LABORATOR 1.

TASK 1.

Obiective

Modelul de rețea din această activitate încorporează multe dintre tehnologiile care vor fi înțelese prin participarea la cursuri.

Rețeaua prezentată în Exemplul 1 din PacketTracer este o versiune simplificată a modului în care ar putea arăta o rețea de afaceri mici și mijlocii. În această etapă de lucru este important să fie explorată rețeaua pe cont propriu. După observarea cu atenție a tuturor elementelor prezentate, se solicit parcurgerea următorilor pași pentru a găsi răspunsuri la întrebări.

Notă: Este important să fie înțeles cât de mult posibil din acest exemplu. Dacă se dorește o procedură mai sistematică, este de preferat să fie urmați pașii de mai jos, după care se poate răspunde la întrebări cât mai bine.

Instrucțiuni

Pasul 1: Identificarea componentelor comune ale unei rețele așa cum sunt reprezentate în Packet Tracer.

Bara de instrumente cu pictograme din colțul din stânga jos are diferite categorii de componente de rețea. Ar trebui să fie observate categoriile care corespund dispozitivelor intermediare, dispozitivelor finale și media. Categoria ***Conexiuni*** (cu pictograma fulger) reprezintă mediul de rețea acceptat de Packet Tracer. Există, de asemenea, o categorie ***End Devices*** și două categorii specifice Packet Tracer: ***Custom Made Devices*** și ***Multiuser Connection.***

Întrebări:

1. Listarea categoriilor de dispozitive intermediare.

Răspunsuri aici.

2. Fără a intra în cloud-ul de internet sau cloud-ul intranet, câte pictograme din topologie reprezintă dispozitive terminale (o singură conexiune care duce la acestea)?

Răspunsuri aici.

3. Fără a număra cei doi nori, câte pictograme din topologie reprezintă dispozitive intermediare (conexiuni multiple care duc la acestea)?

Răspunsuri aici.

4. Câte dispozitive finale nu sunt computere desktop ?

Răspunsuri aici.

5. Câte tipuri diferite de conexiuni media sunt utilizate în această topologie de rețea?

Răspunsuri aici.

Pasul 2: Explicarea scopului dispozitivelor.

Întrebări:

a. În Packet Tracer, numai dispozitivul Server-PT poate acționa ca server. PC-urile desktop sau laptop-urile nu pot acționa ca server. Pe baza studiilor de până acum,să se explice modelul client-server.

Răspunsuri aici.

b. Să se enumere cel puțin două funcții ale dispozitivelor intermediare.

c. Să se enumere cel puțin două criterii pentru alegerea unui tip de medii de comunicații de rețea.

Răspunsuri aici.

Pasul 3: Compararea și verificarea contrastelor dintre rețelele LAN și WAN-urile.

Întrebări:

A. Care este diferența dintre un LAN și un WAN. Exemple pentru fiecare.

Răspunsuri aici.

b. În rețeaua Packet Tracer, câte rețele WAN sunt ?

Răspunsuri aici.

c. Câte rețele LAN ?

Răspunsuri aici.

d. Internetul din această rețea Packet Tracer este excesiv de simplificat și nu reprezintă structura și forma internetului real. Să se descrie pe scurt internetul.

Răspunsuri aici.

e. Care sunt câteva dintre modurile comune în care un utilizator casnic se conectează la internet ?

Răspunsuri aici.

f. Care sunt metodele comune pe care companiile le folosesc pentru a se conecta la internet în zona noastră de interes ?

Răspunsuri aici.

PROVOCARE

Acum că am avut ocazia de a explora rețeaua reprezentată în această activitate cu Packet Tracer, este posibil să fi acumulat câteva abilități pe care am dori să le încercăm. Sau poate ne-am dori oportunitatea de a explora această rețea mai detaliat. Dându-ne seama că cea mai mare parte a ceea ce vedem și experimentăm în Packet Tracer depășește în prezent nivelul nostru de calificare, iată câteva provocări pe care am dori să le încercăm. Nu ne facem griji dacă nu le putem face pe toate. În timp devenim utilizatori principali și designeri de rețea prin utilizarea Packet Tracer.

• Mai întâi adăugăm un dispozitiv final la topologie și îl conectăm la una dintre rețelele LAN cu o conexiune media. De ce altceva are nevoie acest dispozitiv pentru a trimite date altor utilizatori finali? Putem furniza informațiile? Există vreo modalitate de a verifica dacă am conectat corect dispozitivul?

• În al doilea rând, adăugăm un nou dispozitiv intermediar la una dintre rețele și îl conectăm la una dintre rețele LAN sau WAN cu o conexiune media. De ce altceva are nevoie acest dispozitiv pentru a servi ca dispozitiv intermediar pentru alte dispozitive din rețea?

• În a treia etapă deschidem o nouă instanță de Packet Tracer. Creăm o nouă rețea cu cel puțin două rețele LAN conectate printr-un WAN. Conectăm toate dispozitivele. Investigam activitatea originală Packet Tracer pentru a vedea ce altceva ar putea fi nevoie să facem pentru ca noua noastră rețea să funcționeze.

TASK 2.

Locurile de muncă în tehnologia informației (IT) și rețelele de calculatoare continuă să crească. Majoritatea angajatorilor solicită o anumită formă de certificare standard, diplomă sau alte calificări de la potențialii lor angajați, în special de la cei cu experiență limitată. Certificarea Cisco CCNA este o certificare de rețea entry-level cunoscută și consacrată, care este respectată în industrie. Există niveluri și tipuri suplimentare de certificări Cisco pe care le putem atinge și fiecare certificare poate îmbunătăți oportunitățile de angajare, precum și intervalul de salariu.

În aceste condiții, putem finaliza căutarea de locuri de muncă vizate pe web pentru a găsi ce tipuri de locuri de muncă IT și rețele de computere sunt disponibile; de ce fel de aptitudini și certificări vom avea nevoie; și intervalele de salariu asociate diferitelor titluri de post.

Pasul 1: Căutăm joburi legate de rețea.

A. La acest pas introducem cuvântul Network Administrator în caseta Cuvânt cheie sau Titlu. Facem clic pe „Găsiți locuri de muncă” pentru a continua.

B. Putem observa rezultatele căutării. Acum, ne concentrăm căutarea adăugând termeni la căutarea pentru Administrator de rețea. Încercăm termeni precum Cisco CCNA, CCNP, CCNA Security, CCNA Voice etc.

C. Acum încercăm să ne rafinam căutarea adăugând diferite locații geografice. Găsim locuri de muncă în locațiile în care am intrat?

Răspunsuri aici.

D. Încercăm să căutăm un alt site web. Accesați http://www.salary.com și facem clic pe butonul din bara de meniu Căutare locuri de muncă.

Notă: pentru listele de salarii din afara S.U.A., folosim următorul link pentru a căuta țara noastră:

http://www.payscale.com/rccountries.aspx

E. Adăugăm un termen de căutare, cum ar fi Tehnologia informației, în caseta de câmp Titlul postului sau Cuvânt cheie și facem clic pe Obține estimarea salariului meu.

ÎNTREBĂRI DE REFLECȚIE

Putem răspunde la următoarele întrebări pe baza rezultatelor cercetării noastre.

1. Ce titluri de post am căutat?

Răspunsuri aici.

2. Ce aptitudini sau certificări au fost necesare?

Răspunsuri aici.

3. Am găsit locuri de muncă despre care nu știam că există? Dacă da, care au fost?

Răspunsuri aici.

4. Am găsit locuri de muncă care ne interesează? Dacă da, care dintre ele și ce aptitudini sau certificări necesită?

Răspunsuri aici.

1. Navigarea prin IOS - Obiective

În această activitate, vor fi exersate abilitățile necesare pentru a naviga prin IOS, cum ar fi diferite moduri de acces utilizator, diferite moduri de configurare și comenzi comune utilizate în mod regulat. De asemenea, se va exersa accesarea ajutorului sensibil la context prin configurarea comenzii ***clock***.

Partea 1: Stabilirea conexiunilor de bază.

Pasul 1: Conectăm PC1 la Sw1 folosind un cablu de consolă.

A. Facem clic pe pictograma Conexiuni (cea care arată ca un fulger) din colțul din stânga jos al ferestrei Packet Tracer.

b. Selectăm cablul de consolă albastru deschis făcând clic pe el. Indicatorul mouse-ului se va schimba în ceea ce pare a fi un conector cu un cablu atârnând de el.

c. Facem clic pe PC1. O fereastră afișează o opțiune pentru o conexiune RS-232. Conectam cablul la portul RS-232.

d. Tragem celălalt capăt al conexiunii consolei la comutatorul Sw1 și facem clic pe comutator pentru a accesa lista de conexiuni.

e. Selectăm portul Consolă pentru a finaliza conexiunea.

Pasul 2: Stabilim o sesiune terminală cu Sw1.

A. Facem clic pe PC1 și apoi selectăm fila Desktop.

b. Facem clic pe pictograma aplicației Terminal. Verificăm că setările implicite de configurare a portului sunt corecte.

Întrebare:Care este setarea pentru biți pe secundă?

Introducem răspunsurile aici.

c. Facem clic pe OK.

d. Ecranul care apare poate avea mai multe mesaje afișate. Undeva pe ecran ar trebui să fie un mesaj să se apese RETURN pentru a începe. Apăsăm ENTER.

Întrebare: - Care este promptul afișat pe ecran ?

Explorarea modurilor EXEC

În partea 2 a acestei activităţi, vom trece la modul EXEC privilegiat și vom lansa comenzi suplimentare

Pasul 1: Intrăm în modul EXEC privilegiat.

A. La prompt, introducem semnul de întrebare (?).

Sw1> ?

Întrebare: -Ce informaţii sunt afișate pentru comanda de activare?

b. Tastam ro și apăsăm tasta Tab.

Sw1> en<Tab>

Întrebare: - Ce se afișează după apăsarea tastei Tab?

Introducem răspunsurile aici.

Aclockta se numește finalizarea comenzii (sau completarea filei). Când se introduce o parte a unei comenzi, tasta Tab poate fi folosită pentru a finaliza comanda parţială. Dacă caracterele tastate sunt suficiente pentru a face comanda unică, ca în cazul comenzii de activare, este afișată partea rămasă a comenzii.

Întrebare: - Ce s-ar întâmpla dacă am tasta te<Tab> la prompt?

Introducem răspunsurile aici.

c. Introducem comanda de activare și apăsăm ENTER.

Întrebare: - Cum se schimbă promptul?

Introducem răspunsurile aici.

d. Când ni se solicită, introducem semnul întrebării (?).

Sw1# ?

O comandă începe cu litera „C” în modul EXEC utilizator.

Întrebare: - Câte comenzi sunt afișate acum când modul EXEC privilegiat este activ? (Sugestie: am putea tasta c? pentru a enumera doar comenzile care încep cu „C”.)

Introducem răspunsurile aici.

Pasul 2: Intrăm în modul Configurare globală

A. Când suntem în modul EXEC privilegiat, una dintre comenzile care încep cu litera „C” este configurată. Introducem fie comanda

completă, fie suficientă comandă pentru a o face unică. Apăsăm tasta <Tab> pentru a lansa comanda și apăsăm ENTER.

Sw1# configure

Întrebare: - Care este mesajul care este afișat?

Introducem răspunsurile aici.

b. Apăsăm Enter pentru a accepta parametrul implicit care este inclus între paranteze [terminal].

Întrebare: - Cum se schimbă promptul?

Introducem răspunsurile aici.

c. Acesta se numește modul de configurare globală. Acest mod va fi explorat în continuare în activitățile și laboratoarele viitoare. Pentru moment, revenim la modul EXEC privilegiat tastând ***end, exit*** sau combinația de taste ***Ctrl-Z***.

Sw1(config)# exit

Sw1#

Setarea timpului

Pasul 1: Folosim comanda clock.

A. Folosim comanda ***clock*** pentru a explora în continuare Ajutor și sintaxa comenzilor. Tastăm ***show clock*** la promptul EXEC privilegiat.

Sw1# ***show clock***

Întrebare: - Ce informații sunt afișate?

- Care este anul care este afișat?

Introducem răspunsurile aici.

b. Folosim ajutorul sensibil la context și comanda clockului pentru a seta ora de pe comutator la ora curentă. Intrăm în comanda clocku și apăsăm ENTER.

Sw1# clock <ENTER>

Întrebare: - Ce informații sunt afișate?

Introducem răspunsurile aici.

c. Mesajul „% comandă incompletă” este returnat de IOS. Acest lucru indică faptul că comanda clock are nevoie de mai mulți parametri.

d. Setăm clockul folosind comanda ***clock set***. Procedăm prin comanda pas câte unul.

Sw1# clock set ?

Întrebări: - Ce informații sunt solicitate?

Ce s-ar fi afișat dacă ar fi fost introdusă doar comanda de setare a clockului și nu s-ar fi făcut nicio cerere de ajutor folosind semnul întrebării?

Introducem răspunsurile aici.

e. Pe baza informațiilor solicitate prin emiterea comenzii set clock ?, introducem ora 3:00 p.m. prin utilizarea formatului de 24 de ore ex: 15:00:00. Verificăm pentru a vedea dacă sunt necesari mai mulți parametri.

Sw1# clock set 15:00:00 ?

Ieșirea returnează o solicitare pentru mai multe informații:

<1-31> Ziua lunii LUNA Luna anului

f. Încercăm să setăm data la 25.03.2024 folosind formatul solicitat. Lansîm comanda ***show clock*** pentru a afișa setarea ceasului. Ieșirea de comandă rezultată ar trebui să se afișeze ca cea de mai jos:

Sw1# ***show clock***

*15:0:4.869 UTC Monday, 25 Monday 2024

g. Comanda corectă este :

Sw1# clock set 15:00:00 25 March 2024

2. Navigarea în IOS prin Uutilizarea unui Client Terminal prin conectivitate Consolă/RS 232 - modul fizic

Partea 1: Accesarea unui switch Cisco prin conexiunea la portul serial/portul consolă.

În această parte, va fi conectat un PC la un comutator Cisco folosind un cablu de consolă rollover. Această conexiune va permite accesarea CLI și setările de afișare și configurarea comutatorului.

Pasul 1: Instalarea și investigarea unui comutator 2960.

a. Există mai multe comutatoare, routere și alte dispozitive pe raft. Se va face clic și trage Switch 2960 în Rack.

În Packet Tracer, majoritatea dispozitivelor care vor fi trase în Rack sau pe masă sunt conectate automat la alimentare. Unele dispozitive necesită această pornire. Cu toate acestea, un Switch 2960 pornește imediat ce va fi mutat în Rack.

b. Se va face clic dreapta pe comutatorul 2960 și se selectează Inspect Front. Se va face clic pe instrumentul de zoom pentru a obține o vizualizare mai bună. Se va observa că există 24 de porturi pentru conectarea utilizatorilor și două porturi suplimentare pentru a conecta comutatorul la alte switch-uri sau routere.

c. Se va face clic pe X pentru a închide vizualizarea Inspect Front.

d. Se va face clic dreapta pe Switch 2960 și se va selecta Inspect Rear. Se va folosi instrumentul de zoom pentru a obține o vizualizare mai bună. Se va observa că există un port CONSOLE pentru conectarea unui cablu „rollover” la un PC.

e. Se va face clic pe X pentru a închide Inspect Rear View.

Pasul 2: Instalarea și investigarea PC-ului.

a. Se va face clic și trage computerul pe masă.

b. Se va face clic dreapta pe computer și se selectează „Inspect Front”. Se va face clic pe butonul roșu de pornire pentru a porni computerul. Acum ar trebui să se vadă o lumină verde pe partea din față a computerului. În partea de jos a computerului, se va observa că există o interfață Fast Ethernet. Alături de acesta se află un port RS 232 pentru conectarea unui cablu „rollover”. Mai jos sunt două porturi USB care pot fi folosite și pentru acces la consolă.

Pasul 3: Se va conecta comutatorul și PC-ul utilizând un cablu de consolă rollover.

a. Pe panoul pentru cabluri, se va face clic pe cablul albastru al consolei.

b. Pe computer, se va face clic pe portul RS 232.

c. Se va face clic dreapta pe Switch 2960 și alege Inspect Rear.

d. Se va face clic pe portul CONSOLE pentru a conecta cablul consolei rollover.

Pasul 4: Configurarea programului Terminal pentru a stabili o sesiune de consolă cu comutatorul.

Terminal este un program de emulare a terminalului care a fost creat special pentru Packet Tracer. Acest program va permite accesul la ieșirea terminalului comutatorului. De asemenea, va permite configurarea comutatorului.

a. Se va face clic pe ***PC > fila Desktop > Terminal***. Parametrii impliciti pentru portul de consolă sunt 9600 baud, 8 biți de date, fără paritate, 1 bit de oprire și fără control al fluxului. Setările implicite ale terminalului se potrivesc cu setările portului consolei pentru comunicațiile cu IOS pe comutator.

b. Se va face clic pe OK. Ultima linie din ieșirea terminalului ar trebui să fie ***Press RETURN*** pentru a începe.

c. Se va apăsa tasta ***ENTER*** pentru a ajunge la promptul modului EXEC utilizator de pe Switch.

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2005 by Cisco Systems, Inc.

Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

<ENTER>

Switch>

Partea 2: În această etapă vor fi afișate și configurate setările de bază ale dispozitivului

În această parte, vor fi introduse modurile EXEC utilizator și privilegiate. Se va determina versiunea iOS, se va afișa setările de ceas și se va configura ceasul pe comutator.

Pasul 1: Se va afișa versiunea de imagine a comutatorului IOS.

În modul EXEC utilizator, va fi folosită comanda ***show version*** pentru a afișa versiunea IOS pentru Switch.

Switch> show version

Ce imagine și versiune iOS este utilizată în prezent de comutator?

Răspunsurile aici.

Pasul 2: Se va configura ceasul.

După ce vom afla mai multe despre rețea, vom vedea că prin configurarea orei corecte pe un Switch, aceasta va fi utilă atunci când vor fi depanate problemele ce pot apărea. Următorii pași permit configurarea manuală a ceasului intern al comutatorului.

a. Afișarea setărilor curente ale ceasului.

Switch> show clock

*00:30:05.261 UTC Mon Mar 1 1993

b. Va trebui să fie accesat modul EXEC privilegiat pentru a schimba setările ceasului. Pentru a intra în modul EXEC privilegiat, va trebui să se tasteze comanda ***enable*** la promptul utilizatorului pentru modul EXEC.

Switch> enable

3 Configurarea setărilor inițiale ale comutatorului-Obiective

Pasul 1: Se va intra în modul EXEC privilegiat.

Din acest mod se vor putea accesa toate comenzile pe Switch din modul EXEC privilegiat. Cu toate acestea, deoarece multe dintre comenzile privilegiate configurează parametrii de funcționare, accesul privilegiat ar trebui protejat prin parolă pentru a preveni utilizarea neautorizată.

Setul de comenzi EXEC privilegiat include comenzile disponibile în modul EXEC utilizator, multe comenzi suplimentare și comanda configure prin care se obține accesul la modurile de configurare.

a. Se face clic pe S1 și apoi pe fila CLI, apoi se apasă Enter.

b. Se va intra în modul EXEC privilegiat introducând comanda de activare:

Switch> enable

Switch#

Se va observa că promptul s-a schimbat pentru a reflecta modul EXEC privilegiat.

Pasul 2: Se va examina configurația curentă a comutatorului.

Va fi introdusă comanda ***show running-config***.

Switch# show running-config

Este necesar să se răspundă la următoarele întrebări:

- Câte interfețe Fast Ethernet are comutatorul?

Răspunsurile aici.

- Câte interfețe Gigabit Ethernet are comutatorul?

Răspunsurile aici.

- Care este intervalul de valori afișat pentru liniile vty ?

Răspunsurile aici.

- Ce comandă va afișa conținutul curent al memoriei nevolatile cu acces aleatoriu (NVRAM)?

Răspunsurile aici.

- De ce Switch-ul răspunde cu „startup-config is not present?”

Răspunsurile aici.

Partea 2: Se va crea o configurație de bază a comutatorului

Pasul 1: Va fi atribuit un nume unui comutator.

Pentru a configura parametrii pe un comutator, este necesar să se facă deplasarea între diferite moduri de configurare.

Se va observa cum se schimbă promptul pe măsură ce se navighează prin IOSul Switchului.

Switch# configure terminal

S1(config)#no ip domain-lookup

Switch(config)# hostname S1

S1(config)# exit

S1#

Pasul 2: Se va face acces securizat la IOS-ul dispozitivului.

Pentru a securiza accesul la IOS prin linia consolei sau liniile vty se va accesa în modul linie de configurare și se vor seta parolele:

S1(config)# no cdp run

S1(config)# service password-encryption

S1(config)# enable secret ciscosecpa55

S1(config)# enable password ciscoenapa55

Pe linia de console:

S1(config)# line console 0

S1(config)# password ciscoconpa55

S1(config)# login

S1(config)# logging synchronous

S1(config)# exec-timeout 30 30

Pe liniile vty:

S1(config)# line vty 0 15

S1(config)# password ciscovtypa55

S1(config)# login

S1(config)# logging synchronous

S1(config)# exec-timeout 25 25

De ce este necesară comanda de autentificare?

