Switch0(config)#interface port-channel 1
Switch0(config-if)#switchport mode trunk

9. Repetați pasul anterior și pentru Switch1.
10. Conectați-vă la Switch0 și intrați în modul Privileged EXEC. Vizualizați fișierul running-config folosind comanda show running-config. Examinați și explicați rezultatul acestei comenzi. Vizualizați informațiile despre trunking folosind comanda show interfaces trunk. Examinați și explicați rezultatul acestei comenzi.

Switch0#show running-config
Switch0#show interfaces trunk

11. Repetați pasul anterior și pentru Switch1.
12. Conectați-vă la Switch0 și configurați metoda de balansare a încărcării pentru EtherChannel folosind comanda `port-channel load-balance` în modul de configurare globală. Selectați metoda de distribuire a încărcării bazată pe adresa MAC a gazdei de destinație a pachetului primit (`dst-mac`). Intrați în modul Privileged EXEC și vizualizați informațiile despre metoda de balansare a încărcării pentru EtherChannel folosind comanda `show etherchannel load-balance`. Examinați și explicați rezultatul acestei comenzi.

Switch0(config)#port-channel load-balance dst-mac
Switch0(config)#end
Switch0#show etherchannel load-balance

CAPITOLUL 12: AMENINȚĂRI DE SECURITATE ÎN REȚELELE DE CALCULATOARE

1. Obiective

Acest capitol demonstrează principiile de lucru ale câtorva amenințări de securitate folosind instrumentul Cisco Packet Tracer. Într-un scenariu din viața reală ar putea fi necesare instrumente suplimentare pentru a efectua aceste atacuri, dar obiectivul acestei activități de laborator este doar academic. Scopul dorit este de a înțelege cum sunt implementate anumite atacuri și care sunt cele mai bune modalități de a preveni producerea lor.

2. Consideraţii teoretice

Capitolul curent se concentrează pe straturile de legături de date, rețea și aplicații ale stivei ISO/OSI (Figura 12.1).

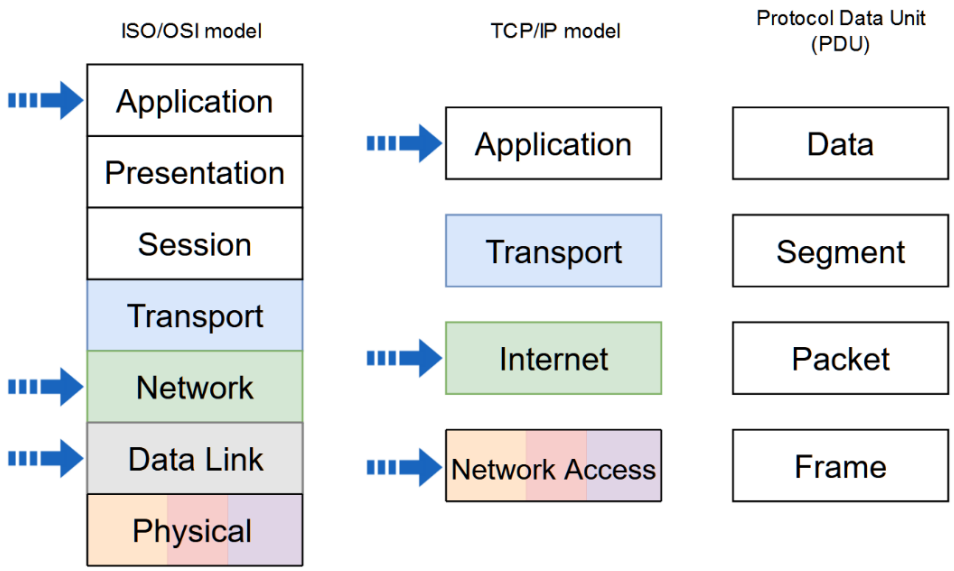


Figura 12.1 *Modele de stivă de rețea și denumire PDU în fiecare nivel. Săgețile indică nivelurile adresate în activitatea curentă*

Principalele concepte care sunt abordate în acest capitol sunt următoarele:

- **ARP spoofing**: Acesta este procesul prin care un dispozitiv rău intenționat își falsifică propria adresă MAC, ceea ce înseamnă că își maschează propria adresă MAC cu o adresă MAC diferită care poate aparține unui dispozitiv de rețea diferit. Pentru a informa celelalte dispozitive despre adresa MAC falsă, dispozitivul rău intenționat trimite un ARP gratuit celorlalte gazde de rețea, informându-le despre adresa MAC care se află la o anumită adresă IP. După ce fiecare gazdă de rețea primește răspunsul ARP, va stoca noua pereche de adrese IP - MAC în propria tabelă ARP cache și când va trimite un pachet către respectivul dispozitiv, va completa antetul Layer 2 cu adresa MAC falsificată.