Pasul 3: Se va verifica dacă accesul la consolă este securizat.

Se va ieși din modul privilegiat pentru a verifica dacă parola portului consolei este în vigoare.

S1# exit

Switch con0 is now available

Press RETURN to get started.

User Access Verification

Password:

S1>

Pasul 4: Se va verifica dacă accesul în modul privilegiat este securizat.

a. Va fi introdusă din nou comanda de ieșire pentru a deconecta din Switch.

b. Se va apăsa <Enter> și acum se va cere o parolă:

User Access Verification

Password:

c. Prima parolă este parola consolei care a fost configurată pentru linia ***con 0***. Va fi introdusă această parolă pentru a reveni la modul EXEC utilizator.

d. Se va introduce comanda pentru a accesa modul privilegiat.

e. Va fi introdusă a doua parolă care a fost configurată pentru a proteja modul EXEC privilegiat.

f. Se va verifica configurația prin examinarea conținutului fișierului de configurare în curs de funcționare:

S1# show running-config

Se va observa că parolele de consolă și de activare sunt ambele în text simplu. Acest lucru ar putea reprezenta un risc de securitate dacă cineva se uită peste umăr sau obține acces la fișierele de configurare stocate într-o locație de rezervă.

Din acest motiv, parola de activare a fost înlocuită cu parola secretă criptată mai nouă folosind comanda ***enable secret***.

Partea 5: Provocarea de a configura S2.

Când se va finaliza configurarea pe S1, este important să se configureze S2. Dacă nu se pot aminti comenzile, se vor consulta Părțile 1 până la 4 pentru asistență.

Se va configura S2 cu următorii parametri:

Va fi deschisă fereastra de configurare pentru S2

A. Nume dispozitiv: S2

b. Acces protejat la consolă folosind parola.

c. Se va configura o parolă de activare și o parolă secretă de activare.

d. Se va configura un mesaj adecvat pentru cei care se conectează la Switch.

e. Vor fi criptate toate parolele text simplu.

f. Se va asigura faptul că toată configurația este corectă.

g. Se va salva fișierul de configurare pentru a evita pierderea în cazul în care Switch-ul este oprit.

4. Implementarea Conectivității de Bază

Tabel de Adresare

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

Partea 1: Se va efectua o configurare de bază pe S1 și S2

Se vor parcurge următorii pași pe S1 și S2.

Pasul 1: Se va configura S1 cu un nume de gazdă.

a. Se va face conectarea pe S1 prin consolă.

b. Se va introduce comanda corectă pentru a configura numele de gazdă ca S1.

Pasul 2: Se vor configura consola și parolele privilegiate criptate ale modului EXEC.

A. Se va folosi ciscoconpa55 pentru parola consolei.

b. Se va folosi ciscosecpa55 pentru parola privilegiată a modului EXEC.

Pasul 3: Se vor verifica configurațiile parolei pentru S1.

Întrebare:

Cum se poate verifica dacă ambele parole au fost configurate corect?

Pasul 4: Se va configura un banner MOTD.

Se va folosi un text banner adecvat pentru a avertiza accesul neautorizat. Următorul text este un exemplu: ***Authorized access only. Violators will be prosecuted to the full extent of the law.***

Pasul 5: Se va salva fișierul de configurare pe NVRAM.

Întrebare:

Ce comandă se va lansa pentru a realiza acest pas?

Pasul 6: Se vor repeta pașii de la 1 la 5 pentru S2.

Partea 2: Vor fi configurate PC-urile

Vor fi configurate PC1 și PC2 cu adrese IP.

Pasul 1: Vor fi configurate ambele PC-uri cu adrese IP.

a. Se va face clic pe PC1 și apoi pe fila Desktop.

b. Se va face clic pe Configurare IP. În tabelul de adrese de mai sus, se poate vedea că adresa IP pentru PC1 este 192.168.1.1 și masca de subrețea este 255.255.255.0. Aceste informații vor fi introduse pentru PC1 în fereastra Configurare IP.

c. Se vor repeta pașii 1a și 1b pentru PC2.

Pasul 2: Se va testa conexiunea la Switches.

a. Se va face clic pe PC1. Se va închide fereastra Configurare IP dacă este încă deschisă. În fila Desktop, se va face clic pe Command Prompt.

b. Se va tasta comanda ***ping*** și adresa ***IP*** pentru ***S1*** și se va apăsa ***Enter.***

PC> ping 192.168.1.253

A avut succes? Explicație.

Partea 3: Se va configura interfața de management pe Switch.

Se vor configura S1 și S2 cu o adresă IP.

Pasul 1: Se va configura S1 cu o adresă IP.

Switch-urile pot fi folosite ca dispozitive plug-and-play. Aceasta înseamnă că nu trebuie să fie configurate pentru ca acestea să funcționeze. Comută transmiterea informațiilor de la un port la altul pe baza adreselor MAC.

Întrebare:

Dacă acesta este cazul, de ce l-am configura cu o adresă IP ?

Se vor folosi următoarele comenzi pentru a configura S1 cu o adresă IP.

S1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# interface vlan 1

S1(config-if)#description Legatura cu ramura 192.168.1.0/24

S1(config-if)# ip address 192.168.1.253 255.255.255.0

S1(config-if)# no shutdown

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#

S1(config-if)# exit

S1#

De ce este introdusă comanda ***no shutdown***?

Pasul 2: Se va configura S2 cu o adresă IP.

Se vor folosi informațiile din tabelul de adrese pentru a configura S2 cu o adresă IP.

Pasul 3: Se va verifica configurația adresei IP pe S1 și S2.

Se va utiliza comanda ***show ip interface brief*** pentru a afișa adresa IP și starea tuturor porturilor și interfețelor Switch-ului. Se poate folosi și comanda ***show running-config***.

Pasul 4: Se vor salva configurațiile pentru S1 și S2 pe NVRAM.

Întrebare:

Ce comandă este folosită pentru a salva fișierul de configurare din RAM în NVRAM?

Pasul 5: Se va verifica conectivitatea la rețea.

Conectivitatea la rețea poate fi verificată folosind comanda ***ping***. Este foarte important ca această conectivitate să existe în întreaga rețea. Trebuie luate măsuri corective dacă există o defecțiune. Ping la S1 și S2 de la PC1 și PC2.

a. Se va face clic pe PC1 și apoi pe fila Desktop.

b. Se va face clic pe Command Prompt.

c. Ping adresa IP pentru PC2.

d. Ping adresa IP pentru S1.

e. Ping adresa IP pentru S2.

Notă: Se poate folosi și comanda ***ping*** pe CLI-ul comutatorului și pe PC2.

Toate ping-urile ar trebui să aibă succes. Dacă rezultatul primului ping este de 80%, va fi încercat din nou. Acum ar trebui să fie

100%. În viitor, se va afla de ce un ping poate eșua uneori când este lansat prima dată. Dacă nu se va putea da ping la niciunul dintre dispozitive, va trebui să se verifice din nou configurația pentru erori.

5. Configurarea de Bază a Dispozitivului Final și a Switchului

Device	Interface	IP Address	Subnet Mask
	VLAN 1		255.255.255.0
	VLAN 1		255.255.255.0
	NIC		255.255.255.0
	NIC		255.255.255.0

Obiective

• Se vor configura numele de gazdă și adresele IP pe două Switch-uri ale sistemului de operare Internetwork (IOS) folosind interfața de linie de comandă (CLI) prin consolă.

• Se vor folosi comenzi IOS pentru a specifica sau limita accesul la configurațiile dispozitivului.

• Se va folosi comenzile IOS pentru a salva configurația care rulează.

• Vor fi configurate două dispozitive gazdă cu adrese IP.

• Se va verifica conectivitatea între cele două dispozitive finale PC.

Instrucțiuni

Dispozitivele vor fi configurate pentru a îndeplini cerințele de mai jos.

Cerințe

• Se va folosi o conexiune la consolă pentru a accesa fiecare comutator.

• Nume și comutatoare.

• Se va folosi parola pentru toate liniile.

• Se va folosi parola secretă.

• Vor fi criptate toate parolele text clar.

• Se va configura un banner adecvat pentru mesajul zilei (MOTD).

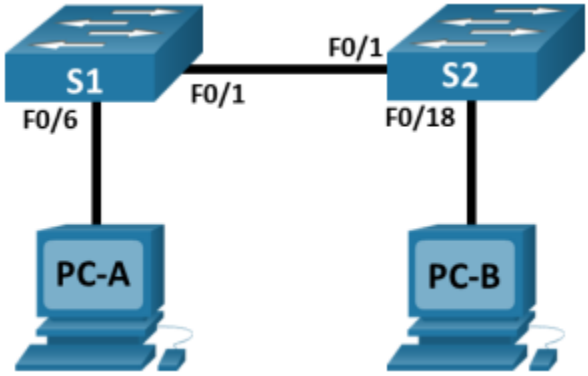
• Se va configura adresarea pentru toate dispozitivele conform Tabelului de Adresări.

• Se vor salva configurațiile.

• Se va verifica conectivitatea între toate dispozitivele

6. A doua configurare de bază, pentru End Device și Switch

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0



Obiective

• Se va configura topologia rețelei

• Vor fi configurate PC-uri

• Se va configura și se va verifica setările de bază pe Switch.

Instrucțiuni

Pasul 1: Se va configura topologia rețelei

În acest pas, vor fi conectate dispozitivele în funcție de topologia rețelei.

a. Dispozitivele vor fi alimentare.

b. Se vor conecta cele două comutatoare.

c. Vor fi conectate PC-urile la comutatoarele respective.

d. Se va inspecta vizual conexiunile de rețea.

Pasul 2: Se va configura PC-urile Gazde

a. Se vor configura informațiile de adresă IP statică de pe computere conform Tabelului de adrese.

b. Se vor verifica setările PC-ului și conectivitatea.

Pasul 3: Se va configura și se va verifica setările de bază ale comutatorului

a. Cu ajutorul consolei se va intra în comutator. Se va intra în modul de configurare globală.

Va fi deschisă fereastra de configurare

b. Se va da comutatorului un nume conform tabelului de adrese.

c. Se vor preveni căutările DNS nedorite.

d. Vor fi introduse parole locale.

e. Va fi configurat și activat SVI-ul conform Tabelului de Adresări.

f. Va fi introdus un banner MOTD de conectare pentru a avertiza despre accesul neautorizat.

g. Se va salva configurația.

h. Va fi afișată configurația curentă.

i. Se va afișa versiunea iOS și alte informații utile despre comutare.

j. Va fi afișată starea interfețelor conectate pe comutator.

k. Se va configura comutatorul S2.

l. Se va înregistra starea interfeței pentru următoarele interfețe.

m. De pe un PC, se va da ping S1 și S2. Ping-urile ar trebui să aibă succes.

n. De la un comutator, se va da ping PC-A și PC-B. Ping-urile ar trebui să aibă succes.

Interface	S1 Status	S1 Protocol	S2 Status	S2 Protocol
Fa 0/1				
Fa 0/6				
Fa 0/18				
VLAN 1				

7. Proiectarea unui sistem de comunicații în ritm propriu

Obiective

Se va explica rolul organizațiilor de protocoale și standarde în facilitarea interoperabilității în comunicațiile de rețea.

Scenariu

Tocmai a fost achiziționat un autoturism nou pentru uz personal. După ce se va conduce mașina timp de aproximativ o săptămână, se va constata că nu funcționează corect. Se va discuta problema cu mai mulți colegi și se va lua decizia să se ducă mașina la o unitate de reparații auto. Este singura unitate de reparații situată în imediata apropiere.

Când se va ajunge la unitatea de reparații, se va descoperi că toți mecanicii vorbesc o altă limbă. În acest mod sunt întâmpinate dificultăți în a explica problemele de performanță ale automobilului, dar reparațiile chiar trebuie făcute. Nu se poate reveni înapoi acasă pentru a căuta alte opțiuni.

Trebuie găsită o modalitate de a lucra cu unitatea de reparații pentru a se asigura faptul că automobilul este reparat corect.

Cum se comunica cu mecanicii ?

Se solicit proiectarea unui model de comunicații pentru a se asigura faptul că mașina este reparată corespunzător.

LABORATOR 3.Stivele de Protocoale

Partea 1: Cercetarea standardelor de rețea - Obiective

- Cercetarea organizațiilor de standarde de rețea
- Internet și rețele de calculatoare

Utilizarea motoarelor de căutare web precum Google, efectuarea cercetării organizațiilor non-profit care sunt responsabile pentru stabilirea standardelor internaționale pentru internet și dezvoltarea tehnologiilor internet.

Instrucțiuni

Pasul 1: Cercetarea organizațiilor de standarde de rețea

În acest pas, se vor identifica unele dintre organizațiile de standardizare majore și caracteristicile importante, cum ar fi numărul de ani de existență, dimensiunea membrilor lor, figurile istorice importante, unele dintre responsabilități și îndatoriri, rolul de supraveghere organizațională și locația. a sediului organizației.

Utilizarea unui browser web sau site-uri web pentru diverse organizații pentru a căuta informații despre următoarele organizații și despre persoanele care au jucat un rol esențial în menținerea acestora.

Se pot găsi răspunsuri la întrebările de mai jos căutând următoarele acronime și termeni organizaționali:

ISO, ITU, ICANN, IANA, IEEE, EIA, TIA, ISOC, IAB, IETF, W3C, RFC și Wi-Fi Alliance.

Întrebări:

1. Cine este Jonathan B. Postel și pentru ce este cunoscut ?

Răspunsurile aici.

2. Care două organizații conexe sunt responsabile pentru gestionarea spațiului de nume de domeniu de nivel superior și a rădăcinii Servere de nume DNS (Domain Name System) de pe internet ?

Răspunsurile aici.

3. Vinton Cerf a fost numit unul dintre principalii părinți ai internetului. Ce organizații de internet a prezidat el sau a ajutat la găsit? Ce tehnologii de internet a ajutat el să dezvolte?

Răspunsurile aici.

4. Ce organizație este responsabilă pentru publicarea cererii de comentarii (RFC)?

Răspunsurile aici.

5. Ce au în comun RFC 349 și RFC 1700?

Răspunsurile aici.

6. Ce număr RFC este ARPAWOCKY? Ce este?

Răspunsurile aici.

7. Cine a fondat Consorțiul World Wide Web (W3C)?

Răspunsurile aici.

8. Numirea a 10 standarde World Wide Web (WWW) pe care W3C le dezvoltă și le menține?

Răspunsurile aici.

9. Unde se află sediul Institutului de Ingineri Electrici și Electronici (IEEE) și care este semnificația logo-ului său?

Răspunsurile aici.

10. Care este standardul IEEE pentru protocolul de securitate Wi-Fi Protected Access 2 (WPA2)?

Răspunsurile aici.

11. Este Wi-Fi Alliance o organizație non-profit de standardizare? Care este scopul lor?

Răspunsurile aici.

12. Cine este Hamadoun Touré?

Răspunsurile aici.

13. Ce este Uniunea Internațională a Telecomunicațiilor (ITU) și unde are sediul ?

Răspunsurile aici.

14. Numirea celor trei sectoare ITU.

Răspunsurile aici.

15. Ce înseamnă RS în RS-232 și ce organizație l-a introdus?

Răspunsurile aici.

16. Ce este SpaceWire ?

Răspunsurile aici.

17. Care este misiunea ISOC și unde se află sediul acestuia ?

Răspunsurile aici.

18. Ce organizații supraveghează IAB ?

Răspunsurile aici.

19. Ce organizație supraveghează IAB ?

Răspunsurile aici.

20. Când a fost fondat ISO și unde se află sediul său?

Răspunsurile aici.

EXERCIȚIUL 1.- Investigarea modelelor TCP/IP și OSI în acțiune.

Obiective

Partea 1: Examinarea traficului web HTTP.

Instrucțiuni

Partea 1: Examinarea traficului web HTTP

În partea 1 a acestei activități, se va folosi modul de simulare Packet Tracer (PT) pentru a genera trafic web și a examina HTTP.

Pasul 1: Trecerea de la modul în timp real la modul de simulare.

În colțul din dreapta jos al interfeței Packet Tracer sunt butoane care comută între modul în timp real și simulare. PT începe întotdeauna în modul în timp real, în care protocoalele de rețea funcționează în mod realist. Cu toate acestea, o caracteristică puternică a Packet Tracer permite utilizatorului să „oprească timpul” trecând la modul Simulare. În modul Simulare, pachetele sunt afișate ca plicuri animate, timpul este determinat de evenimente, iar utilizatorul poate parcurge evenimentele de rețea.

a. Pentru a face acest lucru, se face clic pe pictograma mod Simulare pentru a comuta de la modul în timp real la modul Simulare.

b. Selectarea HTTP din Filtrele listei de evenimente.

1) HTTP poate fi deja singurul eveniment vizibil. Dacă este necesar, se face clic pe butonul Editare filtre din partea de jos a panoului de simulare pentru a afișa evenimentele vizibile disponibile. Se comută la caseta de selectare Afișare tot/Niciuna și se poate observa cum casetele de selectare trec de la nebifat la bifat sau bifat la nebifat, în funcție de starea curentă.

2) Se face clic pe caseta de selectare Show All/None până când toate casetele sunt golite și apoi se selectează HTTP din fila Diverse a ferestrei Editare filtre. Se face clic pe X din colțul din dreapta sus al ferestrei pentru a închide fereastra Editare filtre. Evenimentele vizibile ar trebui să afișeze acum doar HTTP.

Pasul 2:Se generează trafic web (HTTP).

În prezent, panoul de simulare este gol. Există cinci coloane listate în partea de sus a Listei de evenimente din panoul de simulare. Pe măsură ce traficul este generat și parcurs, evenimentele apar în listă.

Partea 2: Afișarea elementelor TCP/IP Protocol Suite.

Notă: Serverul Web și Clientul Web sunt afișate în panoul din stânga. Panourile pot fi ajustate în dimensiune trecând cu mouse-ul peste bara de defilare și trăgând la stânga sau la dreapta când apare săgeata cu două capete.

a. Se face clic pe Web Client din panoul din stânga.

b. Se face clic pe fila Desktop și se face clic pe pictograma Browser Web pentru a o deschide.

c. În câmpul URL, se introduce www.osi.local și se face clic pe Go. Deoarece timpul în modul Simulare este determinat de evenimente, trebuie să folosească butonul Captură/Redirecționare pentru a afișa evenimentele de rețea. Butonul de captură înainte este situat în stânga barei albastre de sub fereastra topologiei. Dintre cele trei butoane de acolo, este cel din dreapta.

d. Se face clic pe Captură/Înainte de patru ori. Ar trebui să existe patru evenimente în Lista de evenimente.

Întrebare:

Privind pagina browser-ului Web Client. S-a schimbat ceva?

Răspunsurile aici.

Pasul 3: Explorarea conținutului pachetului HTTP.

a. Se face clic pe prima casetă pătrată colorată de sub coloana Lista de evenimente > Tip. Poate fi necesar să extindeți panoul de simulare sau să utilizați bara de defilare direct sub Lista de evenimente.

Este afișată fereastra PDU Information at Device: Web Client. În această fereastră, există doar două file (OSI Model și Outbound PDU Details), deoarece acesta este începutul transmisiei. Așa cum sunt revizuite mai multe evenimente, vor fi afișate trei file, adăugând o filă pentru Detalii PDU primite. Când un eveniment este ultimul eveniment din fluxul de trafic, sunt afișate numai filele Model OSI și Detalii PDU de intrare.

b. Este necesar să vă asigurați că fila Model OSI este selectată.

Sub coloana Straturi exterioare, se face clic pe Stratul 7.

Întrebări:

Pentru ce informații sunt listate în pașii numerotați direct sub casetele Straturi de intrare și Straturi de ieșire Layer 7?

Răspunsurile aici.

Care este valoarea Dst Port pentru Layer 4 sub coloana Out Layers?

Răspunsurile aici.

Ce este Dest. Valoarea IP pentru Layer 3 sub coloana Out Layers?

Răspunsurile aici.

Ce informații sunt afișate la Layer 2 sub coloana Out Layers?

Răspunsurile aici.

c. Faceți clic pe fila Outbound PDU Details.

Informațiile listate sub formatele PDU reflectă straturile din modelul TCP/IP.

Notă: Informațiile enumerate în secțiunea Ethernet II din fila Outbound PDU Details oferă informații și mai detaliate decât cele enumerate în Layer 2 din fila OSI Model. Detaliile PDU trimise oferă informații mai descriptive și detaliate. Valorile din DEST MAC și SRC MAC

în secțiunea Ethernet II a PDU Detaliile apar pe fila OSI Model sub Layer 2, dar nu sunt identificate ca atare.

Întrebări:

Care sunt informațiile comune enumerate în secțiunea IP din Detalii PDU în comparație cu informațiile enumerate în fila Model OSI ?

Cu ce strat este asociat?

Răspunsurile aici.

Care sunt informațiile comune enumerate în secțiunea TCP din Detalii PDU, în comparație cu informațiile listate în fila Model OSI și cu ce strat este asociat?

Răspunsurile aici.

Care este gazda listată în secțiunea HTTP din Detaliile PDU? Cu ce strat ar fi asociate aceste informații în fila Model OSI?

Răspunsurile aici.

d. Se face clic pe următoarea casetă pătrată colorată de sub coloana Lista de evenimente > Tip. Numai Stratul

1 este activ (nu este gri afară). Dispozitivul mută cadrul din buffer și îl plasează în rețea.

e. Se face avansarea la următoarea casetă de tip HTTP din Lista de evenimente și se face clic pe caseta pătrată colorată. Această fereastră conține atât InLayers, cât și OutLayers. Se poate observa direcția săgeții direct sub coloana InLayers; este îndreptată în sus, indicând direcția în care se deplasează datele. Se face derularea prin aceste straturi notând elementele vizualizate anterior. În partea de sus a coloanei, săgeata indică spre dreapta. Acest lucru indică faptul că serverul trimite acum informațiile înapoi către client.

Întrebare:

Comparând informațiile afișate în coloana InLayers cu cele din coloana OutLayers, care sunt diferențele majore?

Răspunsurile aici.

f. Se face clic pe fila Detalii PDU de intrare și de ieșire. Se face revizuirea detaliilor PDU.

g. Se face clic pe ultima casetă pătrată colorată de sub coloana Info.

Întrebare:

Câte file sunt afișate cu acest eveniment? Explicație.

Partea 2: Se face prin afișarea Elementelor TCP/IP Protocol Suite

În partea 2 a acestei activități, se va folosi modul Packet Tracer Simulation pentru a vizualiza și examina unele dintre celelalte protocoale care cuprind suita TCP/IP.

Pasul 1: Vizualizarea evenimentelor suplimentare

a. Se face prin închiderea oricăror ferestre deschise de informații PDU.

b. În secțiunea Filtre liste de evenimente > Evenimente vizibile, se face clic pe Afișare tot/Niciunul.

Întrebare:

Ce tipuri de evenimente suplimentare sunt afișate?

Răspunsurile aici.

Aceste intrări suplimentare joacă diverse roluri în suita TCP/IP. Address Resolution Protocol (ARP) solicită adrese MAC pentru gazdele destinație. DNS este responsabil pentru conversia unui nume (de exemplu, www.osi.local) într-o adresă IP. Evenimentele TCP suplimentare sunt responsabile pentru conectarea, acordul asupra parametrilor de comunicare și deconectarea sesiunilor de comunicații între dispozitive. Aceste protocoale au fost menționate anterior și vor fi discutate în continuare pe măsură ce cursul progresează.

În prezent, există peste 35 de protocoale posibile (tipuri de evenimente) disponibile pentru capturare în Packet Tracer.

c. Se face clic pe primul eveniment DNS din coloana Tip. Se realizează explorând filele Model OSI și Detaliu PDU și notează procesul de încapsulare. Privind fila Model OSI cu Stratul 7 evidențiat, o descriere a ceea ce se întâmplă este listată direct sub Straturile de intrare și Straturile de ieșire („1. Clientul DNS trimite o interogare DNS către serverul DNS.”). Acestea sunt informații foarte utile pentru a ajuta la înțelegerea a ceea ce se întâmplă în timpul procesului de comunicare.

d. Se face clic pe fila Outbound PDU Details.

Ce informații sunt listate în câmpul NAME: în secțiunea DNS QUERY?

Răspunsurile aici.

e. Se face clic pe ultima casetă pătrată colorată cu informații DNS din lista de evenimente.

Întrebări:

La ce dispozitiv a fost capturat PDU-ul?

Răspunsurile aici.

Care este valoarea listată lângă ADRESĂ: în secțiunea RĂSPUNS DNS din Detaliile PDU de intrare?

Răspunsurile aici.

f. Se găsește primul eveniment HTTP din listă și se face clic pe caseta pătrată colorată a evenimentului TCP imediat după acest eveniment. Se evidențiază Stratul 4 în fila Model OSI.

Întrebare:

În lista numerotată, direct sub Straturile de intrare și straturi de ieșire, care sunt informațiile afișate la articolele 4 și 5?

Răspunsurile aici.

TCP gestionează conectarea și deconectarea canalului de comunicații împreună cu alte responsabilități. Acest eveniment special arată faptul că canalul de comunicare a fost STABILIT.

g. Se face clic pe ultimul eveniment TCP. Se evidențiază Stratul 4 în fila Model OSI. Este făcut pentru a examina pașii enumerați direct sub InLayers și OutLayers.

Întrebare:

Care este scopul acestui eveniment, pe baza informațiilor furnizate la ultimul punct din listă (ar trebui să fie punctul 4)?

Răspunsurile aici.

EXERCIȚIUL 2. Utilizarea Wireshark pentru a vizualiza traficul de rețea.

Obiective

Partea 1: Se face captarea și analizarea datelor ICMP locale în Wireshark.

Partea 2: Se face captarea și analizarea datelor ICMP la distanță în Wireshark.

Instrucțiuni

Partea 1: Se realizează prin capturarea și analiza datelor ICMP locale în Wireshark.

În partea 1 a acestui laborator, se va face ping pe un alt PC pe LAN și va captura cererile ICMP și răspunsurile în Wireshark. Se va uita, de asemenea, în interiorul cadrelor capturate pentru informații specifice. Această analiză ar trebui să ajute la clarificarea modului în care anteturile pachetelor sunt utilizate pentru a transporta date la destinație.

Pasul 1: Este făcut pentru a prelua adresele interfeței PC-ului.

Pentru acest laborator, va trebui să se recupereze adresa IP a PC-ului și adresa fizică a plăcii de interfață de rețea (NIC), numită și adresa MAC.

Deschiderea unui prompt de comandă Windows.

a. Într-o fereastră de prompt de comandă, se introduce ipconfig /all, prin intermediul căreia se poate observa adresa IP a interfeței PC, descrierea acesteia și adresa MAC (fizică).

```
C:\Users\Student> ipconfig /all

Windows IP Configuration

 Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC

 Primary Dns Suffix . . . . . . . :
```

```
 Node Type . . . . . . . . . . . . . : Hybrid
 IP Routing Enabled. . . . . . . . . : No
 WINS Proxy Enabled. . . . . . . . . : No
Ethernet adapter Ethernet:
 Connection-specific DNS Suffix . :
 Description . . . . . . . . . . . . : Intel(R) 82577LM
Gigabit Network Connection
 Physical Address. . . . . . . . . . :00-26-B9-DD-00-91
 DHCP Enabled. . . . . . . . . . . . : No
 Autoconfiguration Enabled . . . . : Yes
 Link-local IPv6 Address . . . . . :
fe80::d809:d939:110f:1b7f%20(Preferred)
 IPv4 Address. . . . . . . . . . . . :
192.168.1.147(Preferred)
 Subnet Mask . . . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . . . : 192.168.1.1
<output omitted>
```

Pasul 2: Se face Pornirea Wireshark și începerea captării datelor.

a. Navigarea la Wireshark. Se face dublu clic pe interfața dorită pentru a porni captura de pachete. Se asigură că interfața dorită are trafic.

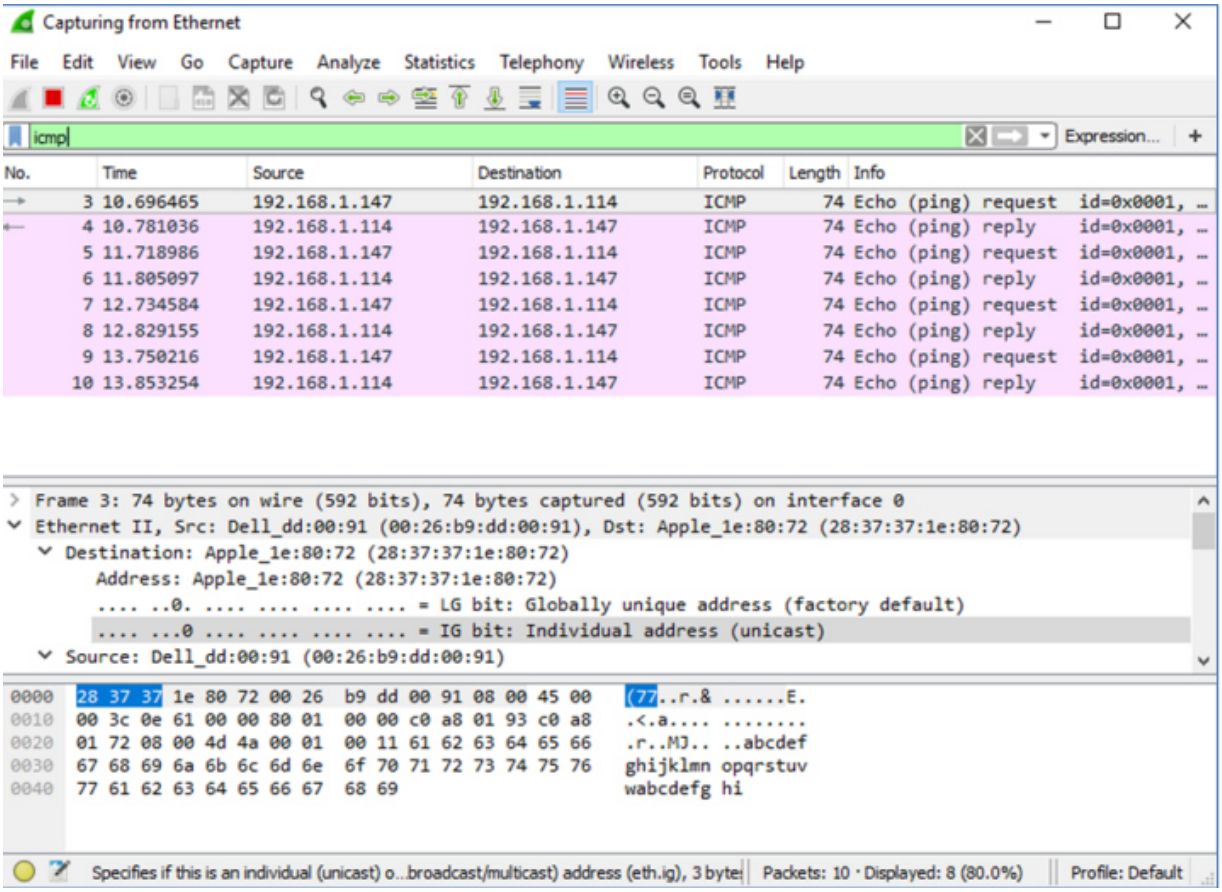
b. Informațiile vor începe să defileze în jos în secțiunea de sus în Wireshark. Liniile de date vor apărea în culori diferite în funcție de protocol.

Aceste informații se pot derula foarte repede, în funcție de ce comunicare are loc între computer și LAN. Putem aplica un filtru pentru a facilita vizualizarea și lucrul cu datele care sunt capturate de Wireshark.

Pentru această etapă, ne interesează doar afișarea PDU-urilor ICMP (ping). Se face prin tastarea icmp în caseta Filtru din partea de sus a Wireshark și prin apăsarea tastei Enter sau să prin clic pe butonul Aplay (semnul săgeată) pentru a vedea numai PDU-urile ICMP (ping).

c. Acest filtru face ca toate datele din fereastra de sus să dispară, dar încă se captează traficul de pe interfață. Se face Navigarea la o fereastră de prompt de comandă și se face ping adresa IP dorită.

```
C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.114:

 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

 Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
No. Time Source Destination Protocol Length Info
3 10.696465 192.168.1.147 192.168.1.114 ICMP 74 Echo (ping) request id=0x0001, …
4 10.781036 192.168.1.114 192.168.1.147 ICMP 74 Echo (ping) reply id=0x0001, …
5 11.718986 192.168.1.147 192.168.1.114 ICMP 74 Echo (ping) request id=0x0001, …
6 11.805097 192.168.1.114 192.168.1.147 ICMP 74 Echo (ping) reply id=0x0001, …
7 12.734584 192.168.1.147 192.168.1.114 ICMP 74 Echo (ping) request id=0x0001, …
8 12.829155 192.168.1.114 192.168.1.147 ICMP 74 Echo (ping) reply id=0x0001, …
9 13.750216 192.168.1.147 192.168.1.114 ICMP 74 Echo (ping) request id=0x0001, …
10 13.853254 192.168.1.114 192.168.1.147 ICMP 74 Echo (ping) reply id=0x0001, …
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Dell_dd:00:91 (00:26:b9:dd:00:91), Dst: Apple_1e:80:72 (28:37:37:1e:80:72)
Destination: Apple_1e:80:72 (28:37:37:1e:80:72)
Address: Apple_1e:80:72 (28:37:37:1e:80:72)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Dell_dd:00:91 (00:26:b9:dd:00:91)
0000 28 37 37 1e 80 72 00 26 b9 dd 00 91 08 00 45 00 (77..r.& ......E.
0010 00 3c 0e 61 00 00 80 01 00 00 c0 a8 01 93 c0 a8 .<.a.... ....
0020 01 72 08 00 4d 4a 00 01 00 11 61 62 63 64 65 66 .r..MJ.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
Specifies if this is an individual (unicast) o...broadcast/multicast) address (eth.ig), 3 byte
Packets: 10 · Displayed: 8 (80.0%)
Profile: Default

LABORATOR 4. Vizualizarea informațiilor NIC cu fir și fără fir.

Obiective

Partea 1: Identificarea și lucrul cu NIC-urile PC.

Instrucțiuni

Partea 1: Identificarea și lucrul cu NIC-urile PC.

În partea 1, vom identifica tipurile de NIC din computerul pe care îl folosim. Vom explora diferite moduri de a extrage informații despre aceste NIC-uri și cum să le activăm și să le dezactivem.

Pasul 1: Este realizat folosind „Centrul de rețea și partajare”.

a. Se face prin navigarea la Panoul de control. Se face clic pe Vizualizarea stării rețelei și a activităților sub titlul Rețea și Internet din Vizualizarea categoriei.

b. În panoul din stânga, se face clic pe linkul Schimbare setări adaptor.

c. În fereastra Conexiuni de rețea, rezultatele oferă o listă de NIC-uri disponibile pe acest computer. Se face prin căutarea adaptoarelor Wi-Fi.

Notă: Adaptoarele de rețea privată virtuală (VPN) și alte tipuri de conexiuni la rețea pot fi, de asemenea, afișate în această fereastră.

Pasul 2: Este posibil să lucrăm cu NIC wireless.

a. Se realizează prin localizarea conexiunii la rețeaua wireless. Dacă este dezactivat, se face clic dreapta și selectează ***Enable*** pentru a activa NIC wireless.

b. Dacă conexiunea de rețea fără fir nu este conectată în prezent, se face clic dreapta și selectează Conectare/Deconectare pentru a se conecta la un SSID la care sunt autorizate să se conecteze.

c. Se realizează făcând clic dreapta pe o conexiune de rețea fără fir, apoi se face clic pe ***Status***.

Se afișează fereastra de stare a conexiunii la rețea fără fir unde se pot vizualiza informații despre conexiunea fără fir.

Întrebări:

Care este identificatorul de set de servicii (SSID) pentru routerul wireless de conexiune?

Răspunsurile aici.

Care este viteza conexiunii tale wireless?

Răspunsurile aici.

e. Se face clic pe Detalii pentru a afișa fereastra Detalii conexiune la rețea.

Întrebări:

Care este adresa MAC a NIC-ului wireless?

Răspunsurile aici.

Dacă sunt listate mai multe servere DNS IPv4, atunci, dacă da, de ce ar fi listate mai multe servere DNS?

Răspunsurile aici.

f. Se face Deschiderea unui prompt de comandă Windows și tastarea ***ipconfig /all***.

```
C:\Users\ITE> ipconfig /all

Windows IP Configuration

 Host Name . . . . . . . . . . . . : DESKTOP-VITJF61

 Primary Dns Suffix . . . . . . . :
```

Node Type . . . . . : Hybrid

IP Routing Enabled. . . . . : No

WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Description . . . . . : Intel(R) Ethernet Connection (4) I219-LM

Physical Address. . . . . : 08-00-27-80-91-DB

DHCP Enabled. . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::d829:6d18:e229:a705%5(Preferred)

IPv4 Address. . . . . : 192.168.1.10(Preferred)

Subnet Mask . . . . . : 255.255.255.0

Lease Obtained. . . . . : Wednesday, September 4, 2019 1:19:07 PM

Lease Expires . . . . . : Thursday, September 5, 2019 1:19:08 PM

Default Gateway . . . . . : 192.168.1.1

DHCP Server . . . . . : 192.168.1.1

DHCPv6 IAID . . . . . : 50855975

DHCPv6 Client DUID. . . . . : 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB

DNS Servers . . . . . : 68.105.28.16

68.105.29.16

NetBIOS over Tcpip. . . . . : Enabled

Se realizează prin deschiderea unui prompt de comandă Windows.

Se poate observa că informațiile afișate aici sunt aceleași informații care au fost afișate în fereastra Detalii conexiune la rețea la Pasul e.

g. Se realizează prin închiderea ferestrei de comandă și a ferestrei Network Connection Details. Aceasta ar trebui să revină la fereastra Stare Wi-Fi. Se realizează făcând clic pe Proprietăți wireless.

În acest moment se face închiderea unui prompt de comandă Windows.

h. În fereastra Wireless Network Properties, se face clic pe fila Security.

i. Afișează tipul de securitate pe care routerul wireless conectat îl are implementat. Se face făcând clic pe caseta de selectare Afișare caractere pentru a afișa cheia de securitate reală a rețelei, în loc de caracterele ascunse, apoi se face clic pe OK.

j. După aceea, se închidei ferestrele Wireless Network Properties și Wi-Fi Status. Se face prin selectare și se face clic dreapta pe opțiunea ***Wi-Fi > Conectare/Deconectare***. Ar trebui să apară o fereastră pop-up în colțul din dreapta jos al desktopului, care afișează conexiunea curentă, împreună cu o listă de SSID-uri care se află în raza de acțiune a NIC-ului wireless al computerului. Dacă apare o bară de derulare în partea dreaptă a acestei ferestre, o putem folosi pentru a afișa SSID-uri suplimentare.

k. Ne putem alătura unuia dintre celelalte SSID-uri de rețea fără fir enumerate, făcând clic pe SSID-ul la care dorim să ne alăturăm, apoi facem clic pe Conectare.

l. Dacă am selectat un SSID securizat, ni se solicită să introducem cheia de securitate pentru SSID. Introducem cheia de securitate pentru acel SSID și facem clic pe OK.

Putem face clic pe caseta de selectare Ascundere caractere pentru a împiedica oamenii să vadă ceea ce introducem în câmpul Cheie de securitate.

Partea 2: Identificarea și utilizarea pictogramelor de rețea din bara de sistem.

În partea 2, se utilizează pictogramele de rețea din bara de sistem pentru a determina și controla NIC-urile de pe computer.

Pasul 1: Se folosește pictograma de rețea.

a. Se face clic pe bara de sistem. Se face clic pe pictograma de rețea pentru a vizualiza fereastra pop-up care afișează SSID-urile care se află în raza NIC fără fir.

b. Se face clic pe Rețea și Internet.

c. În ferestrele Setări, se face clic pe Modificare opțiuni adaptor sub titlul Modificare setări de rețea.

d. În fereastra Conexiuni de rețea, se face clic dreapta pe Wi-Fi și selectează Dezactivare.

e. Acum se face examinarea barei de sistem. Se face clic pe pictograma Rețea din nou. Cu Wi-Fi dezactivat, rețelele wireless nu mai sunt în raza de acțiune și nu mai sunt disponibile pentru conexiunile wireless.

f. De asemenea, poate dezactiva rețeaua Ethernet prin dezactivarea adaptoarelor Ethernet.

Pasul 2: Identificarea pictogramei Problemă de rețea.

a. În fereastra Conexiuni de rețea, se face dezactivarea tuturor adaptoarelor Wi-Fi și Ethernet.

b. Bara de sistem afișează acum pictograma Rețea dezactivată, care indică faptul că conectivitatea la rețea a fost dezactivată.

c. Se poate face clic pe această pictogramă pentru a reveni la setările de rețea și Internet.

EXERCITIUL 1. Explorarea stratului fizic

Obiective

Pasul 1. Examinarea informațiilor locale de adresare IP

Pasul 2. Se va folosi utilitarul ***Traceroute*** pentru a se determina calea între Sursă și Destinație.

Instrucțiuni

Partea 1: Vor fi examinate informațiile locale de adresare IP

În această parte, vor fi examinate informațiile de adresare IP în rețeaua locală de domiciliu.

Pasul 1: Ce este adresa IPv4?

Adresa IP este folosită pentru a identifica un computer atunci când trimite și primește pachete, similar cu modul în care adresa de domiciliu este utilizată pentru a trimite și primi e-mail. Se poate folosi comanda ipconfig pe Windows și comanda ifconfig pe macOS și Linux.

Notă: această activitate se deschide în interiorul rețelei de domiciliu. Dacă sunt explorate alte locații, se va naviga înapoi la Rețeaua de domiciliu.

a. Se va face clic pe PC-ul de pe birou, apoi se va face clic pe fila ***Desktop tab > Command Prompt***.

b. Se va introduce comanda ***ipconfig*** și se vor examina informațiile de adresare IPv4 pentru PC-ul existent.

C:\> ipconfig