- **Network sniffer:** Un sniffer de rețea este un dispozitiv care poate intercepta traficul de rețea și îl poate înregistra folosind instrumente de monitorizare a traficului.
- **Denial of Service (DoS):** Acesta este un tip de atac care are scopul de a restricționa accesul la funcțiile normale ale rețelei.
- **Rogue server:** Un server necinstit (rogue) nu aparține instituției (sau părților interesate) care deține rețeaua. Un astfel de server poate oferi diverse servicii și informații nevalide dispozitivelor din rețea cu intenții rău intenționate.
    - **Rogue web server:** poate oferi pagini web care arată ca un site web real, dar sunt de fapt copii ale unui site real
    - **Rogue DHCP server:** poate oferi adresare nevalidă, de ex. gateway implicit greșit pentru a refuza accesul altor gazde la internet, server DNS greșit pentru a face gazdele să acceseze un server web invalid
    - **Rogue DNS server:** adresa IP cu scopul de a forța utilizatorii să acceseze un server web fals care aparent se află la o adresă URL validă
- **Phishing:** Un tip de atac menit să fure informații printr-un mesaj sau un site web fraudulos.

3. Desfăşurarea lucrării practice

3.1. ARP spoofing pentru DoS și data sniffing

Un exemplu de atac ARP spoofing cu scopul final de a interzice accesul la anumite resurse și de a permite sniffingul de date poate fi văzut în Figura 12.2:

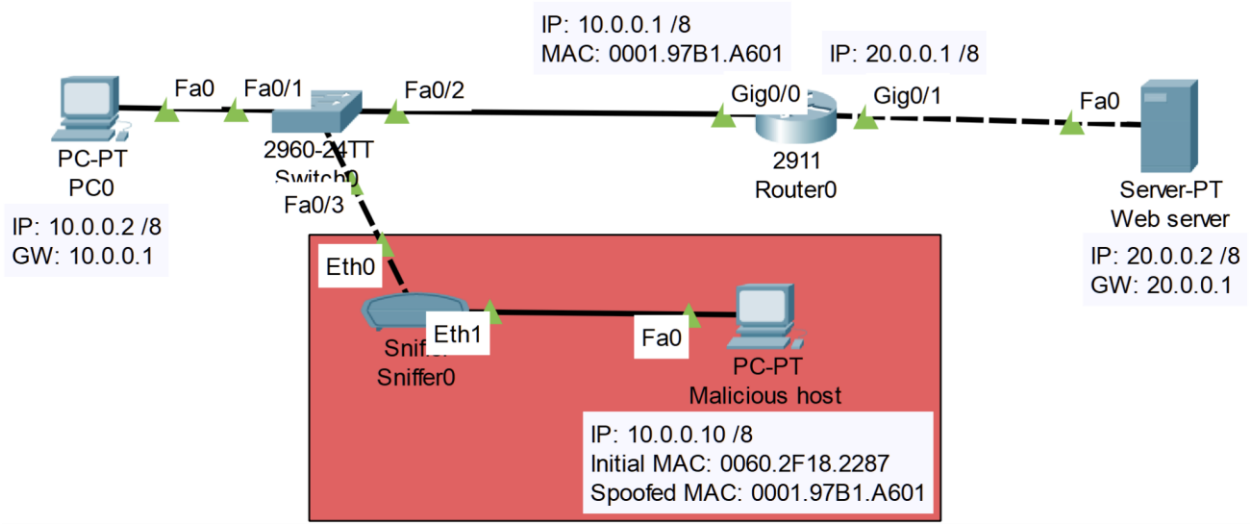
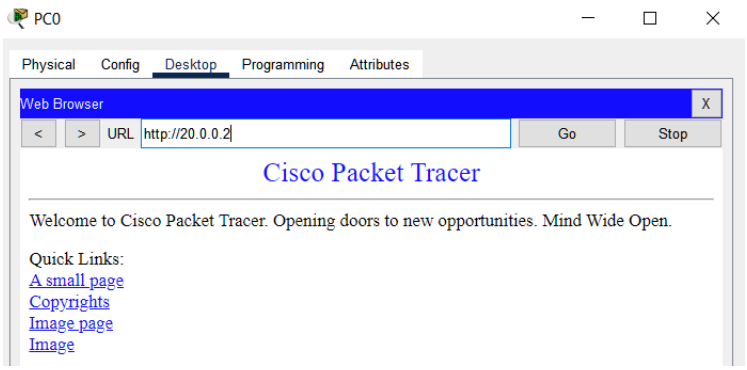
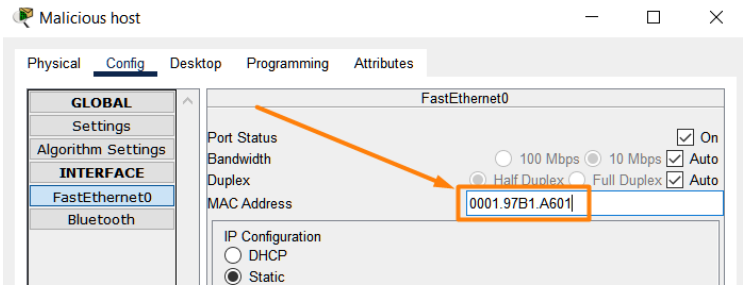
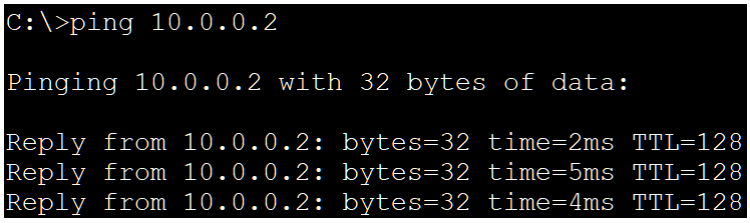
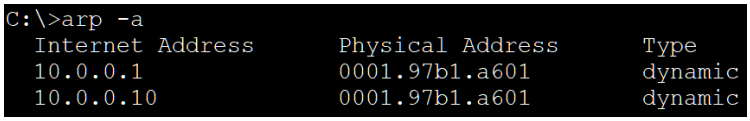
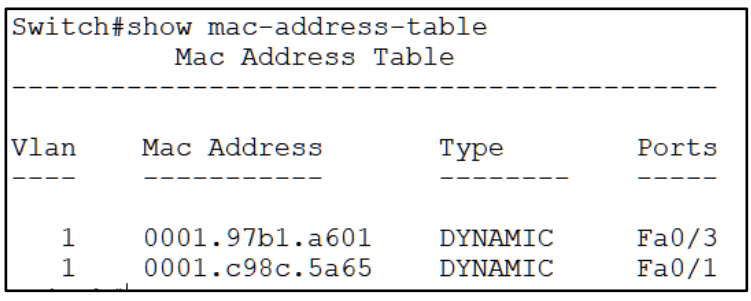
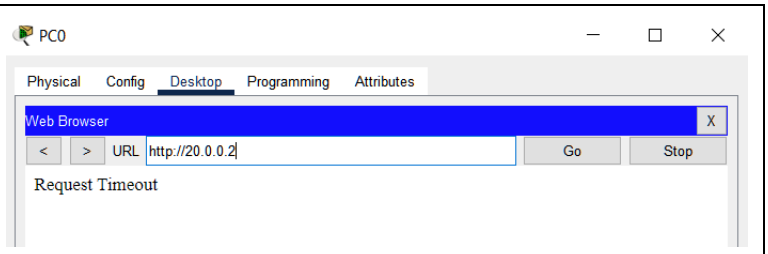
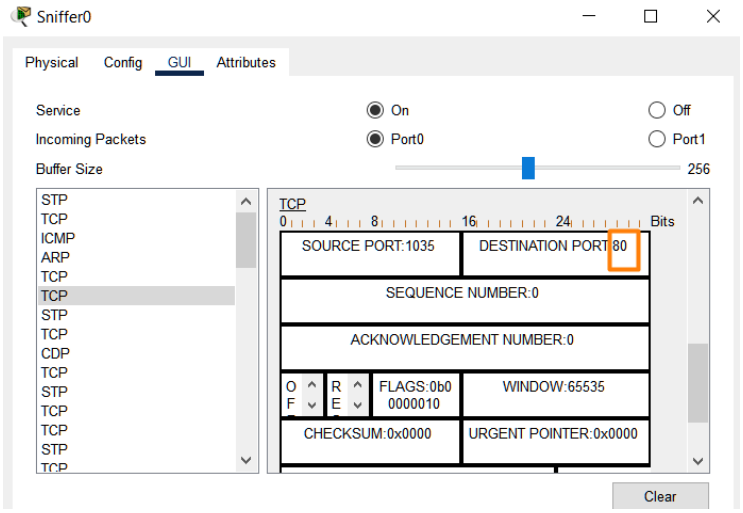


Figura 12.2 *Topologia atacurilor de rețea: falsificarea ARP pentru DoS și detectarea datelor*

Pentru a efectua atacul, configurați topologia în Packet Tracer, apoi urmați pașii descriși mai jos (Tabel 12.1).