```
FastEthernet0 Connection:(default port)
 Connection-specific DNS Suffix..:
Link-local IPv6Address.........: FE80::240:BFF:FEA6:4D5A
 IPv6 Address....................: :
 IPv4 Address....................: 192.168.0.75
 Subnet Mask.....................: 255.255.255.0
 Default Gateway.................: : 192.168.0.1
<output omitted>
C:\>
```

Adresa IPv4 este 192.168.0.75, care este cunoscută ca o adresă IPv4 privată. Majoritatea computerelor client și a altor dispozitive folosesc o adresă IPv4 privată. Acestea sunt dispozitive care nu necesită un alt dispozitiv pentru a-l accesa de pe internet. Adresele IPv4 private sunt folosite pentru a conserva numărul limitat de adrese IPv4 publice rutabile la nivel global.

c. Acest pas se va repeta pe propriul dispozitiv. Care este adresa IPv4 și gateway-ul implicit pentru dispozitivul nou?

Răspunsurile aici.

Pasul 2: Care este adresa IPv4 pentru router?

Aceeași comandă Windows ipconfig arată adresa IPv4 a router-ului local sau de acasă, cunoscută și ca gateway implicit. Se poate observa că routerul nostru local are adresa IPv4 192.168.0.1.

Acesta este routerul care conectează rețeaua locală de acasă la rețeaua furnizorului de servicii de internet și oferă acces la internet.

Notă: Se poate utiliza comanda ***route -n get*** default pentru a determina gateway-ul implicit pe un computer care utilizează sistemul de operare MacOS sau Linux.

Care este adresa IPv4 pentru router ?

Răspunsurile aici.

Pasul 3: Ce este adresa IPv4 publică?

Adresele IPv4 private nu sunt rutabile pe internet. Când pachetele IP părăsesc rețeaua locală, acestea trebuie să aibă adresa IPv4 privată înlocuită cu o adresă IPv4 publică. Adresa IPv4 publică este utilizată de servere sau de orice altă destinație pentru a trimite pachete înapoi la computerul client.

Unde are loc această traducere între adresele IPv4 private și publice? Routerul local face această traducere.

Cum se poate afla adresa publică pe care routerul local o înlocuiește cu adresa IPv4 privată?

a. Pe dispozitivul local, se va căuta pe internet „***what is my ip***”. Unele motoare de căutare vor spune o adresă IPv4 publică fără a fi nevoie să viziteze un alt site web. În plus, vor fi listate mai multe site-uri web care vor oferi această și alte informații.

Notă: Multe ISP-uri au început să folosească adrese IPv6. Adresele private sunt necesare doar pentru a conserva numărul limitat de adrese IPv4 publice. Folosind două adrese diferite și traducând între nu este necesar pentru IPv6.

b. În Packet Tracer, se va închide fereastra de comandă, apoi se va face clic pe Browser web.

c. În câmpul URL, se tastează www.tellmemyip.com și apoi se face clic pe Go.

Notă: Acest site web este fictiv și există în prezent numai în Packet Tracer.

Pe lângă adresa IPv4 publică, se poate observa că site-ul web pe care l-am folosit a furnizat și alte informații, inclusiv numele ISP-ului nostru și locația geografică. Informațiile ISP-ului sunt de obicei foarte fiabile.

Cu toate acestea, informațiile geografice (oraș, stat și țară) și localizarea geografică (latitudine și longitudine) nu sunt întotdeauna complet exacte. Se va observa că site-ul web pe care l-am folosit arată orașul ca Pacific Grove, la aproximativ 5 mile de locația noastră din Monterey. Aceste informații sunt de obicei o regiune pe care ISP-ul a folosit-o pentru toți clienții din acea zonă.

d. Pe dispozitivul local, se va utiliza unul dintre site-urile web „***what is my ip***" găsite în ultima căutare. Va fi listată adresa IPv4 publică, locația și ISP.

Răspunsurile aici.

Pasul 4: Se vor examina conexiunile în rețeaua locla.

A. Cum arată conexiunea dintre dispozitiv și router? Este cu fir sau fără fir ?

Răspunsurile aici.

b. Unde este routerul pe care îl folosește dispozitivul pentru a accesa internetul?

Răspunsurile aici.

c.Cum arată conexiunea dintre routerul local și internet? Folosește un cablu de la compania de cablu sau de la compania de telefonie ? Este wireless ? Se poate găsi cablul când iese din casă sau se poate vedea turnul de la distanță dacă este o conexiune wireless?

Răspunsurile aici.

d. Se va căuta pe YouTube ***„Tour of Home Network 2020 8-bit guy”***. Aceasta nu este o rețea locală medie de domiciliu, dar poate se pot recunoaște multe dintre aceleași dispozitive găsite în rețeaua locală proprie.

Partea 2: Se va urmări Calea Între Sursă și Destinație

În această parte, va fi folosită comanda ***traceroute*** care este folosită pentru diagnosticarea rețelei și pentru afișarea căii pe care o parcurg pachetele către o destinație. Aceasta adună informații despre fiecare hop de la dispozitiv la destinație.

Fiecare linie din ieșire desemnează adresa IP a unui router, folosită pentru a trimite pachete de la o rețea la o altă rețea. Acestea sunt cunoscute sub denumirea de ***„hops”***. În Windows, comanda este ***tracert***, în timp ce sistemele de operare macOS și Linux folosesc comanda ***traceroute***. În Packet Tracer, se va utiliza comanda Windows tracert. Hop-urile sunt simulate. Cu toate acestea, ele aderă îndeaproape la calea reală pe care ar urma-o datele între un dispozitiv din Monterey, California, și serverul web de la Universitatea din Hawaii din Honolulu.

Notă: În timpul acestei părți, se va investiga rezultatul pentru două trasee. Unul va fi de pe PC-ul de casă din Packet Tracer. Celălalt va fi de pe propriul dispozitiv.

Pasul 1: Se va utiliza comanda ***traceroute*** pentru a afișa calea de la Monterey la Hawaii.

a. În Packet Tracer, pe PC-ul de casă, va fi închisă fereastra browserului web dacă este încă deschisă. Din fila Desktop, se va face clic pe ***Command Prompt***.

b. Se va introduce comanda tracert www.hawaii.edu. Packet Tracer va dura ceva timp pentru a rezolva numele de domeniu hawaii.edu la adresa IPv4.

c. Pe laptop sau alt computer, se va deschide o fereastră de terminal și se va introduce comanda ***traceroute*** pentru

sistemul de operare local. Ieșirea locală va fi diferită de rezultatul de mai jos și de rezultatul din Packet Tracer.

Ieșirea locală va afișa cel mai probabil numele routerelor reale și adresele IPv4 publice.

Notă: În rezultatul de mai jos, adresele IPv4 reale au fost convertite în adrese IPv4 private.

C:\> tracert www.hawaii.edu

Tracing route to web00.its.hawaii.edu [172.31.149.56]

over a maximum of 30 hops:

1 3 ms 4 ms 3 ms 10.0.0.1

2 13 ms 16 ms 11 ms 10.120.89.61

3 44 ms 18 ms 18 ms po-302-1222-rur02.monterey.ca.sfba.comcast.net [10.110.178.133]

4 13 ms 14 ms 13 ms po-2-rur01.monterey.ca.sfba.comcast.net [10.139.198.129]

5 21 ms 17 ms 15 ms be-222-rar01.santaclara.ca.sfba.comcast.net [10.151.78.177]

6 16 ms 20 ms 19 ms be-39931-cs03.sunnyvale.ca.ibone.comcast.net [10.110.41.121]

7 27 ms 14 ms 20 ms be-1312-cr12.sunnyvale.ca.ibone.comcast.net [10.110.46.30]

8 24 ms 19 ms 23 ms be-303-cr01.9greatoaks.ca.ibone.comcast.net [10.110.37.178]

9 19 ms 21 ms 17 ms be-2211-pe11.9greatoaks.ca.ibone.comcast.net [10.110.32.246]

10 16 ms 23 ms 16 ms ae-3.2011.rtsw.sunn.net.internet2.edu [172.16.69.141]

11 24 ms 24 ms 23 ms et-2-3-0.3457.rtsw.losa.net.internet2.edu [172.16.20.255]

12 85 ms 87 ms 85 ms 172.16.47.134

13 87 ms 85 ms 85 ms xe-1-1-0-54-kolanut-re0.uhnet.net [172.30.205.29]

14 87 ms 86 ms 87 ms vl-669-10gigcolol3.uhnet.net [172.30.213.2]

15 * * * Request timed out.

16 * * * Request timed out.

^C

C:\>

d. Când ieșirea începe să expire, ca și pentru al 15-lea și al 16-lea hop din ieșirea de mai sus, se va introduce ***Ctrl+C*** pentru a termina traseul. În caz contrar, va continua până la atingerea maximului de 30 de hopuri. Traceroute începe să expire în acest exemplu, deoarece routerul de la sfârșitul căii este cel mai probabil configurat să nu răspundă la solicitările de traceroute.

Prima intrare evidențiată din exemplu arată primul hop ca 1.

e. Se va urmări cu atenție prima linie de ieșire. Cele trei numere care preced adresa IP sunt valori de marcaj temporal, cum ar fi 3ms, 4ms, 5ms, pentru primul hop. Acesta este timpul de călătorie dus-întors între dispozitivul sursă și router la acea adresă IPv4, în milisecunde. Traceroute include, de asemenea, adresa IP a interfeței routerului care a primit pachetul de la sursa traceroute-ului, computerul client. Intrarea evidențiată din exemplu arată că primul router are o adresă IPv4 de 10.0.0.1.

Unele hop-uri pot include, de asemenea, informații despre numele de domeniu utilizate de furnizorul de servicii pentru a ajuta la documentarea informațiilor despre router, cum ar fi:

po-302-1222-rur02.monterey.ca.sfba.comcast.net evidențiate în rezultat.

Deși ieșirea a expirat înainte de a ajunge la serverul de la hawaii.edu, hopurile anterioare oferă suficiente informații pentru a urmări calea pachetelor.

f. Pe dispozitivul local, se va încerca să urmărească traseul către alte site-uri web, cum ar fi www.netacad.com sau www.google.com.

Unele hopuri probabil vor expira. Este posibil ca unele servere web să nu răspundă la traceroute.

Pasul 2: Va fi investigat al doilea hop din ieșirea traceroute.

Traceroute arată un al doilea hop:

2 13 ms 16 ms 11 ms 10.120.89.61

Pachetele IP părăsesc acum rețeaua de domiciliu și sunt trimise către ISP.

10.120.89.61 este adresa IPv4 a primului router din afara rețelei locale de domiciliu. Acest router aparține ISP-ului. Acest router este cunoscut ca punctul de prezență al ISP-ului sau POP. Acesta este locul în care ISP-ul oferă clienților săi acces la internet.

Conexiunea fizică dintre utilizatorul final și POP este cunoscută sub numele de buclă locală sau este uneori denumită „ultima milă”.

În mod tradițional, bucla locală reprezenta liniile telefonice de la sediul unui client la centrala telefonică locală, uneori denumită Biroul Central (CO). Cablurile de cupru, perechi răsucite au fost folosite pentru a transporta voce analogică și informații de semnalizare.

Astăzi, bucla locală poate include și cabluri pentru a transporta informații digitale, care pot fi cu fir sau

fără fir. În ceea ce privește conexiunea la internet, bucla locală conectează sediul clientului la ISP POP.

Bucla locală poate fi unul dintre mai multe tipuri diferite de conexiuni, inclusiv:

• *Conexiune prin cablu, folosind de obicei același cablu coaxial folosit pentru televizor și telefon*

• *DSL (Digital Subscriber Line) folosind aceeași linie telefonică pentru telefon și TV*

• *Semnale wireless sau buclă locală wireless (WLL), inclusiv tehnologii celulare*

• *Conexiune prin satelit, de obicei același semnal transmis ca cel utilizat pentru televizor*

• *Cablu de fibra optica*

• *Linie telefonică cu acces dial-up folosind același cablu de cupru cu pereche răsucită folosit pentru telefon*

a. În Packet Tracer, se va observa că PC-ul de casă de pe birou este conectat la routerul de casă de pe raftul din spatele biroului. Cu toate acestea, routerul de casă nu este conectat direct la router la următorul hop.

În schimb, este conectat la un modem prin cablu. Acest cablu modem nu este un router. Prin urmare, nu este raportat ca un hop în ieșirea traceroute.

b. Se va naviga la Monterey. Se va observa că următorul hop este legat fizic de clădirea Comcast POP. Se va face clic pe Comcast POP. Un POP este situat fizic într-un centru de date. Un centru de date este o facilitate fizică pe care organizațiile o folosesc pentru a-și găzdui echipamentele, aplicațiile și datele esențiale. Componentele cheie ale designului unui centru de date includ routere, comutatoare, firewall-uri, sisteme de stocare și servere. Deși Comcast POP ar fi de obicei un centru de date în lumea reală, în Packet Tracer stochează doar echipamentul necesar pentru această activitate. În

Rack, vor fi văzute mai multe dispozitive, inclusiv un dispozitiv care simulează un sistem de terminare a modemului de cablu (CMTS), routerul Comcast-POP-Monterey, un comutator multistrat și două servere.

c. Se vor investiga conexiunile fizice dintre dispozitive. O interfață a Comcast-CMTS este conectată direct la modemul prin cablu din rețeaua de domiciliu. Cealaltă interfață este conectată la următorul router hop, Comcast-POP-Monterey, care se află direct sub acesta. A doua interfață Comcast-POP-Monterey se conectează la următorul hop, care va fi investigat în următorul pas. A treia interfață este

conectat la comutator, care este apoi conectat la cele două servere. Serverul DNS traduce www.hawaii.edu și ww.tellmemyip.com la adresa IPv4 respectivă. Serverul web deservește site-ul web www.tellmemyip.com.

d. În rețeaua locală, ce tehnologie folosește bucla locală? Cablu? DSL? Satelit? Celular?

Dacă este o conexiune prin cablu, se va vedea dacă poate găsi cablul care părăsește rețeaua de acasă. Unde se duce? La un stâlp de telefon? Subteran?

e. Al doilea hop din comanda ta traceroute de pe dispozitiv este de obicei POP-ul ISP-ului local. Care este adresa IP pentru POP-ul acestui ISP?

Pasul 3: Se va încerca să se descopere locația fizică a adresei IP pentru ISP local POP.

Cine deține POP-ul pentru al doilea router din ieșirea ta traceroute? Se poate căuta pe internet ***„ip lookup”***, ceea ce va avea ca rezultat o listă de site-uri web care vor oferi informații despre o adresă IP.

Va fi completat tabelul de mai jos cu informațiile descoperite din cercetarea căutării IP. Poate fi necesar să fie vizitate mai multe site-uri web de căutare pentru a obține toate informațiile.

2nd Hop IPv4 address:	
ISP:	
CITY:	
REGION:	
COUNTRY:	

Informațiile despre numele ISP-ului sunt de obicei foarte sigure. Cu toate acestea, este posibil ca informațiile despre locația locală fizică să nu fie exacte. În multe cazuri, locația fizică enumerată poate fi la sute de mile de locul unde se află de fapt routerul și centrul de date. Ar putea fi biroul administrativ al ISP-ului sau chiar o locație aleatorie.

Deoarece informațiile de geolocalizare (longitudine și latitudine) înregistrate de ISP sunt rareori exacte, nu se va putea baza pe aceste informații pentru a găsi locația reală a POP.

În acest caz, trebuie să fie contactat ISP-ul local pentru a vedea dacă vor spune unde este localizat acest POP.

Pasul 4: Se va investiga de ce informațiile de localizare geografică nu sunt întotdeauna exacte.

Se vor căuta pe Internet „600 de milioane de adrese IP din Kansas”. Vor fi găsite mai multe articole despre un ISP care a ales să folosească o locație geografică (latitudine și longitudine) din centrul Statelor Unite pentru a înregistra peste 600 de milioane de adrese IP. Din păcate, această latitudine și longitudine anume sa întâmplat să fie o casă privată în mijlocul Kansasului și nu un ISP.

Oricine are plângeri cu privire la ISP, conexiunea la internet sau primind spam de la una dintre aceste adrese IP ar contacta proprietarii.

Este corect a fi sceptic cu privire la orice informații de localizare geografică care arată că pachetele merg dintr-o locație, la sute sau mii de mile distanță, apoi

înapoi. De exemplu, pachetele nu sunt în mod normal trimise din California în Kansas și înapoi în California.

Pasul 5: Se va investiga rețeaua ISP-ului local.

Pentru exemplul de ieșire reală de traceroute prezentat mai jos, hopurile de la 2 la 9 aparțin Comcast. Reamintim că adresele IPv4 reale pentru aceste routere au fost modificate pentru această activitate. Prin urmare, nu vor putea fi folosite pentru a face o căutare IP. Cu toate acestea, se va putea căuta adresele IP pentru ieșirea locală de traceroute pentru a determina câte dintre hop-uri aparțin ISP-ului local.

C:\> tracert www.hawaii.edu

Tracing route to web00.its.hawaii.edu [172.31.149.56]

over a maximum of 30 hops:

1 3 ms 4 ms 3 ms 10.0.0.1

2 13 ms 16 ms 11 ms 10.120.89.61

3 44 ms 18 ms 18 ms po-302-1222-rur02.monterey.ca.sfba.comcast.net

[10.110.178.133]

4 13 ms 14 ms 13 ms po-2-rur01.monterey.ca.sfba.comcast.net

[10.139.198.129]

5 21 ms 17 ms 15 ms be-222-rar01.santaclara.ca.sfba.comcast.net

[10.151.78.177]

6 16 ms 20 ms 19 ms be-39931-cs03.sunnyvale.ca.ibone.comcast.net

[10.110.41.121]

7 27 ms 14 ms 20 ms be-1312-cr12.sunnyvale.ca.ibone.comcast.net

[10.110.46.30]

8 24 ms 19 ms 23 ms be-303-cr01.9greatoaks.ca.ibone.comcast.net

[10.110.37.178]

9 19 ms 21 ms 17 ms be-2211-pe11.9greatoaks.ca.ibone.comcast.net

[10.110.32.246]

10 16 ms 23 ms 16 ms ae-3.2011.rtsw.sunn.net.internet2.edu [172.16.69.141]

11 24 ms 24 ms 23 ms et-2-3-0.3457.rtsw.losa.net.internet2.edu

[172.16.20.255]

12 85 ms 87 ms 85 ms 172.16.47.134

13 87 ms 85 ms 85 ms xe-1-1-0-54-kolanut-re0.uhnet.net [172.30.205.29]

14 87 ms 86 ms 87 ms vl-669-10gigcolol3.uhnet.net [172.30.213.2]

15 * * * Request timed out.

16 * * * Request timed out.

^C

C:\>

a. În Packet Tracer, se va naviga la Monterey, apoi se va face clic pe clădirea monterey.ca.

b. Se va observa că cele două routere din rack aparțin comcast.net. Se va putea trece mouse-ul peste fiecare router pentru a vedea adresele IPv4. De asemenea, se poate face clic pe fiecare router și investiga adresa IPv4 în fila Config.

c. Care este adresa IPv4 a celui de-al treilea hop din ieșirea Packet Tracer traceroute ?

Răspunsuri aici.

d. Ce router și interfață din clădirea monterey.ca sunt configurate cu această adresă IPv4 ?

Răspunsuri aici.

e. Care este adresa IPv4 a celui de-al 4-lea hop din ieșirea Packet Tracer traceroute ?

Răspunsuri aici.

f. Ce router și interfață din clădirea monterey.ca sunt configurate cu această adresă IPv4 ?

Răspunsuri aici.

g. De ce credeți că adresele IP pentru celelalte interfețe nu sunt afișate în ieșirea traceroute ?

Răspunsuri aici.

h. Vor fi listate hopurile din ieșirea locală de traceroute proprii care aparțin ISP-ului local.

Răspunsuri aici.

Pasul 6: Se vor investiga numele de domenii din ieșire pentru a descoperi mai multe indicii despre locația routerelor la fiecare hop.

Numele de domeniu (dacă există unul) din traceroute poate oferi informații suplimentare. Nu există o convenție standard de denumire. Dacă și cum este utilizat este numai la latitudinea administratorului dispozitivului. În rezultatul traceroute de mai sus, Comcast a furnizat informații în numele domeniului care vă oferă un indiciu despre unde poate fi localizat de fapt routerul:

- po-302-1222-rur02.monterey.ca.sfba.comcast.net
- po-2-rur01.monterey.ca.sfba.comcast.net

- be-222-rar01.santaclara.ca.sfba.comcast.net
- be-39931-cs03.sunnyvale.ca.ibone.comcast.net
- be-1312-cr12.sunnyvale.ca.ibone.comcast.net
- be-303-cr01.9greatoaks.ca.ibone.comcast.net
- be-2211-pe11.9greatoaks.ca.ibone.comcast.net

Toate aceste orașe sunt situate în aceeași regiune geografică cunoscută sub numele de San Francisco Bay Area (SFBA) și sunt controlate de Comcast.

- Monterey, California
- Santa Clara, California
- Sunnyvale, California
- San Jose, California (9greatoaks.ca)

Sa făcut ipoteza în Packet Tracer că toate routerele cu același oraș în nume de domeniu sunt în același centru de date. De exemplu, după cum am văzut, aceste două routere se află în clădirea monterey.ca:

- po-302-1222-rur02.monterey.ca.sfba.comcast.net
- po-2-rur01.monterey.ca.sfba.comcast.net

a. Ce informații, dacă există, pot fi descifrate din numele de domenii pentru ISP-ul local ?

Răspunsuri aici.

b. În Packet Tracer, se va naviga la Monterey. Se va observa legătura spre nord care iese din monterey.ca.

c. Se va naviga cu un nivel până la Intercity. (Packet Tracer nu permite redenumirea Intercity.) Se va vedea o reprezentare a legăturilor fizice dintre casa din Monterey și insula Oahu, unde este serverul Jose, și apoi Los Angeles înainte de a traversa Oceanul Pacific la Honolulu.

d. Se va face clic pe San Jose. Se va observa că există trei clădiri, fiecare etichetată cu o parte a numelui de

domeniu descoperit în ieșirea traceroute. Routerele cu același nume de domeniu sunt situate în aceeași clădire.

Se va investiga fiecare clădire, router și interfață pentru a completa următorul tabel.

Hop	Domain Name	Interface	Ipv4 Address
5			
6			
7			
8			
9			

Care este clădirea, routerul, interfața și adresa IPv4 pentru legătura de ieșire către Los Angeles?

Răspunsuri aici.

IXP Data Center - Un IXP (Internet Exchange Point) este de obicei un centru de colocare care găzduiește ISP-uri și alți clienți, cu scopul de a se conecta între ei.

La un moment dat, un ISP precum Comcast va trebui să trimită pachetele către un alt ISP. Acest lucru se întâmplă de obicei într-un IXP. Locațiile sunt adesea considerate ca fiind la „marginea” rețelei unui ISP, adică un loc în care pachetele părăsesc rețeaua internă a ISP-ului și sunt redirecționate către un alt ISP.

Acesta este un loc în care ISP-ii și alții pot face schimb de trafic de internet între rețelele lor.

IXP-urile sunt de obicei deținute și operate de o parte neutră, ceea ce înseamnă că nu sunt un ISP sau „client” al propriului centru de date.

Notă: Termenul Network Access Point (NAP) este un termen mai vechi pentru IXP, care a fost acum depreciat.

Pasul 7: Se va investiga legătura dintre Comcast și Internet2.

HOP 9 - Acesta este ultimul hop în rețeaua ISP Comcast înainte ca pachetele să fie transmise către un alt ISP.

9 19 ms 21 ms 17 ms be-2211-pe11.9greatoaks.ca.ibone.comcast.net

[10.110.32.246]

Din nou, Comcast oferă un indiciu unde se află routerul. Cu toate acestea, numele de domeniu nu indică un oraș, ci o adresă.

a. Se va căuta pe internet „9 great oaks California” și se va găsi că un centru de date Equinix este situat la 9 Great Oaks Boulevard din San Jose, California. Dacă atunci se va folosi Google Maps și se va căuta adresa respectivă, se va putea folosi vizualizarea prin satelit sau vizualizarea străzii pentru a vedea clădirea reală.

Equinix este un Internet Exchange Point (IXP) cunoscut sub numele de Equinix SV5. Oferă conexiuni între diferite ISP-uri și găzduiește conexiunea dintre Comcast și următorul ISP, care este Internet2.

b. Există multe site-uri web care oferă informații despre marile centre de date IXP, inclusiv ISP-urile pe care le găzduiesc. Se va căuta pe internet „Inflect data center”. Se va folosi site-ul web pentru a explora și se va vedea dacă se poate găsi unde listează Comcast ca una dintre organizațiile găzduite la Equinix SV5.

c. În Packet Tracer, se va naviga la San Jose, dacă este necesar, apoi se va face clic pe clădirea 9greatoaks.ca. Se va observa că numele celui de-al treilea router din rack indică faptul că acesta aparține Internet2. Acest router este al 10-lea hop din ieșirea traceroute.

10 16 ms 23 ms 16 ms ae-3.2011.rtsw.sunn.net.internet2.edu [172.16.69.141]

d. Care este interfața pentru al 10-lea hop?

Răspunsuri aici.

Pasul 8: Va fi investigat Internet2.

Internet2 ? Este aceasta o versiune nouă a internetului? Nu. Internet2 este un ISP non-profit. Este un consorțiu de cercetare, educație, industrie și comunități guvernamentale care oferă servicii de rețea de mare viteză, servicii cloud și alte servicii adaptate pentru cercetare și educație.

Se vor căuta informații Wikipedia și alte site-uri web pentru a obține mai multe informații despre Internet2. Ce viteză are coloana vertebrală a Internetului care oferă conexiuni între membrii săi?

Răspunsuri aici.

Pentru informare, se va căuta „This Man Launched a New Internet Service Provider from His Garage”. Este povestea despre Brandt Kuykendall, un locuitor al orășelului Dillon Beach, California. Serviciul de internet din orașul său era prea lent și scump, așa că și-a început propriul ISP din garaj.

Pasul 9: Se va investiga legătura cu Los Angeles.

Traceroute-ul nostru dezvăluie că următorul hop este un alt router Internet2. Din fericire, numele de domeniu ne oferă aceste informații.

11 24 ms 24 ms 23 ms

et-2-3-0.3457.rtsw.losa.net.internet2.edu

[172.16.20.255]

O căutare a „internet2 router proxy” poate ajuta la verificarea faptului că „losa” din numele domeniului indică faptul că acest router Internet2 se află în Los Angeles, California. Pachetele IP au părăsit zona golfului San Francisco ("sfba") se deplasează spre sud, la aproximativ 350 de mile, până la Los Angeles, California.

a. În Packet Tracer, se va naviga la nivelul Intercity, apoi se va face clic pe Los Angles.

b. Clădirea losa.net.internet2.edu este situată undeva în Los Angeles. Se va face clic pe clădire pentru a intra în ea.

c. Rack-ul are un router, care se conectează la zona golfului San Francisco și un cablu submarin care traversează Oceanul Pacific. Care este interfața folosită pentru acest al 11-lea hop în ieșirea traceroute?

Răspunsuri aici.

Pasul 10: Se va investiga legătura peste Oceanul Pacific.

Următorul hop în traceroute este:

12 85 ms 87 ms 85 ms 172.16.47.134

Deși nu sunt furnizate informații despre numele de domeniu, există două informații interesante aici.

Deși nu se va putea folosi adresa IP pentru acest exemplu, deoarece a fost convertit într-o adresă IP privată, va putea folosi un site web „IP lookup” pentru a determina cine deține adresa IP pentru cercetare. În exemplul de aici, autorii au putut determina că adresa IP pentru hop 12 aparține și Internet2.

Și mai interesant este atunci când ne uităm la timpii dus-întors de 85 ms, 87 ms și 85 ms. Se va observa că există o creștere mare a timpului în comparație cu hopul anterior de la San Jose la Los Angeles (24 ms, 24 ms, respectiv 23 ms).

De ce vedem creșteri incrementale mai mici de la hopurile 1 la 11 și apoi un salt atât de mare în timpul dus-întors la hop 12?

Putem deduce că acest router de la hop 12 trebuie să fie mult mai departe decât routerul anterior de la hop 11 din Los Angeles, California. De asemenea, observăm că nu există alte locuri din traseul nostru care să prezinte o diferență atât de mare de timp, precum cea dintre hop 11 din California și hop 12.

Prin urmare, aceste pachete trebuie să fi parcurs o distanță mult mai mare decât oricare alte două puncte de-a lungul căii de la Monterey la Hawaii. Routerul de la hop 12 trebuie să fie în Hawaii, unde pachetele au călătorit la aproape 2.500 de mile de California.

Acest router se află la Internet2 Peer Exchange (IP2X) din Hawaii și este ultimul hop din rețeaua Internet2.

IP2X redirecționează pachetele către următorul router hop care aparține Universității din Hawaii.

a. Se va căuta pe internet „hartă cablu submarin” și se va vedea dacă se pot găsi cabluri submarine care au un punct de aterizare atât în Hermosa Beach, cât și în Hawaii. Câte cabluri submarine se termină la Hermosa Beach?

Răspunsuri aici.

b. Cum se numește cablul submarin care merge de la Hermosa Beach la Hawaii?

Răspunsuri aici.

c. Cum se numește punctul de aterizare din Hawaii?

Răspunsuri aici.

d. Câte cabluri submarine se termină în acest punct de aterizare din Hawaii?

Răspunsuri aici.

e. Cablul SEA-US a fost realizat printr-un parteneriat între Universitatea din Hawaii și RAM Telecom International, Inc. (RTI). Acest parteneriat permite sistemului Universității din Hawaii să conecteze Hawaii cu Statele Unite continentale, Guam și nu numai.

Se va căuta „Cablul submarin viteză conexiunile UH în Pacific” pentru a găsi un articol și un videoclip despre acest cablu întins peste Oceanul Pacific.

f. Pentru mai multe informații, vor fi căutate pe YouTube sau alte site-uri video pentru „cablu submarin”. Se vor găsi multe videoclipuri care arată cum sunt construite și așezate aceste cabluri pe fundul mării.

g. În Packet Tracer, se va naviga la nivelul Intercity. Se va urmări cablul peste Oceanul Pacific. Aici sunt afișate două repetoare, deși mai sunt zeci. Se va căuta pe internet pentru a afla câți kilometri separă fiecare repetitor pe un cablu submarin.

Răspunsuri aici.

h. Se va face clic pe Honolulu. Se va face transferul acum pe insula Oahu. Se va observa că acum cablul submarin se termină la Makaha.

i. Se va face clic pe clădirea I2px-Hawaii. Există două routere în rack. Primul aparține lui I2PX și reprezintă al 12-lea hop de la ieșirea traceroute. Ce interfață este atribuită celui de-al 12-lea hop ?

Pasul 11: Se va investiga legătura dintre Internet2 și rețeaua Universității din Hawaii.

Următorul hop pe traseu este:

13 87 ms 85 ms 85 ms xe-1-1-0-54-kolanut-re0.uhnet.net [205.166.205.29]

Numele de domeniu pentru acest router indică faptul că face parte din rețeaua Universității din Hawaii (uhnet.net). Acest router este situat la Honolulu Internet Exchange (HIX) din Honolulu, Hawaii, cel mai probabil situat în același IXP ca și routerul i2px.hawaii.

În Packet Tracer, se va observa că al doilea router din rack i2px-Hawaii este router-ul kolanut-re0.uhnet.net. Ce interfață este atribuită celui de-al 13-lea hop ?

Pasul 12: Se va investiga ultima adresă IP cunoscută din ieșirea traceroute.

În Packet Tracer, toate hopurile sunt simulate. Se va naviga înapoi la Honolulu și se va investiga clădirea uhnet.net și campusul hawaii.edu. În fiecare clădire, se vor găsi dispozitivele care simulează restul traseului ***traceroute*** în Packet Tracer..

În ieșirea traceroute din lumea reală, hopurile încep să expire. Pentru exemplul din această activitate, expiră la hop 15, dar cel mai probabil, expiră la un hop diferit dacă va urma o altă rută.

C:\> tracert www.hawaii.edu

Tracing route to web00.its.hawaii.edu [172.31.149.56]

over a maximum of 30 hops:

<output omitted>

14 87 ms 86 ms 87 ms vl-669-10gigcolol3.uhnet.net [172.30.213.2]

15 * * * Request timed out.

16 * * * Request timed out.

^C

Pentru hop 14, numele implică faptul că acesta este un alt router care face parte din rețeaua Universității din Hawaii. În acest moment, traseul începe să expire.

Este obișnuit ca routerele și alte dispozitive, cum ar fi un server web, să nu răspundă la mesajele ***traceroute***. Un router poate fi chiar configurat să interzică orice mesaje ***traceroute*** care sunt transmise către următorul router hop.

Cel mai probabil, un router sau firewall de la Universitatea din Hawaii, înainte de serverul web, blochează orice alte mesaje ***traceroute*** să intre în rețea.

Contents

CAPITOLUL 5. NUMBER SYSTEMS 2

5.0 Introduction 2

5.0.1 - Tthis course 2

5.0.2 – OBJECTIVE 2

5.1 Binary Number System 2

5.1.1 - Binary and IPv4 Addresses 2

5.1.2 - Binary Positional Notation 4

5.1.4 - Convert Binary to Decimal 6

5.1.5 - Activity - Binary to Decimal Conversions 7

5.1.6 - Decimal to Binary Conversion 7

5.1.7 - Decimal to Binary Conversion Example 11

5.1.8 - Activity - Decimal to Binary Conversions 12

5.1.9 - Activity - Binary Game 12

5.1.10 - IPv4 Addresses 12

5.2 Hexadecimal Number System 13

5.2.1 - Hexadecimal and IPv6 Addresses 13

5.2.3 - Decimal to Hexadecimal Conversions 15

5.2.4 - Hexadecimal to Decimal Conversion 15

5.2.5 - Check Your Understanding - Hexadecimal Number System 16

5.3 SUMMARY 16

CAPITOLUL 5. NUMBER SYSTEMS

5.0 Introduction

5.0.1 - Tthis course

Aceasta este o adresă IPv4 pe 32 de biți a unui computer dintr-o rețea: 11000000.10101000.00001010.00001010. Este afișat în binar.

Aceasta este adresa IPv4 pentru același computer în zecimală punctată: 192.168.10.10.

Cu care este de prefera să selucreze ?

Adresele IPv6 au 128 de biți ! Pentru a face aceste adrese mai ușor de gestionat, IPv6 folosește un sistem hexazecimal de la 0-9 și literele A-F.

Ca specialist in rețele de calculatoare, trebuie să știm cum să convertim adresele binare în zecimale punctate și adresele zecimale punctate în binar. De asemenea, va trebui să știm cum să convertim o valoare zecimală în hexazecimal și invers.

5.0.2 – OBJECTIVE

Calcularea numerelor între sisteme zecimal, binar și hexazecimal.

Topic Title	Topic Objective
Binary Number System	Calcularea numerelor între sistemele zecimal și binar.
Hexadecimal Number System	Calcularea numerelor între sistemele zecimal și hexazecimal.

5.1 Binary Number System

5.1.1 - Binary and IPv4 Addresses

Adresele IPv4 încep in format binar, ca o serie de valori de 1 și 0. Acestea sunt greu de gestionat, așa că administratorii de rețea trebuie să le convertească în numere zecimale.

Binar este un sistem de numerotare care constă din cifrele 0 și 1 numite biți. În schimb, sistemul de numerotare zecimală este format din 10 cifre formate din cifrele 0 – 9.

Formatul Binar este important să fie înțeles, deoarece gazdele, serverele și dispozitivele de rețea folosesc adresare binară. Mai exact, folosesc adrese IPv4 binare, așa cum se arată în figură, pentru a se identifica reciproc.

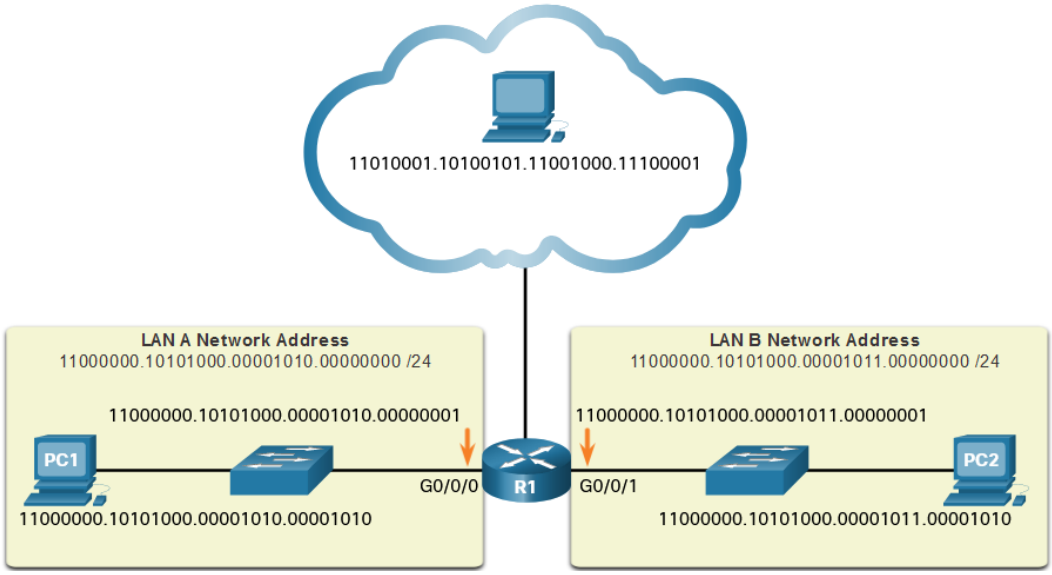


Fig. 5.1. Reprezentare IPv4 in format binar.

Fiecare adresă este formată dintr-un șir de 32 de biți, împărțit în patru secțiuni numite octeți. Fiecare octet conține 8 biți (sau 1 octet) separați cu un punct. De exemplu, PC1 din figură îi este atribuită adresa IPv4 11000000.10101000.00001010.00001010. Adresa gateway-ului implicită ar fi cea a interfeței R1 Gigabit Ethernet 11000000.10101000.00001010.00000001.

Formatul Binar funcționează bine cu gazde și dispozitive de rețea. Cu toate acestea, este foarte dificil să lucreze oameni cu astfel de reprezentari.

Pentru ușurința utilizării de către oameni, adresele IPv4 sunt de obicei exprimate în notație zecimală punctată. PC1 i se atribuie adresa IPv4 192.168.10.10, iar adresa de gateway implicită este 192.168.10.1, așa cum se prezinta în figura de mai jos.

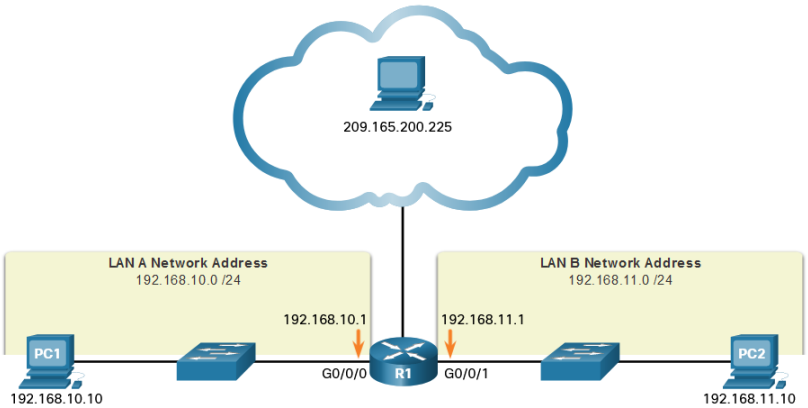


Fig. 5.2. Reprezentarea adresei IPv4 in format zecimal.

Pentru o înțelegere solidă a adresei de rețea, este necesar să se cunoasca adresarea binară și să deține abilități practice de conversie între adrese IPv4 binare și zecimale punctate. De aceea in

acest subcapitol se va acoperi modul de conversie între sistemele de numerotare de bază doi (binar) și de bază 10 (zecimală).

5.1.2 - Binary Positional Notation

Învățarea unei conversii rapide din binar în zecimal necesită înțelegerea notației poziționale. Notarea pozițională înseamnă că o cifră reprezintă valori diferite în funcție de „poziția” pe care o ocupă cifra în succesiunea de numere. Este bine cunoscut cel mai comun sistem de numerotare, sistemul de notație zecimală (bază 10).

Sistemul de notație pozițională zecimală funcționează așa cum este descris în tabel.

Radix	**10**	**10**	**10**	**10**
Position in Number	3	2	1	0
Calculate	(10^3)	(10^2)	(10^1)	(10^0)
Position value	1000	100	10	1

Următoarele marcatoare descriu fiecare rând al tabelului.

Rândul 1, Radix este baza numerică. Notația zecimală se bazează pe 10, prin urmare radica este 10.

Rândul 2, Poziția în număr are în vedere poziția numărului zecimal începând cu, de la dreapta la stânga, 0 (poziția 1), 1 (poziția 2), 2 (poziția 3), 3 (poziția 4). Aceste numere reprezintă, de asemenea, valoarea exponențială utilizată pentru a calcula valoarea poziațională în al 4-lea rând.

Rândul 3 calculează valoarea poziațională luând radica și ridicând-o cu valoarea exponențială a poziției sale în rândul 2. Notă: n^0 este = 1.

Valoarea poziațională a rândului 4 reprezintă unități de mii, sute, zeci și unități.

Pentru a utiliza sistemul poziațional, potriviți un anumit număr cu valoarea sa poziațională. Exemplul din tabel ilustrează modul în care este utilizată notația poziațională cu numărul zecimal 1234.

	Thousands	**Hundreds**	**Tens**	**Ones**
Positional Value	1000	100	10	1
Decimal Number (1234)	1	2	3	4
Calculate	1 x 1000	2 x 100	3 x 10	4 x 1
Add them up…	1000	+ 200	+ 30	+ 4
Result	**1.234**			

În schimb, notația pozițională binară funcționează așa cum este descris în tabelelul urmator:

Radix	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**
Position in Number	7	6	5	4	3	2	1	0
Calculate	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Position value	128	64	32	16	8	4	2	1

Următoarele marcatoare descriu fiecare rând al tabelului.

Rândul 1, Radacina este baza numerică. Notația binară se bazează pe 2, prin urmare radacina este 2.

Rândul 2, Poziția în număr consideră poziția numărului binar începând cu, de la dreapta la stânga, 0 (poziția 1), 1 (poziția 2), 2 (poziția 3), 3 (poziția 4). Aceste numere reprezintă, de asemenea, valoarea exponențială utilizată pentru a calcula valoarea pozițională în al 4-lea rând.

Rândul 3 calculează valoarea pozițională luând radacina și ridicând-o cu valoarea exponențială a poziției sale în rândul 2.

Notă: n^0 este = 1.

Valoarea pozițională a rândului 4 reprezintă unitățile de unu, doi, patru, opt etc.

Exemplul din tabel ilustrează modul în care un număr binar 11000000 corespunde numărului 192. Dacă numărul binar ar fi fost 10101000, atunci numărul zecimal corespunzător ar fi 168.

Positional Value	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Binary Number (11000000)	1	1	0	0	0	0	0	0
Calculate	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Add Them Up..	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	**192**							

5.1.3 - Check Your Understanding - Binary Number System

1. Which is the binary equivalent to the 192.168.11.10 IP address?

- 11000000.11000000.00001011.00001010
- 11000000.10101000.00001011.00001010
- 11000000.10101000.00001010.00001011
- 11000000.10101000.00001011.00010010

2. Which of the following is the binary equivalent to the 172.16.31.30 IP address?

- 11000000.00010000.00011111.00011110
- 10101000.00010000.00011111.00011110
- 10101100.00010000.00011110.00011110
- 10101100.00010000.00011111.00011110

5.1.4 - Convert Binary to Decimal

Pentru a converti o adresă IPv4 binară în echivalentul său zecimal punctat, împărțim adresa IPv4 în patru octeți de 8 biți. Apoi aplicam valoarea pozițională binară la primul număr binar octet și calculam în consecință.

De exemplu, luam în considerare că 11000000.10101000.00001011.00001010 este adresa IPv4 binară a unei gazde. Pentru a converti adresa binară în zecimală, începem cu primul octet, așa cum se arată în tabel. Introducem numărul binar de 8 biți sub valoarea pozițională a rândului 1 și apoi calculam pentru a produce numărul zecimal 192. Acest număr intră în primul octet al notației zecimale punctate.

Positional Value	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Binary Number (11000000)	1	1	0	0	0	0	0	0
Calculate	128	64	32	16	8	4	2	1
Add Them Up...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	**192**							

Apoi convertim al doilea octet de 10101000 așa cum se arată în tabel. Valoarea zecimală rezultată este 168 și intră în al doilea octet.

Positional Value	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Binary Number (10101000)	1	0	1	0	1	0	0	0
Calculate	128	64	32	16	8	4	2	1
Add Them Up...	128	+ 0	+ 32	+ 0	+ 8	+ 0	+ 0	+ 0
Result	**168**							

Convertim al treilea octet de 00001011 așa cum se arată în tabel.

Positional Value	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Binary Number (00001011)	0	0	0	0	1	0	1	1
Calculate	128	64	32	16	8	4	2	1
Add Them Up...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 1
Result	**11**							

Convertim al patrulea octet din 00001010 așa cum se arată în tabel. Aceasta completează adresa IP și produce 192.168.11.10.

Positional Value	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Binary Number (00001010)	0	0	0	0	1	0	1	0
Calculate	128	64	32	16	8	4	2	1
Add Them Up...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 0
Result	**10**							

5.1.5 - Activity - Binary to Decimal Conversions

Instrucțiuni

Această activitate vă permite să exersați conversia binar în zecimal pe 8 biți atât cât este necesar. Este recomandat să se lucreze cu acest instrument până când se poate face conversia fără erori. Sa se converteasca numărul binar afișat în octet la valoarea sa zecimală.

Enter decimal answer below.

Decimal Value								
Base	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0
Position	128	64	32	16	8	4	2	1
Bit	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**0**

Binary Number

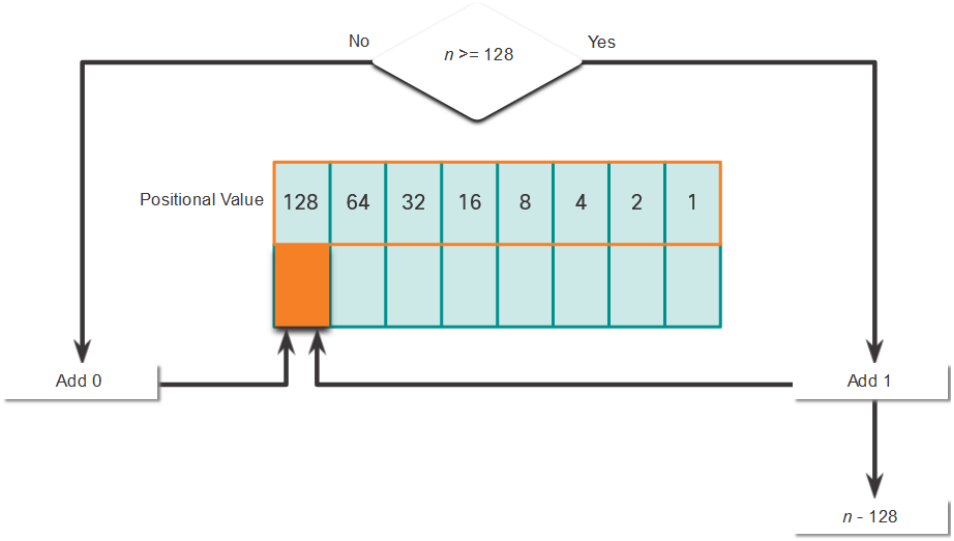
5.1.6 - Decimal to Binary Conversion

De asemenea, este necesar să se înțeleaga cum să se converteasca o adresă IPv4 zecimală punctată în binar. Un instrument util este tabelul binar de valori poziționale.

Numărul zecimal al octetului (n) este egal sau mai mare decât bitul cel mai semnificativ (128)?

Dacă nu, atunci se introduce 0 binar în valoarea poziţională 128.

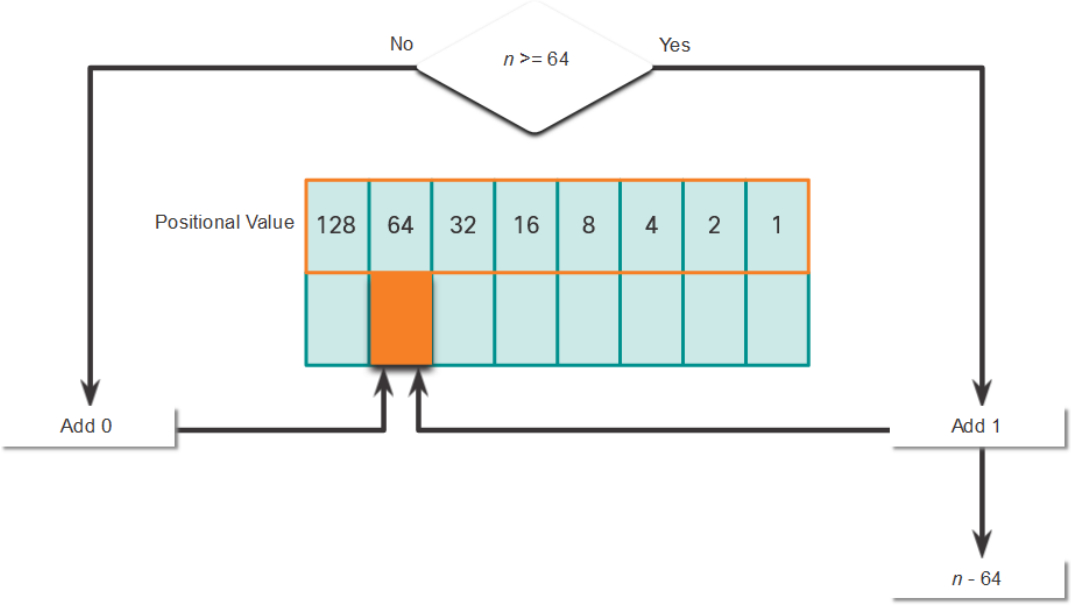
Dacă da, se adăuga un 1 binar în valoarea poziţională 128 şi se scade 128 din numărul zecimal.



Este numărul zecimal al octetului (n) egal sau mai mare decât următorul bit cel mai semnificativ (64)?

Dacă nu, atunci se introduce 0 binar în valoarea poziţională 64.

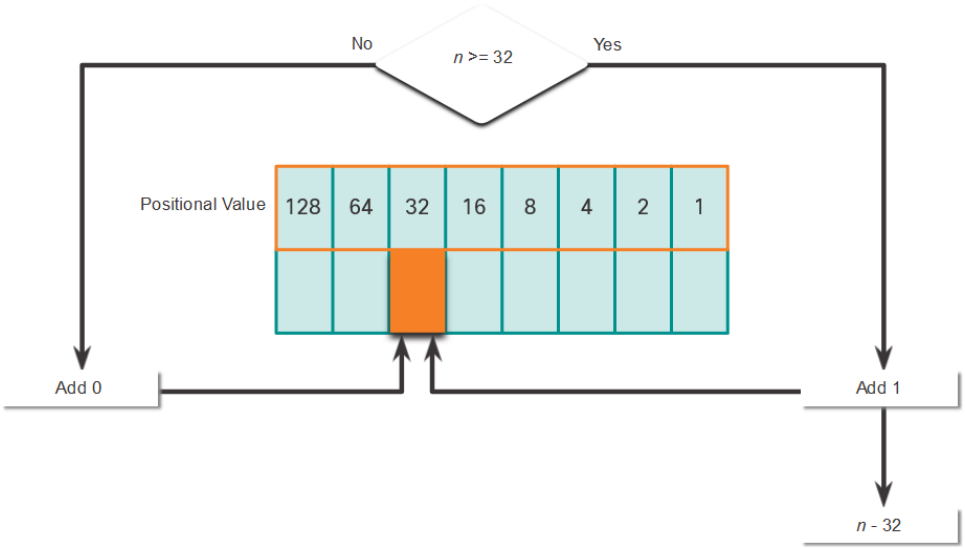
Dacă da, se adauga un 1 binar în valoarea poziţională 64 şi se scade 64 din numărul zecimal.



Numărul zecimal al octetului (n) este egal sau mai mare decât următorul bit cel mai semnificativ (32)?

Dacă nu, atunci se introduce 0 binar în valoarea poziţională 32.

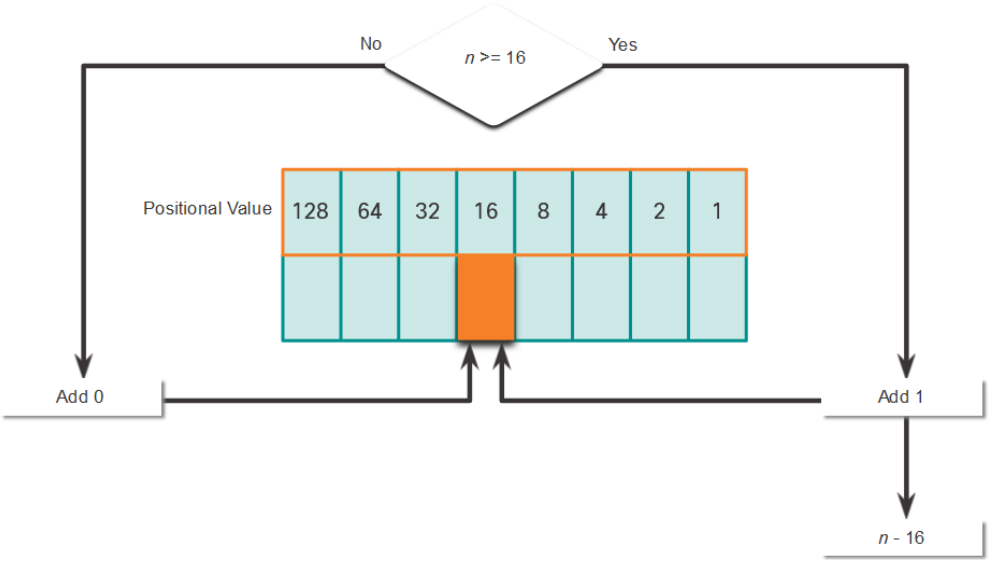
Dacă da, se adaugă un 1 binar în valoarea poziţională 32 şi se scade 32 din numărul zecimal.



Numărul zecimal al octetului (n) este egal sau mai mare decât următorul bit cel mai semnificativ (16)?

Dacă nu, atunci se introduce 0 binar în valoarea poziţională 16.

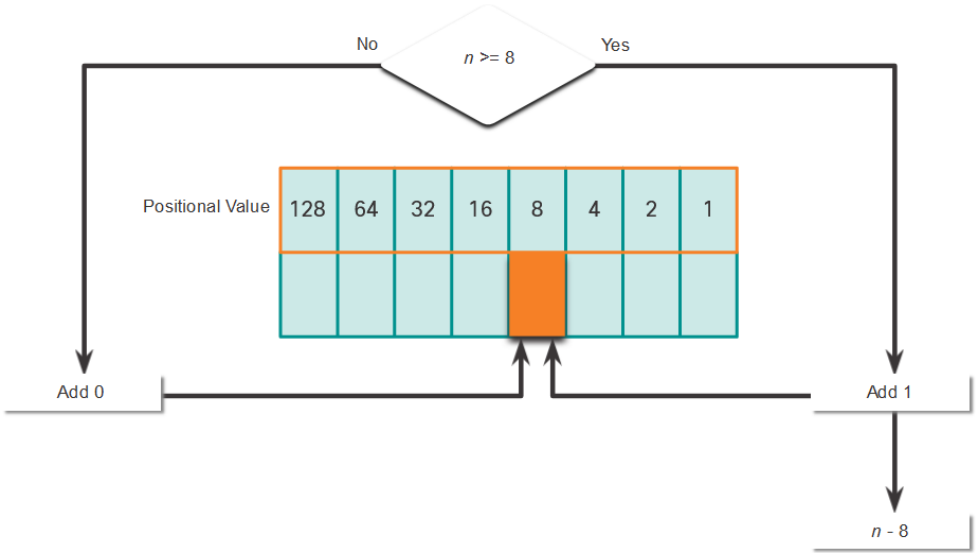
Dacă da, se adaugă un 1 binar în valoarea poziţională 16 şi se scade 16 din numărul zecimal.



Numărul zecimal al octetului (n) este egal sau mai mare decât următorul bit cel mai semnificativ (8)?

Dacă nu, atunci se introduce 0 binar în valoarea poziţională 8.

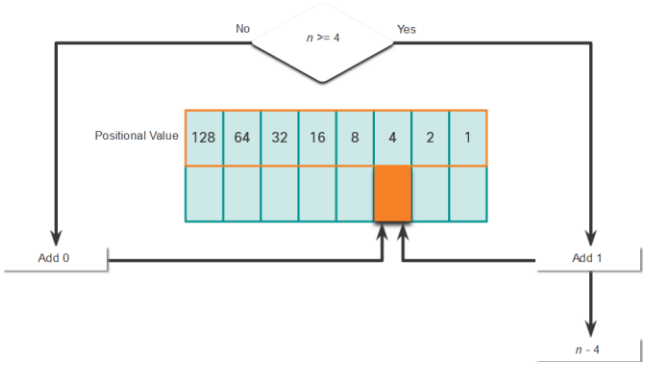
Dacă da, se adaugă un 1 binar în valoarea poziţională 8 şi se scade 8 din numărul zecimal.



Numărul zecimal al octetului (n) este egal sau mai mare decât următorul bit cel mai semnificativ (4)?

Dacă nu, atunci se introduce 0 binar în valoarea poziţională 4.

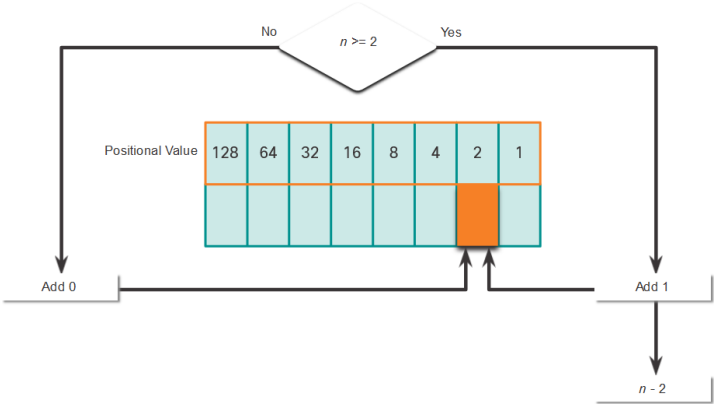
Dacă da, se adaugă un 1 binar în valoarea poziţională 4 şi se scade 4 din numărul zecimal.



Numărul zecimal al octetului (n) este egal sau mai mare decât următorul bit cel mai semnificativ (2)?

Dacă nu, atunci se introduce 0 binar în valoarea poziţională 2.

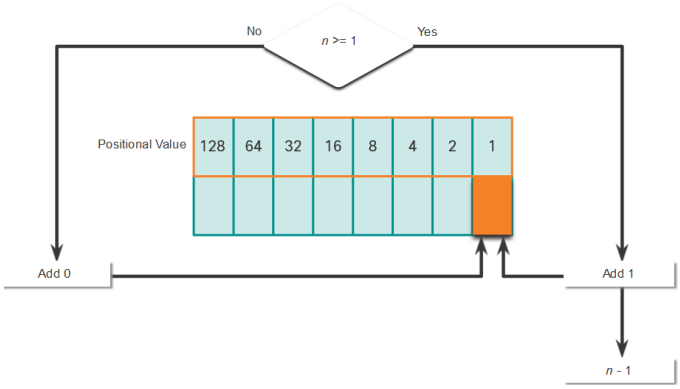
Dacă da, se adaugă un 1 binar în valoarea poziţională 2 şi se scade 2 din numărul zecimal.



Numărul zecimal al octetului (n) este egal sau mai mare decât următorul bit cel mai semnificativ (2)?

Dacă nu, atunci se introduce 0 binar în valoarea pozițională 1.

Dacă da, se adaugă un 1 binar în valoarea pozițională 1 și se scade 1 din numărul zecimal.



5.1.7 - Decimal to Binary Conversion Example

Pentru a ajuta la înțelegerea procesului, se ia în considerare adresa IP 192.168.10.11.

Primul număr octet 192 este convertit în binar utilizând procesul de notație pozițional explicat anterior.

Este posibil să fie ocolit procesul de scădere cu numere zecimale mai mici. De exemplu, se observa că este destul de ușor să se calculeze al treilea octet convertit într-un număr binar fără a trece efectiv prin procesul de scădere (8 + 2 = 10). Valoarea binară a celui de-al treilea octet este 00001010.

Al patrulea octet este 11 (8 + 2 + 1). Valoarea binară a celui de-al patrulea octet este 00001011.

Conversia între binar și zecimal poate părea dificilă la început, dar cu practică ar trebui să devină mai ușoară în timp.

5.1.8 - Activity - Decimal to Binary Conversions

Instrucțiuni - Această activitate permite exersarea conversiilor zecimale în valori binare de 8 biți. Recomandat estre să se lucreze cu acest instrument până când se poate face conversia fără erori. Sa se converteasca numărul zecimal afișat 173 Valoare zecimală în biții.

Decimal Value	173							
Base	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0
Position	128	64	32	16	8	4	2	1
Bit								

5.1.9 - Activity - Binary Game

Acesta este un mod distractiv de a învăța numerele binare pentru rețea.

Link joc: https://learningnetwork.cisco.com/docs/DOC-1803

Va trebui să se faca conexiunea la cisco.com pentru a utiliza acest link. Este necesar un cont dacă nu exista deja unul.

Există, de asemenea, o varietate de jocuri binare mobile gratuite. Sa se caute „joc binar” în magazinul de aplicații.

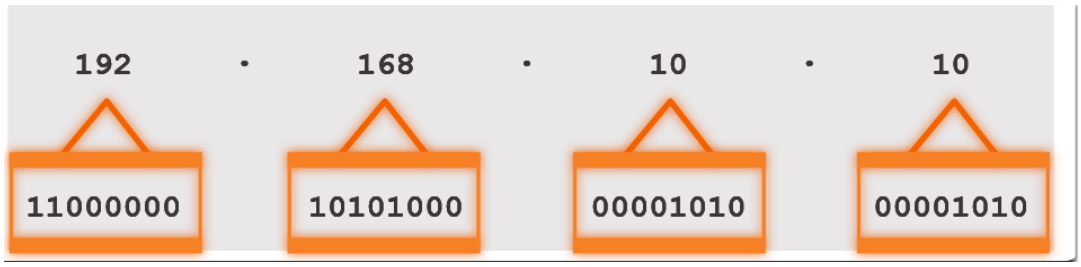
5.1.10 - IPv4 Addresses

După cum a fost menționat la începutul acestui capitol, routerele și computerele înțeleg doar binarul, în timp ce oamenii lucrează în numerotare zecimală. Este important să se realizeze o înțelegere aprofundată a acestor două sisteme de numerotare și a modului în care sunt utilizate în rețele.

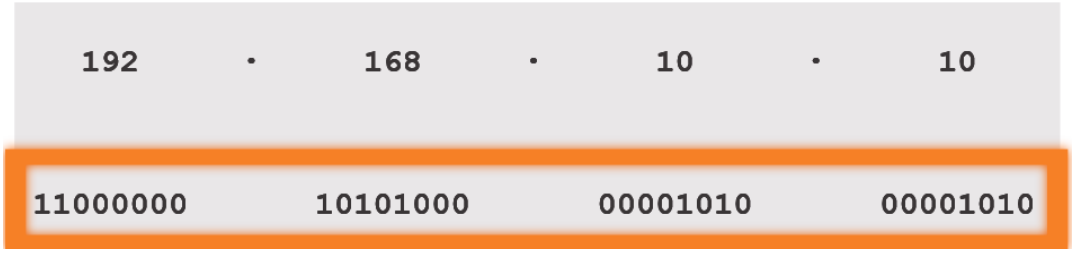
192.168.10.10 este o adresă IP care este atribuită unui computer.

192	.	168	.	10	.	10
11000000		10101000		00001010		00001010

Această adresă este formată din patru octeți diferiți.



Computerul stochează adresa ca întreg flux de date pe 32 de biți.



5.2 Hexadecimal Number System

5.2.1 - Hexadecimal and IPv6 Addresses

Conversia intre sistemele nu numeratie este o abilitate necesara pentru a înțelege adresa IPv4 în rețele de calculatoare. Dar este la fel de probabil să se utilizeze si adrese IPv6 în rețele. Pentru a înțelege adresele IPv6, trebuie să putem converti hexazecimal în zecimal și invers.

Așa cum zecimalul este un sistem numeric de bază zece, hexazecimalul este un sistem de bază șaisprezece. Sistemul numeric de bază șaisprezece folosește cifrele de la 0 la 9 și literele de la A la F. Figura arată valorile zecimale și hexazecimale echivalente pentru binarul de la 0000 la 1111.

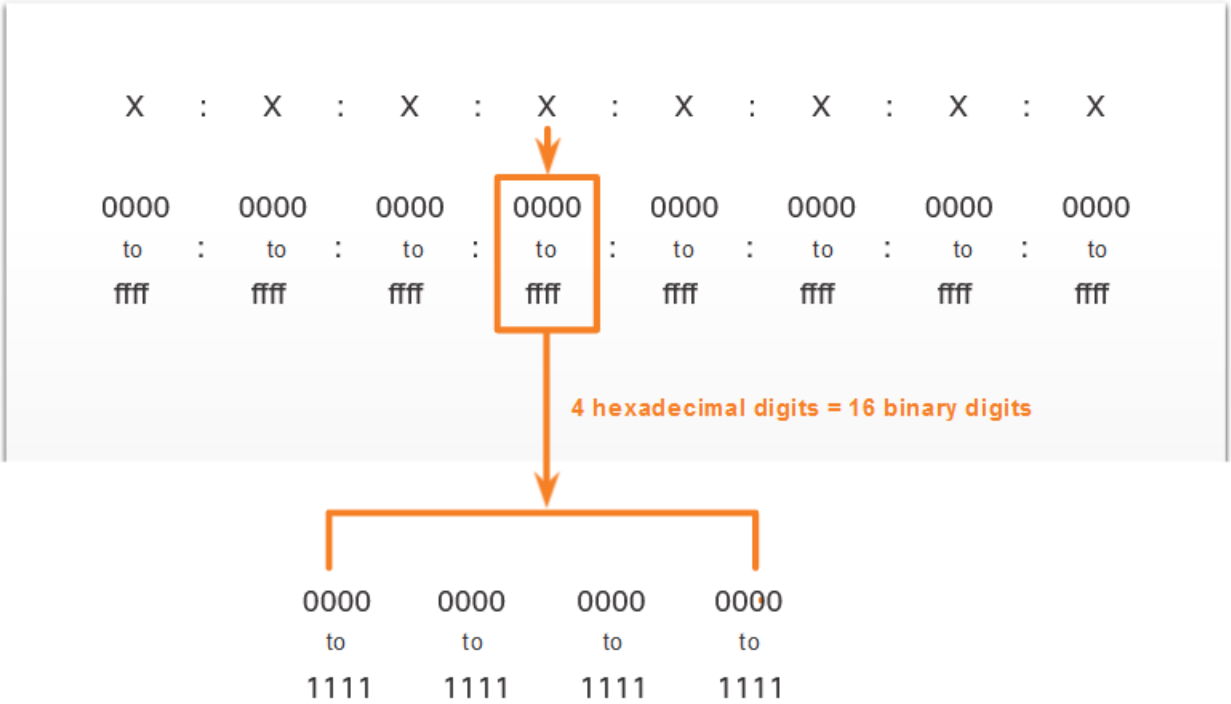
Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Binarul și hexazecimalul funcționează bine împreună, deoarece este mai ușor să se exprime o valoare ca o singură cifră hexazecimală decât ca patru biți binari.

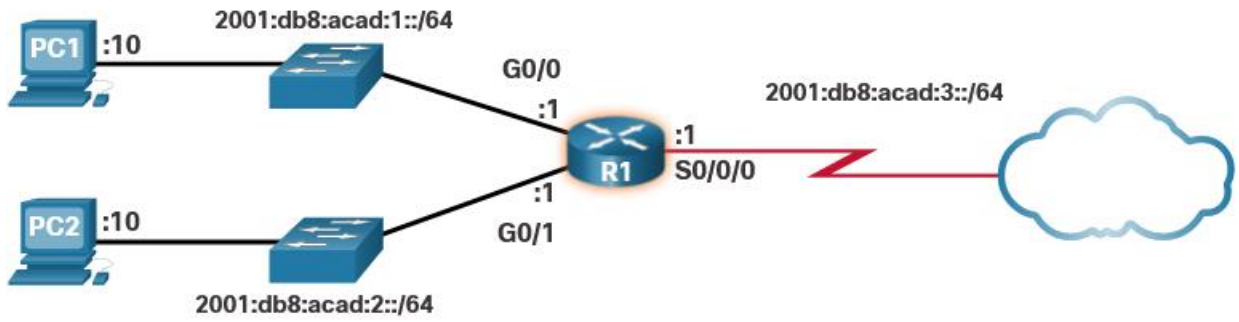
Sistemul de numerotare hexazecimală este utilizat în rețele pentru a reprezenta adrese IP versiunea 6 și adrese MAC Ethernet.

Adresele IPv6 au lungimea de 128 de biți și fiecare 4 biți este reprezentat de o singură cifră hexazecimală; pentru un total de 32 de valori hexazecimale. Adresele IPv6 nu țin cont de majuscule și pot fi scrise fie cu litere mici, fie cu majuscule.

După cum se arată în figură, formatul preferat pentru scrierea unei adrese IPv6 este x:x:x:x:x:x:x:x, fiecare „x” constând din patru valori hexazecimale. Când ne referim la 8 biți ai unei adrese IPv4, folosim termenul octet. În IPv6, un hextet este termenul neoficial folosit pentru a se referi la un segment de 16 biți sau patru valori hexazecimale. Fiecare „x” este un singur hextet, 16 biți sau patru cifre hexazecimale.



Exemplul de topologie din figură afișează adrese IPv6 hexazecimale.



5.2.3 - Decimal to Hexadecimal Conversions

Conversia numerelor zecimale în valori hexazecimale este simplă. De preferat sa se urmeze enumerați:

1. ***Conversia numărului zecimal în șiruri binare de 8 biți.***
2. ***Împărțirea șirurilor binare în grupuri de patru începând din poziția cea mai din dreapta.***
3. ***Convertirea pentru fiecare patru numere binare în cifra lor hexazecimală echivalentă.***

Exemplul oferă pașii pentru conversia numarului 168 în hexazecimal.

De exemplu, 168 s-a transformat în hexa utilizând procesul în trei pași.

1. ***168 în binar este 10101000.***
2. ***10101000 în două grupuri de patru cifre binare este 1010 și 1000.***
3. ***1010 este hex A și 1000 este hex 8.***

Răspuns: 168 este A8 în hexazecimal.

5.2.4 - Hexadecimal to Decimal Conversion

Conversia numerelor hexazecimale în valori zecimale este, de asemenea, simplă. Pașii enumerați reprezinta o buna practica:

A. ***Convertirea numărului hexazecimal în șiruri binare de 4 biți.***

B. ***Crearea unor grupari binare pe 8 biți începând din poziția cea mai din dreapta.***

C. ***Conversia fiecarei grupari binare de 8 biți în cifra lor zecimală echivalentă.***

Acest exemplu oferă pașii pentru conversia D2 în zecimală.

i. ***D2 în șiruri binare pe 4 biți este 1101 și 0010.***

ii. ***1101 și 0010 este 11010010 într-o grupare de 8 biți.***

iii. 11010010 în binar este echivalent cu 210 în zecimală.

Răspuns: D2 în hexazecimal este 210 în zecimal.

5.2.5 - Check Your Understanding - Hexadecimal Number System

1. Which is the hexadecimal equivalent of 202?

- B10
- BA
- C10
- CA

2. Which is the hexadecimal equivalent of 254?

- EA
- ED
- FA
- FE

3. Which is the decimal equivalent of A9?

- 168
- 169
- 170
- 171

5.3 SUMMARY

Sistemul de numere binare - Binar este un sistem de numerotare care constă din numerele 0 și 1 numite biți. În schimb, sistemul de numerotare zecimală constă din 10 cifre formate din numerele 0 – 9. Binarul este important de înțeles pentru că gazdele, serverele și dispozitivele de rețea folosesc adresare binară, în special adrese IPv4 binare, pentru a se identifica reciproc. Trebuie să cunoașteți adresarea binară și cum să convertiți între adrese IPv4 binare și zecimale punctate. Acest subiect a prezentat câteva modalități de a converti zecimal în binar și binar în zecimal.

Sistemul numeric hexazecimal - Așa cum zecimalul este un sistem numeric de bază zece, hexazecimalul este un sistem de bază șaisprezece. Sistemul de numere de bază șaisprezece folosește numerele de la 0 la 9 și literele de la A la F. Sistemul de numerotare hexazecimală este utilizat în rețele pentru a reprezenta adrese IPv6 și adrese MAC Ethernet. Adresele IPv6 au lungimea de 128 de biți și fiecare 4 biți este reprezentat de o singură cifră hexazecimală; pentru un total de 32 de valori hexazecimale. Pentru a converti hexazecimal în zecimal, trebuie mai întâi să convertiți hexazecimalul în binar, apoi convertiți binarul în zecimal. Pentru a converti zecimalul în hexazecimal, mai întâi trebuie să convertiți zecimalul în binar.

LABORATOR 6 . Adresele MAC ale Dispozitivelor de Rețea

Obiective

Partea 1: Se vor configura dispozitivele și se va verifica conectivitatea.

Partea 2: Se vor afișa, se vor descrie și se vor analiza adresele MAC Ethernet.

Instrucțiuni

Partea 1: Va fi făcută configurarea dispozitivelor și verificarea conectivității

În această parte, se va configura topologia rețelei și se vor configura setările de bază, cum ar fi adresele IP ale interfeței și numele dispozitivului. Pentru informații despre numele și adresa dispozitivului, se va consulta Tabelul de topologie și adrese.

Pasul 1: Se va conecta rețeaua așa cum se arată în topologie.

a. Se vor atașa dispozitivele prezentate în topologie și cablu, dacă este necesar.

b.Toate dispozitivele din topologie vor fi pornite.

Pasul 2: Se va configura adresa IPv4 pentru computer.

a. Se va configura adresa IPv4, masca de subrețea pentru PC-A.

b.Din promptul de comandă de pe PC-A, se dă ping la adresa comutatorului. Se va deschide un prompt de comandă Windows.

Întrebare:

Au avut succes ping-urile ? Explicație.

Răspunsuri aici.

Se va închide linia de comandă Windows

Pasul 3: Se vor configura setările de bază pentru comutator.

În acest pas, va fi configurat numele dispozitivului și adresa IP și va dezactiva căutarea DNS pe comutator.

a. Va fi conectată consola în comutator și se va intra în modul de configurare globală.

Switch> enable

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#

b. Va fi dezactivată căutarea DNS.

S1(config)# no ip domain-lookup

c. Se va atribui un nume de gazdă comutatorului pe baza tabelului de adrese.

Switch(config)# hostname S1

d. Va fi configurată și activată interfața SVI pentru VLAN 1.

S1(config)# interface vlan 1

S1(config-if)#description Legatura cu ramura 192.168.1.0/24

S1(config-if)# ip address 192.168.1.2 255.255.255.0

S1(config-if)# no shutdown

S1(config-if)# end

*Mar 1 00:07:59.048: %SYS-5-CONFIG_I: Configured from console by console

Pasul 4: Se va verifica conectivitatea la rețea.

Va fi deschis un prompt de comandă Windows. Se va da un ping la Switch de la PC-A.

Întrebare:

Au avut succes ping-urile ?

Partea 2: Se va afișa, se va descrie și se vor analiza adresele MAC Ethernet.

Fiecare dispozitiv dintr-o rețea LAN Ethernet are o adresă MAC care este atribuită de producător și stocată în firmware-ul NIC. Adresele MAC Ethernet au o lungime de 48 de biți. Acestea sunt afișate folosind șase seturi de cifre hexazecimale care sunt de obicei separate prin liniuțe, două puncte sau puncte. Următorul exemplu arată aceeași adresă MAC utilizând cele trei metode de notare diferite:

00-05-9A-3C-78-00 00:05:9A:3C:78:00 0005.9A3C.7800

Notă: Adresele MAC sunt numite și adrese fizice, adrese hardware sau adrese hardware Ethernet.

Se vor emite comenzi pentru a afișa adresele MAC pe un PC și pe un comutator și pentru a analiza proprietățile fiecăreia.

Pasul 1: Se va analiza adresa MAC pentru PC-A NIC.

Înainte de a analiza adresa MAC de pe PC-A, va fi analizat un exemplu de la un alt PC NIC. Se poate lansa comanda ***ipconfig /all*** pentru a vedea adresa MAC a unei NIC. Un exemplu de ieșire a ecranului este prezentat mai jos.

Când va fi folosită comanda ***ipconfig /all***, se va observa că adresele MAC sunt denumite adrese fizice.

Citind adresa MAC de la stânga la dreapta, primele șase cifre hexadecimale se referă la furnizorul (producătorul) acestui dispozitiv. Aceste prime șase cifre hexadecimale (3 octeți) sunt cunoscute și ca identificatorul unic organizațional (OUI). Acest cod de 3 octeți este atribuit furnizorului de către organizația IEEE.

Pentru a găsi producătorul, se vor utiliza cuvintele cheie Standarde IEEE OUI pentru a găsi un instrument de căutare OUI pe internet sau se va naviga la http://standards-oui.ieee.org/oui.txt pentru a găsi furnizorul OUI înregistrat. coduri. Ultimele șase cifre reprezintă numărul de serie al NIC alocat de producător.

a. Folosind ieșirea din comanda ipconfig /all, se va răspunde la următoarele întrebări.