1.	Un server web se află la adresa IP 20.0.0.2. Accesând pagina web implicită de pe PC0 având adresa IP 10.0.0.2, imaginea Cisco Packet Tracer va arăta ca în figura din dreapta	
2.	Figura arată că interfața Gig 0/0 a routerului are adresa MAC: 0001.97B1.A601 Gazda rău intenționată își poate suprascrie adresa MAC cu cea a routerului	
3.	Următorul pas pentru gazda rău intenționată este să informeze celelalte dispozitive de rețea din rețea că adresa MAC a routerului corespunde de fapt adresei IP a gazdei rău intenționate. Acest lucru se poate realiza prin generarea de trafic continuu în rețea, de ex. folosind comanda ping cu parametrul -t	
4.	Apoi, intrările ARP cache de pe celelalte dispozitive din rețea pot fi verificate (pe PC0 având adresa IP 10.0.0.2 și pe switch) Vizualizând aceste informații se poate observa că hostul va adăuga aceeași adresă MAC atunci când generează trafic către gateway sau către gazda rău intenționată, dar switchul va redirecționa traficul pe interfața Fa 0/3 care face legătura către gazda rău intenționată (dacă tabela de adrese MAC nu se modifică, utilizați comanda *#clear mac-address-table*)	 

5.	În continuare, când PC0, având adresa IP 10.0.0.2, încearcă să acceseze serverul web, va crea un pachet având adresa MAC corectă a gateway-ului de rețea (interfața Gig 0/0 pe router), dar switchul va redirecționa acest pachet către gazda rău intenționată prin intermediul sniffer-ului de rețea	
6.	Sniffer-ul poate fi, de asemenea, deschis și inspectat GUI-ul său. Traficul TCP care este generat de la computer către serverul web poate fi inspectat. Nu se văd prea multe informații în acest exemplu Cisco Packet Tracer, dar un test din viața reală poate dezvălui fluxuri multiple de trafic generate de computerul vizat	

După analizarea întregii secvențe de pași, atacul ARP spoofing a avut succes, având ca rezultat refuzul serviciului către serverul web și interceptarea traficului generat de computer.

Modalitățile posibile de a depăși aceste amenințări de securitate includ (dar nu se limitează la):

- Limitarea numărului de adrese MAC permise pe portul switchului
- Configurarea inspecției consistenței adreselor MAC - IP

Cercetați alte mecanisme pentru a preveni ARP spoofing.

3.2. ARP spoofing pentru phishing

Un exemplu de atac de tip phishing de la un server web poate fi văzut în figura de mai jos, unde un atacator se conectează la rețea cu un router (cu o adresă IP statică) și un server web de phishing în rețeaua din spatele routerului conectat:

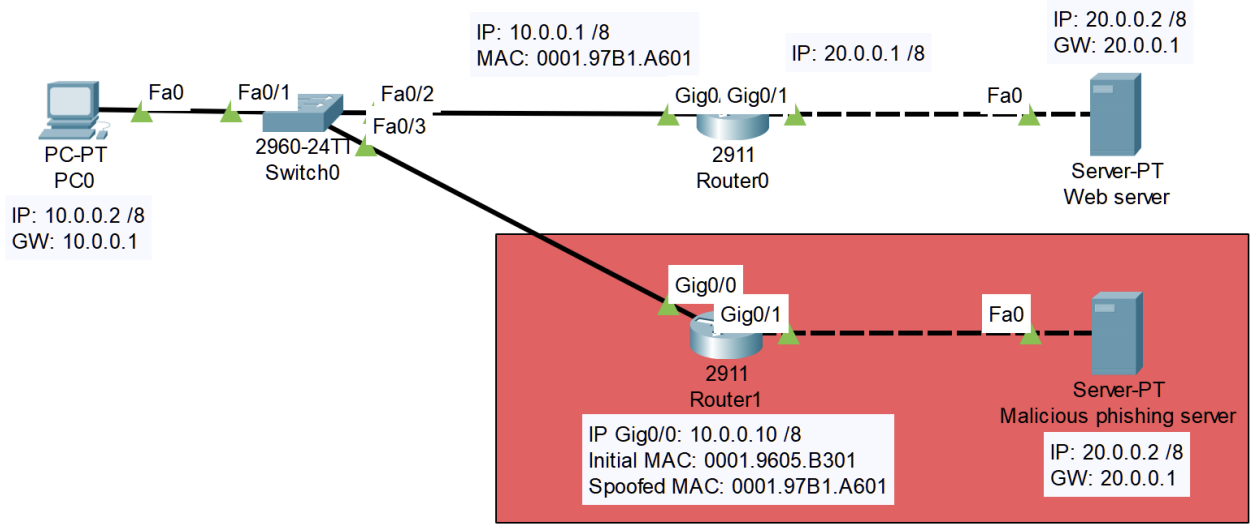
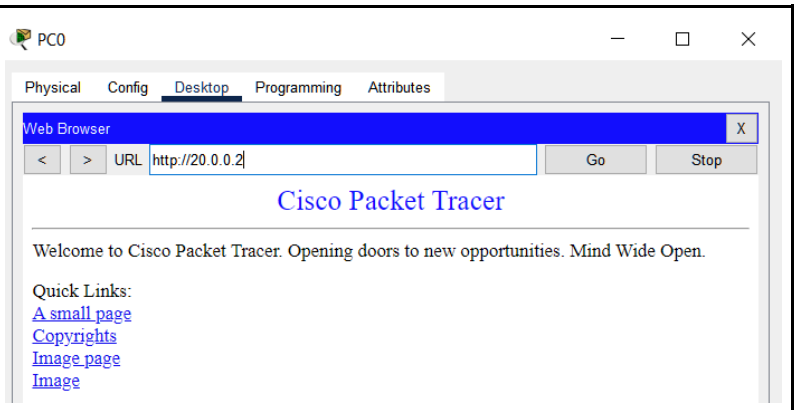
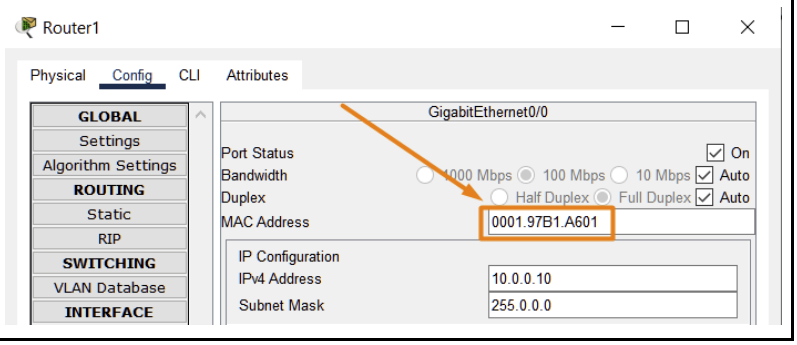


Figura 12.3 Topologia atacurilor de rețea: *falsificarea ARP pentru phishing*

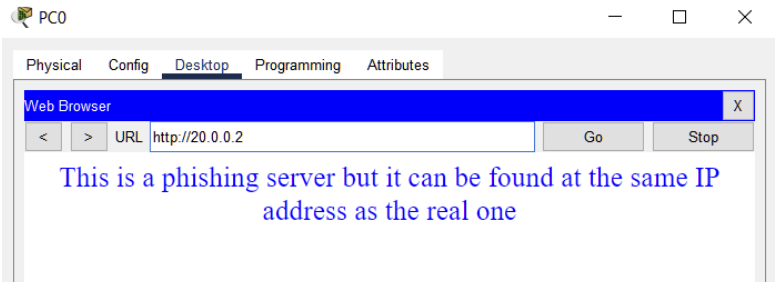
Pentru a efectua atacul, configurați topologia în Packet Tracer, apoi urmați pașii descriși mai jos (Tabel 12.2).

Tabelul 12.2 *Falsificarea ARP pentru etapele atacului de phishing*

1.	Un server web se află la adresa IP 20.0.0.2. Accesând pagina web implicită de pe PC0 având adresa IP 10.0.0.2, imaginea Cisco Packet Tracer va arăta ca în figura din dreapta	
2.	Figura arată că interfața Gig0/0 a Router0 are adresa MAC: 0001.97B1.A601 Actorul rău intenționat se conectează la rețea cu un router unde adresa MAC este suprascrisă cu adresa MAC a Router0	

3.	Următorul pas pentru actorul rău intenționat este să informeze celelalte dispozitive de rețea din rețea că adresa MAC a Router0 corespunde de fapt router-ului Router1 (routerul rău intenționat). Acest lucru se poate realiza prin generarea de trafic continuu în rețea, de ex. folosind comanda ping din CLI-ul Router1, așa cum se arată în imaginea din dreapta	`Router1#ping 10.255.255.255`
		
		`Type escape sequence to abort.`
		`Sending 5, 100-byte ICMP Echos to 10.255.255.255, timeout is 2 seconds:`
		
		`Reply to request 0 from 10.0.0.2, 0 ms`
		`Reply to request 1 from 10.0.0.2, 0 ms`
		`Reply to request 2 from 10.0.0.2, 0 ms`
		`Reply to request 3 from 10.0.0.2, 0 ms`
		`Reply to request 4 from 10.0.0.2, 0 ms`
		
		`Router1#ping 10.0.0.2`
		
		`Type escape sequence to abort.`
		`Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:`
		`!!!!!`
		`Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/13 ms`
		
		`Router1#`

4.	Apoi, intrările cache ARP de pe celelalte dispozitive din rețea pot fi verificate (pe PC0 având adresa IP 10.0.0.2 și pe switch)
	
	Văzând aceste informații se poate observa că hostul va adăuga aceeași adresă MAC atunci când generează trafic către gateway-ul Router1, dar switch-ul va redirecționa de asemenea traficul pe interfața Fa 0/3 care face legătura către Router1 (dacă tabela de adrese MAC nu se modifică, utilizați comanda *#clear mac-address-table*)
		`C:\>arp -a`
		`  Internet Address  Physical Address  Type`
		`  10.0.0.1  0001.97b1.a601  dynamic`
		`  10.0.0.10  0001.97b1.a601  dynamic`
		
		`Switch#show mac-address-table`
		`Mac Address Table`
		`----------`
		
		`Vlan  Mac Address  Type  Ports`
		`----  -----------  --------  -----`
		
		`1  0001.97b1.a601  DYNAMIC  Fa0/3`
		`1  0001.c98c.5a65  DYNAMIC  Fa0/1`

5.	Apoi, când PC0 va încerca să acceseze serverul web, va crea un pachet având adresa MAC corectă a gateway-ului de rețea (interfața Gig 0/0 pe Router0), dar switch-ul va redirecționa acest pachet către Router1. După ce pachetul ajunge la Router1, actorul rău intenționat a creat deja o rețea simulată care imită aceleași adrese IP ca în rețeaua reală, dar creează un site web de phishing care arată conținut diferit, dar care este încă accesibil pe aceeași adresă IP.	

După analizarea întregii secvențe de pași, atacul ARP spoofing a avut succes cu rezultatul de a face gazda vizată să acceseze un server fals care poate realiza scenarii de phishing dacă este configurat de ex. să accepte introducerea credențialelor.

Una dintre cele mai indicate modalități de a depăși această problemă este de a o preveni/evita în întregime prin neaccesarea site-urilor web nesecurizate din rețele nesigure sau prin neintroducerea informațiilor de acreditare sensibile atunci când sunt prezente într-o rețea nesigură.

Cercetați alte mecanisme pentru a preveni ARP spoofing și phishing.

3.3. Servere rogue DHCP si DNS pentru phishing

Un exemplu de atac de tip phishing care este efectuat cu ajutorul unui server DHCP și DNS rogue poate fi văzut în Figura 12.4::