```
C:\> ipconfig /all
<output omitted>
Ethernet adapter Ethernet:
 Connection-specific DNS Suffix . :
 Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit
Network Connection
 Physical Address. . . . . . . . . : 5C-26-0A-24-2A-60
 DHCP Enabled. . . . . . . . . . . : No
 Autoconfiguration Enabled . . . . : Yes
 Link-local IPv6 Address . . . . . :
fe80::b875:731b:3c7b:c0b1%10(Preferred)
 IPv4 Address. . . . . . . . . . . : 192.168.1.3 (Preferred)
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
<output omitted>
```

Care este porțiunea OUI a adresei MAC pentru acest dispozitiv?
Răspunsuri aici.
Care este porțiunea cu numărul de serie a adresei MAC pentru acest dispozitiv?
Răspunsuri aici.
Folosind exemplul de mai sus, va fi găsit numele vânzătorului care a fabricat acest NIC.
Răspunsuri aici.
b. *Din promptul de comandă de pe PC-A, se va lansa comanda* ***ipconfig /all*** *și se va identifica porțiunea OUI a adresei MAC pentru NIC-ul PC-A.*
Răspunsuri aici.
Va fi identificată porțiunea cu numărul de serie a adresei MAC pentru NIC-ul PC-A.
Se va identifica numele furnizorului care a fabricat NIC-ul PC-A.
Răspunsuri aici.
Pasul 2: Se va analiza adresa MAC pentru interfața S1 Fa 0/6. Se pot folosi o varietate de comenzi pentru a afișa adrese MAC pe comutator.
a. Se va conecta consola la S1 și se va folosi comanda ***show interfaces vlan 1*** pentru a găsi informațiile despre adresa MAC. O mostră este prezentată mai jos. Se va utiliza rezultatul generat de comutator pentru a răspunde la întrebări.

```
S1# show interfaces vlan 1
Vlan1 is up, line protocol is up
 Hardware is EtherSVI, address is 001b.0c6d.8f40 (bia 001b.0c6d.8f40)
 Internet address is 192.168.1.2/24
 MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive not supported
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output 00:14:51, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
```

```
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts (0 IP multicasts)
 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 34 packets output, 11119 bytes, 0 underruns
 0 output errors, 2 interface resets
 0 unknown protocol drops
 0 output buffer failures, 0 output buffers swapped out
```

Care este adresa MAC pentru VLAN 1 pe S1?

Răspunsuri aici.

Care este numărul de serie MAC pentru VLAN 1?

Răspunsuri aici.

Ce este OUI pentru VLAN 1?

Răspunsuri aici.

Pe baza acestui OUI, care este numele vânzătorului?

Răspunsuri aici.

Ce înseamnă BIA?

Răspunsuri aici.

De ce ieșirea arată aceeași adresă MAC de două ori?

b. O altă modalitate de a afișa adresa MAC pe comutator este să folosești comanda ***show arp***. Se va folosi comanda ***show arp*** pentru a afișa informații despre adresa MAC. Această comandă mapează adresa de Layer 2 cu adresa corespunzătoare de Layer 3. O mostră este prezentată mai jos. Se va utiliza rezultatul generat de comutator pentru a răspunde la întrebări.

```
S1# show arp

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.1.2 - 001b.0c6d.8f40 ARPA Vlan1

Internet 192.168.1.3 0 5c26.0a24.2a60 ARPA Vlan1
```

Ce adrese de nivel 2 sunt afișate pe S1?

Răspunsuri aici.

Ce adrese de nivel 3 sunt afișate pe S1?

Răspunsuri aici.

Pasul 3: Se vor vedea adresele MAC pe comutator.

Se va lansa comanda ***show mac address-table*** pe S1. O mostră este prezentată mai jos. Se va utiliza rezultatul generat de comutator pentru a răspunde la întrebări.