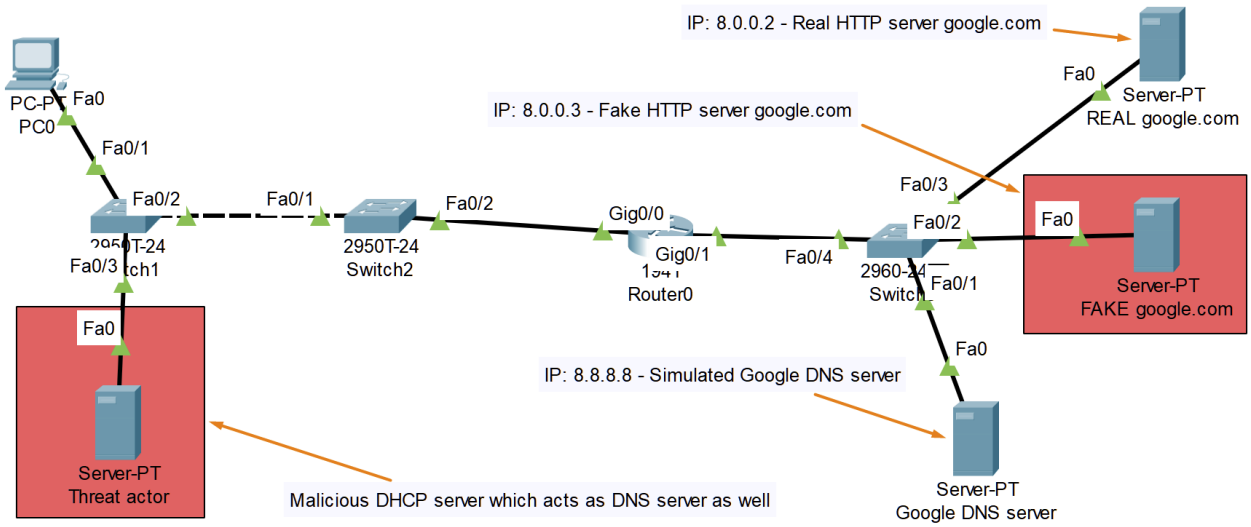
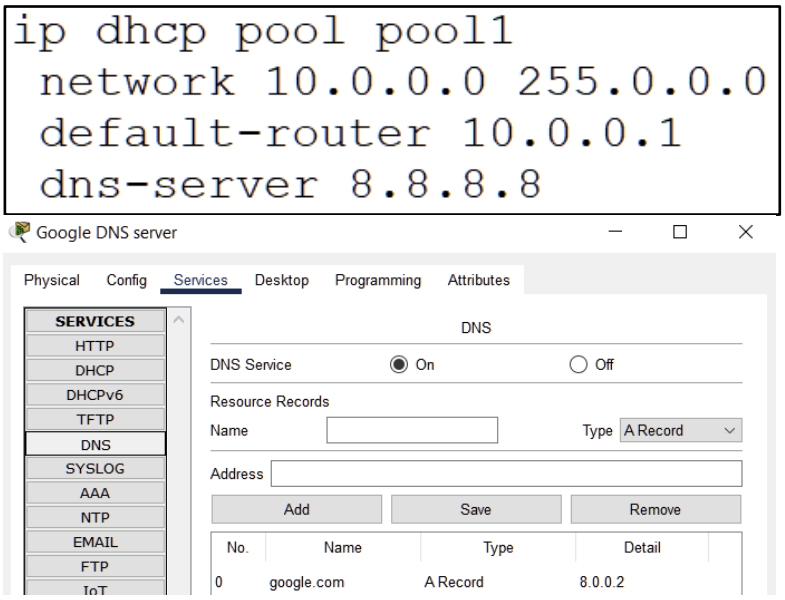
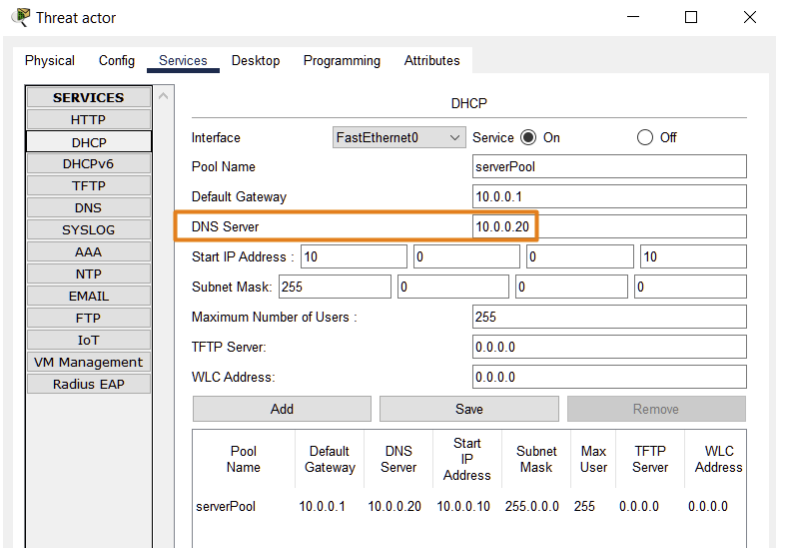


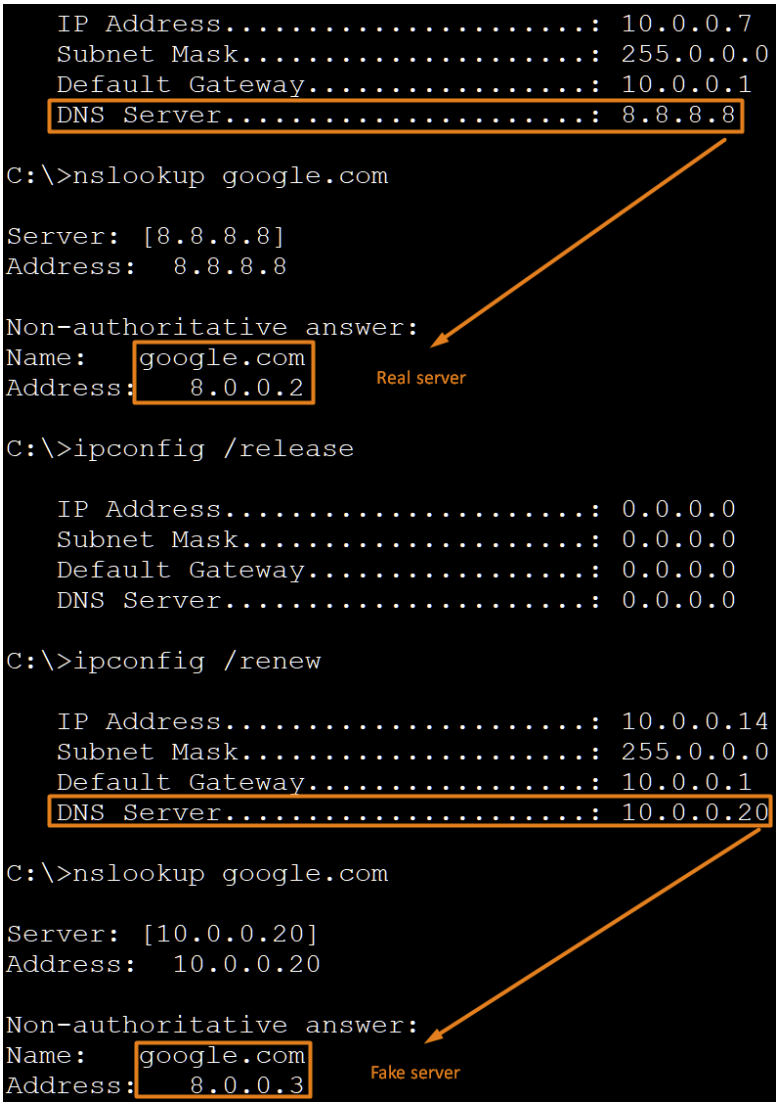
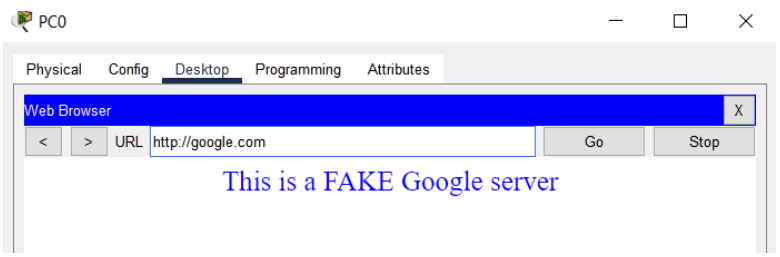
Figura 12.4 Topologia atacurilor de rețea: *servere DHCP și DNS necinstite pentru phishing*

Actorul rău intenționat se conectează la rețea cu un server care furnizează informații de adresare DHCP false (configurația serverului DNS fiind cea mai importantă informație de adresare din acest exemplu). Atunci când computerele din interiorul rețelei folosesc serverul DNS fals pentru a accesa adresa IP a unui server web, acestea vor fi redirecționate către serverul de phishing în loc de cel real.

Configurați topologia în Packet Tracer, apoi urmați pașii descriși mai jos (Tabel 12.3).

Tabelul 12.3 *Servere DHCP și DNS necinstite pentru pașii atacului de phishing*

1.	Etapele inițiale de configurare: - Lăsați actorul rău intenționat neconfigurat (sau eliminați legătura acestuia la switch) - Configurați DHCP pe Router0 și asigurați-vă că furnizează un server DNS valid în informațiile de adresare (așa cum se vede în dreapta) - Configurați serverul DNS Google simulat așa cum se vede în partea dreaptă	
2.	Un server Google simulat se află la serverul care are adresa IP 8.0.0.2. Accesând acest server de pe PC0, imaginea Cisco Packet Tracer va arăta ca figura din dreapta.	
3.	Conectați actorul rău intenționat la rețea și configurați-i serviciul DHCP așa cum se vede în imaginea din partea dreapta. Observați serverul DNS diferit care de fapt corespunde adresei IP statice a actorului rău intenționat.	

4.	La un moment dat, PC0 va trebui să-și actualizeze informațiile de adresare solicitând o nouă rezervare de la serverul DHCP. Acest pas poate fi simulat manual, așa cum se vede în partea dreaptă. Observați cum s-a schimbat serverul DNS, ceea ce înseamnă că PC0 primește rezervarea de la actorul rău intenționat și nu de la Router0. Investigați cum se întâmplă acest lucru utilizând instrumentul de simulare oferit de Cisco Packet Tracer. Este evident că serverul DNS configurat pe serverul actorului rău intenționat nu va lega URL-ul „google.com” la adresa IP corectă, ci va lega URL-ul la adresa IP a serverului fals, așa cum se vede în topologie. Rularea unei comenzi nslookup pe PC0 va dovedi acest lucru.	
5.	După ce PC0 a fost compromis, accesarea paginii web google.com va redirecționa către serverul fals care afișează o altă pagină.	

După analizarea întregii secvențe de pași, acest atac de phishing a avut succes și poate păcăli utilizatorul să-și introducă credențialele pe o pagină web falsă având un URL aparent valid.

Cercetați mecanisme pentru a preveni serverele rogue să ofere servicii de rețea false și mecanisme de prevenire a atacurilor de tip phishing.