```
S1# show mac address-table
 Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
All 0100.0ccc.cccc STATIC CPU
All 0100.0ccc.cccd STATIC CPU
All 0180.c200.0000 STATIC CPU
All 0180.c200.0001 STATIC CPU
All 0180.c200.0002 STATIC CPU
All 0180.c200.0003 STATIC CPU
All 0180.c200.0004 STATIC CPU
All 0180.c200.0005 STATIC CPU
All 0180.c200.0006 STATIC CPU
All 0180.c200.0007 STATIC CPU
All 0180.c200.0008 STATIC CPU
All 0180.c200.0009 STATIC CPU
All 0180.c200.000a STATIC CPU
All 0180.c200.000b STATIC CPU
All 0180.c200.000c STATIC CPU
All 0180.c200.000d STATIC CPU
All 0180.c200.000e STATIC CPU
All 0180.c200.000f STATIC CPU
All 0180.c200.0010 STATIC CPU
All ffff.ffff.ffff STATIC CPU
 1 5c26.0a24.2a60 DYNAMIC Fa0/6
Total Mac Addresses for this criterion: 21
```

Comutatorul a afișat adresa MAC a PC-A? Dacă răspunsul este da, pe ce port era ?

EXERCIȚIUL 1. Tabel de adrese MAC pe Switch

Obiective

Partea 1: Se va construi și se va configura rețeaua.

Partea 2: Va fi examinat tabelul de adrese MAC al comutatorului.

Instrucțiuni

Partea 1: Se va construi și se va configura rețeaua

Pasul 1: Se va cabla rețeaua conform topologiei.

Pasul 2: Vor fi configurate gazde PC.

Pasul 3: Vor fi inițializate și reîncărcate comutatoarele după cum este necesar.

Pasul 4: Se vor configura setările de bază pentru fiecare comutator.

Va fi deschisă fereastra de configurare

a. Va fi configurat numele dispozitivului așa cum se arată în topologie.

b. Va fi configurată adresa IP așa cum este listată în Tabelul de adrese.

c. Vor fi atribuite parolele pe liniile console și vty.

d. Se va atribui o parolă pentru modul de lucru EXEC privilegiat.

Fereastra de configurare va fi închisă.

Partea 2: Va fi examinat tabelul de adrese MAC al comutatorului

Un comutator învață adrese MAC și construiește tabelul de adrese MAC, pe măsură ce dispozitivele de rețea inițiază comunicarea în rețea.

Pasul 1: Vor fi înregistrate adresele MAC ale dispozitivelor de rețea.

a. Se va deschide un prompt de comandă pe PC-A și PC-B și va fi tastată comanda ***ipconfig /all***.

Se va deschide promptul de comandă Windows.

Întrebare:

Care sunt adresele fizice ale adaptorului Ethernet?

Adresa MAC PC-A:

Răspunsuri aici.

Adresa MAC PC-B:

Răspunsuri aici.

b. Se va conecta consola la comutatoarele S1 și S2 și va fi tastată comanda show interface F0/1 pe fiecare comutator.

Se va deschide o fereastră de configurare.

Întrebări:

Pe a doua linie de ieșire de comandă, care sunt adresele hardware (sau adresa inscripționată [bia])?

S1 Fast Ethernet 0/1 Adresa MAC:

Răspunsuri aici.

Adresă MAC S2 Fast Ethernet 0/1:

Răspunsuri aici.

Se va închide o fereastră de configurare

Pasul 2: Se va afișa tabelul de adrese MAC ale comutatorului.

Se va conecta consola la comutatorul S2 și se va vedea tabelul de adrese MAC, atât înainte, cât și după rularea testelor de comunicare în rețea cu ping.

a. Se va stabili o conexiune la consolă la S2 și se va intra în modul EXEC privilegiat.

Se va deschide o fereastră de configurare

b. În modul EXEC privilegiat, se va tasta comanda ***show mac address-table*** și se va apăsa Enter.

S2# show mac address-table

Chiar dacă nu a fost inițiată nicio comunicare în rețea (adică, nu a fost folosit ping), este posibil ca Switch-ul să fi învățat adrese MAC din conexiunea sa la PC și celălalt Switch.

Întrebări:

Există adrese MAC înregistrate în tabelul de adrese MAC?

Răspunsuri aici.

Ce adrese MAC sunt înregistrate în tabel?

La ce porturi de comutare sunt mapate și cărora le aparțin dispozitivele?

Vor fi ignorate adresele MAC care sunt mapate la CPU.

Răspunsuri aici.

Dacă nu au fost înregistrate anterior adresele MAC ale dispozitivelor de rețea în Pasul 1, cum se va putea spune căror dispozitive aparțin adresele MAC, folosind doar rezultatul din comanda show mac address-table ?

Funcționează în toate scenariile ?

Pasul 3: Va fi șters tabelul de adrese MAC S2 și va fi afișat din nou tabelul de adrese MAC.

a. În modul EXEC privilegiat, se va tasta comanda dinamică ***clear mac address-table*** și se va apăsa Enter.

S2# clear mac address-table dynamic

b. Se va tasta rapid din nou comanda show mac address-table.

Întrebări:

Tabelul de adrese MAC conține adrese pentru VLAN 1? Există alte adrese MAC listate?

Răspunsuri aici.

Se va aștepta 10 secunde, se va tasta comanda show mac address-table și se va apăsa Enter. Există adrese noi în tabelul de adrese MAC?

Răspunsuri aici.

Fereastra de configurare va fi închisă.

Pasul 4: De la PC-B, se va da ping dispozitivelor din rețea și se va observa tabelul de adrese MAC ale comutatorului.

a. Din PC-B, se va deschide un prompt de comandă și se va tasta ***arp -a***.

Se va deschide un prompt de comandă.

Întrebare:

Fără a include adresele de multicast sau de difuzare, câte perechi de adrese IP-la-MAC de dispozitiv au fost învățate de ARP?

Răspunsuri aici.

b. Din promptul de comandă PC-B, se va da ping PC-A, S1 și S2.

Întrebare:

Toate dispozitivele au primit răspunsuri de succes? Dacă nu, va fi verificată cablarea și configurațiile IP.

Răspunsuri aici.

Va fi închis promptul de comandă.

c. De la o conexiune la consolă la S2, va fi introdus comanda ***show mac address-table***.

Se va deschide o fereastră de configurare.

Întrebare:

A adăugat comutatorul adrese MAC suplimentare la tabelul de adrese MAC? Dacă da, ce adrese și dispozitive?

Răspunsuri aici.

Se va închide o fereastră de configurare și se va deschide un prompt de comandă. De pe PC-B, se va deschide un prompt de comandă și se va tasta din nou ***arp -a***.

Întrebare:

Cache-ul PC-B ARP are intrări suplimentare pentru toate dispozitivele de rețea cărora li s-au trimis ping-uri?

EXERECIȚIUL 1. Examinrea tabelului ARP.

Device	Interface	MAC Address	Switch Interface
Router0	Gg0/0	0001.6458.2501	G0/1
	S0/0/0	N/A	N/A
Router1	G0/0	00E0.F7B1.8901	G0/1
	S0/0/0	N/A	N/A
10.10.10.2	Wireless	0060.2F84.4AB6	F0/2
10.10.10.3	Wireless	0060.4706.572B	F0/2
172.16.31.2	F0	000C.85CC.1DA7	F0/1
172.16.31.3	F0	0060.7036.2849	F0/2
172.16.31.4	G0	0002.1640.8D75	F0/3

Obiective

Partea 1: Va fi examinată o solicitare ARP.

Partea 2: Va fi examinat un tabel de adrese MAC pe Switch.

Partea 3: Va fi examinat procesul ARP în comunicațiile de la distanță.

Partea 1: Va fi examinată o solicitare ARP

Pasul 1: Se vor genera cereri ARP prin ping 172.16.31.3 de la 172.16.31.2.

Se va deschide un prompt de comandă.

a. Se va face clic pe 172.16.31.2 și se deschide linia de comandă.

b. Se va introduce comanda ***arp -d*** pentru a șterge tabelul ARP.

Se va închide un prompt de comandă.

c. Se va intra în modul Simulare și se va introduce comanda ***ping 172.16.31.3***. Vor fi generate două PDU-uri. Comanda ping nu poate finaliza pachetul ICMP fără a cunoaște adresa MAC a destinației. Deci computerul trimite un cadru de difuzare ARP pentru a găsi adresa MAC a destinației.

d. Se va face clic pe Captură/Redirecționare o dată. PDU-ul ARP mută Switch1 în timp ce PDU-ul ICMP dispare, așteptând răspunsul ARP. Va fi deschis PDU-ul și va înregistra adresa MAC de destinație.

Întrebare:

Această adresă este listată în tabelul de mai sus ?

e. Se va face clic pe Capture/Forward pentru a muta PDU-ul pe următorul dispozitiv.

Întrebare:

Câte copii ale PDU-ului a făcut Switch1?

Răspunsuri aici.

Care este adresa IP a dispozitivului care a acceptat PDU-ul?

Răspunsuri aici.

f. Se va deschide PDU și se va examina stratul 2.

Întrebare:

Ce sa întâmplat cu adresele MAC sursă și destinație?

Răspunsuri aici.

g. Se va face clic pe Captură/Redirecționare până când PDU-ul revine la 172.16.31.2.

Întrebare:

Câte copii ale PDU-ului a făcut schimbarea în timpul răspunsului ARP?

Răspunsuri aici.

Pasul 2: Va fi examinat tabelul ARP.

a. Se va observa că pachetul ICMP reapare. Va fi deschis PDU-ul și va fi examinat adresele MAC.

Întrebare:

Adresele MAC ale sursei și destinației se aliniază cu adresele lor IP?

Răspunsuri aici.

b. Se va comuta înapoi la în timp real și ping-ul se finalizează.

c. Se va face clic pe 172.16.31.2 și se va introduce comanda arp -a.

Întrebare:

Cărei adresă IP corespunde intrarea adresei MAC?

Răspunsuri aici.

În general, când un dispozitiv final emite o solicitare ARP?

Răspunsuri aici.

Partea 2: Va fi examinat un tabel de adrese MAC de comutare

Pasul 1: Se va genera trafic suplimentar pentru a popula tabelul cu adrese MAC ale comutatorului.

Se va deschide un prompt de comandă

a. Din 172.16.31.2, se va introduce comanda ping 172.16.31.4.

b. Se va face clic pe 10.10.10.2 și se va deschide Linia de comandă.

c. Se va introduce comanda ping 10.10.10.3.

Întrebare:

Câte răspunsuri au fost trimise și primite?

Răspunsuri aici.

Se va închide un prompt de comandă

Pasul 2: Va fi examinat tabelul de adrese MAC de pe comutatoare.

a. Se va face clic pe Switch1 și apoi pe fila CLI. Se va introduce comanda ***show mac-address-table***.

Întrebare:

Intrările corespund cu cele din tabelul de mai sus?

Răspunsuri aici.

b. Se va face clic pe Switch0, apoi pe fila CLI. Se va introduce comanda ***show mac-address-table***.

Întrebări:

Intrările corespund cu cele din tabelul de mai sus?

De ce două adrese MAC sunt asociate unui singur port?

Răspunsuri aici.

Partea 3: Va fi examinat procesul ARP în comunicațiile de la distanță

Pasul 1: Se va genera trafic pentru a produce trafic ARP.

Se va deschide un prompt de comandă

a. Se va face clic pe 172.16.31.2 și se deschide linia de comandă.

b. Se va introduce comanda ***ping 10.10.10.1***.

c. Va fi tastat ***arp -a***.

Întrebare:

Care este adresa IP a noii intrări de tabel ARP?

Răspunsuri aici.

d. Se va introduce ***arp -d*** pentru a șterge tabelul ARP și a trece la modul Simulare.

e. Se va repeta ping-ul la 10.10.10.1.

Întrebare:

Câte PDU-uri apar?

Răspunsuri aici.

Va fi închis promptul de comandă

f. Se va face clic pe Captură/Înainte. Se va face clic pe PDU care se află acum la Switch1.

Întrebare:

Care este adresa IP destinație țintă a cererii ARP?

Răspunsuri aici.

g. Adresa IP de destinație nu este 10.10.10.1.

Întrebare:

De ce?

Pasul 2: Va fi examinat tabelul ARP de pe Router1.

a. Se va comuta în modul în timp real. Se va face clic pe Router1 și apoi pe fila CLI prin consolă.

b. Se va intra în modul EXEC privilegiat și apoi în comanda ***show mac-address-table***.

Întrebare:

Câte adrese MAC sunt în tabel? De ce?

Răspunsuri aici.

c. Se va introduce comanda ***show arp***.

Întrebări:

Există o intrare pentru 172.16.31.2?

Răspunsuri aici.

Ce se întâmplă cu primul ping într-o situație în care routerul răspunde la cererea ARP?

EXERCIȚIUL 3. Descoperirea Vecinilor IPv6 - Neighbor Discovery

Obiective

Partea 1: Rețea locală IPv6 Neighbor Discovery

Partea 2: Rețeaua de la distanță IPv6 Neighbor Discovery

Instrucțiuni

Partea 1: Rețea locală IPv6 Neighbor Discovery

În această parte, se va obține adresa MAC a unui dispozitiv de destinație din aceeași rețea.

Pasul 1: Se va verifica routerul pentru orice vecini pe care i-a descoperit.

a. Se va face clic pe routerul RTA. Se va selecta fila CLI și se va lansa comanda ***show ipv6 neighbors*** din modul EXEC privilegiat. Dacă sunt afișate intrări, acestea vor fi eliminate folosind comanda ***clear ipv6 neighbors***.

b. Se va face clic pe PCA1, se va selecta fila Desktop și se va face clic pe pictograma Command Prompt.

Pasul 2: Se va trece la modul Simulare pentru a captura evenimente.

a. Se va face clic pe butonul Simulare din colțul din dreapta jos al ferestrei Packet Tracer Topology.

b. Se va face clic pe butonul Afișare tot/Niciunul din panoul de simulare până când Filtrele listei de evenimente – Evenimente vizibile afișează Nimic.

c. Se va face clic pe Editare filtre. Se va selecta fila IPv6 din partea de sus și se vor bifa casetele pentru ICMPv6 și NDP. Se va închide fereastra Editare filtre ACL. Acum, Filtrele listei de evenimente afișează ICMPv6 și NDP.

d. Din promptul de comandă de pe PCA1, se va lansa comanda ***ping –n 1 2001:db8:acad:1::b***. Aceasta va începe procesul de ping PCA2.

e. Se va face clic pe Play (Hands Free) în PLAY CONTROLS din afara panoului de simulare. Dacă se solicită, se va face clic pe View Previous Events în fereastra Buffer Full - Packet Tracer. Ar trebui să aibă aproximativ 12 intrări în fereastră.

Întrebare:

De ce sunt prezente PDU-urile ND?

Răspunsuri aici.

f. Se va face clic pe pătratul din coloana Tip pentru primul eveniment, care ar trebui să fie ICMPv6.

Întrebare:

Deoarece mesajul începe cu acest eveniment, există doar o PDU de ieșire. În fila Model OSI, care este tipul de mesaj listat pentru ICMPv6?

Răspunsuri aici.

Se va observa că nu există o adresare Layer 2. Se va face clic pe butonul Următorul strat >> pentru a obține o explicație despre procesul ND (Neighbor Discovery).

g. Se va face clic pe pătratul de lângă următorul eveniment din panoul de simulare. Ar trebui să fie la dispozitivul PCA1 și tipul ar trebui să fie NDP.

Întrebări:

Ce s-a schimbat în adresarea Layer 3?

Răspunsuri aici.

Ce adrese de nivel 2 sunt afișate?

Răspunsuri aici.

Când o gazdă nu cunoaște adresa MAC a destinației, o adresă MAC specială multicast este utilizată de IPv6 Neighbor Discovery ca adresă de destinație Layer 2.

h. Se va naviga înapoi la Lista de evenimente. Va fi selectat primul eveniment NDP la SwitchA.

Întrebare:

Există vreo diferență între straturile de intrare și straturile de ieșire pentru stratul 2?

Răspunsuri aici.

i. Va fi selectat primul eveniment NDP la PCA2. Se va face clic pe Detalii PDU de ieșire.

Întrebare:

Ce adrese sunt afișate pentru următoarele?

Notă: Adresele din câmpuri pot fi împachetate. Se va ajusta dimensiunea ferestrei PDU pentru a face informațiile despre adrese mai ușor de citit.

ADDR DEST Ethernet II:

Răspunsuri aici.

ADDR SRC Ethernet II:

Răspunsuri aici.

IP SRC IPv6:

Răspunsuri aici.

IPv6 DST IP:

Răspunsuri aici.

Întrebare:

j. *Va fi selectat primul eveniment NDP la RTA. De ce nu există straturi de afară*?

Răspunsuri aici.

k. Se va face clic pe butonul Următorul strat >> până la sfârșit și se va citi pașii de la 4 la 7 pentru explicații suplimentare.

l. Se va face clic pe următorul eveniment ICMPv6 la PCA1.

Întrebare:

PCA1 are acum toate informațiile necesare pentru a comunica cu PCA2?

m. Se va face clic pe ultimul eveniment ICMPv6 la PCA1. Se va observa că aceasta este ultima comunicare listată.

Întrebare:

Care este tipul de mesaj Echo ICMPv6?

Răspunsuri aici.

n. Se va face clic pe butonul Resetare simulare din panoul de simulare. Din promptul de comandă al PCA1, se va repeta ping-ul către PCA2. (Sugestie: ar trebui să se poată apăsa săgeata în sus pentru a readuce comanda anterioară.)

o. Se va face clic pe Play (Hands Free) pentru a finaliza procesul de ping. Se va face clic pe Vizualizare evenimente anterioare dacă se solicită.

Întrebare:

De ce nu au existat evenimente NPD?

Răspunsuri aici.

Partea 2: Rețeaua de la distanță IPv6 Neighbor Discovery

În partea 2 a acestei activități, se vor efectua pași similari cu cei din partea anterioară, cu excepția cazului în care gazda

destinație se află pe o altă rețea LAN. Se va observa cum diferă procesul Neighbor Discovery de procesul observat în partea anterioară. Se va acorda o atenție deosebită unora dintre pașii suplimentari de adresare care au loc atunci când un dispozitiv comunică cu un dispozitiv care se află într-o altă rețea.

Pasul 1: Vor fi evenimente capturate pentru comunicarea de la distanță.

a. Se va face clic pe butonul Reset Simulation pentru a șterge evenimentele anterioare. Va fi afișată și ștersă orice intrare din tabelul dispozitivului vecin IPv6, așa cum s-a făcut în partea anterioară.

b. Se va verifica că numai ICMPv6 și NDP sunt listate în Filtrele listei de evenimente - Evenimente vizibile.

c. Din promptul de comandă de pe PCA1, se va lansa comanda ***ping -n 1 2001:db8:acad:2::a*** pentru gazda PCB1.

d. Se va face clic pe Play (Hands Free) în PLAY CONTROLS din afara panoului de simulare. Dacă se solicită, se va face clic pe View Previous Events în fereastra Buffer Full -- Packet Tracer.

e. Când procesul de ping se termină, se va face clic pe pătratul din coloana Tip pentru primul eveniment, care ar trebui să fie ICMPv6. Deoarece mesajul începe cu acest eveniment, există doar un PDU de ieșire. Se va observa că îi lipsesc informațiile de nivel 2, așa cum a fost în scenariul anterior.

f. Se va face clic pe primul eveniment NDP la dispozitivul PCA1.

Întrebare:

Ce adresă este utilizată pentru IP-ul Src în PDU-ul de intrare?

Răspunsuri aici.

IPv6 Neighbor Discovery va determina următoarea destinație pentru a redirecționa mesajul ICMPv6.

g. Se va face clic pe al doilea eveniment ICMPv6 pentru PCA1. PCA1 are acum suficiente informații pentru a crea o solicitare de eco ICMPv6.

Întrebare:

Ce adresă MAC este utilizată pentru MAC-ul de destinație?

Răspunsuri aici.

h. Se va face clic pe următorul eveniment ICMPv6 la RTA dispozitiv. Se va observa că PDU-ului de ieșire de la RTA îi lipsește adresa de destinație Layer 2, ceea ce înseamnă că RTA trebuie să efectueze încă o dată o descoperire a vecinilor pentru interfața care are rețeaua 2001:db8:acad:2:: deoarece nu cunoaște Adresele MAC ale dispozitivelor de pe LAN G0/0/1.

i. Se va trece la primul eveniment ICMPv6 pentru dispozitivul PCB1.

Întrebare:

Ce lipsește din informațiile de ieșire de Stratul 2?

j. Următoarele câteva evenimente NDP asociază adresele IPv6 rămase cu adrese MAC. Evenimentele NDP anterioare au asociat adrese MAC cu adrese Link Local.

k. Se va trece la ultimul set de evenimente ICMPv6 și se va observa că toate adresele au fost învățate. Informațiile necesare sunt acum cunoscute, astfel încât PCB1 poate trimite mesaje de răspuns ecou către PCA1.

l. Se va face clic pe butonul Resetare simulare din panoul de simulare. Din promptul de comandă al PCA1 se va repeta comanda pentru a executa ping PCB1.

m. Se va face clic pe Play (Hands Free) pentru a finaliza procesul de ping. Se va face clic pe Vizualizare evenimente anterioare dacă se solicită în fereastra Buffer Full.

Întrebare:

Au existat evenimente NPD?

Răspunsuri aici.

n. Se va face clic pe singurul eveniment PCB1 din noua listă.

Întrebări:

Cu ce corespunde adresa MAC de destinație?

Răspunsuri aici.

De ce PCB1 folosește adresa MAC a interfeței routerului pentru a-și face PDU-urile ICMP?

Răspunsuri aici.

Pasul 2: Se va examina ieșirile routerului.

a. Se va reveni la modul în timp real.

b. Se va face clic pe RTA și se selectează fila CLI. La promptul routerului va fi introdusă comanda ***show ipv6 neighbors***.

Întrebări:

Câte adrese sunt enumerate?

Răspunsuri aici.

Cu ce dispozitive sunt asociate aceste adrese?

Răspunsuri aici.

Există înregistrări pentru PCA2 listate? Explicație.

Răspunsuri aici.

c. Ping PCA2 de la router.

d. Se va lansa comanda ***show ipv6 neighbors***.

Întrebare:

Există intrări pentru PCA2?

LABORATOR 7. Configurare de Bază

EXERCITIUL 1. Configurare de Bază a Dispozitivelor

Obiective

Partea 1. Completarea documentației de rețea. Efectuarea configurațiilor de bază ale dispozitivelor: un Host, un Switch și un Router. Verificarea conectivității și depanarea oricăror probleme.

Tabel de Adrese

Device	Interface	IP Address	Default Gateway
	GIGA 0/0		N/A
	GIGA 0/1		N/A
		VLAN 1	
		VLAN 1	
	NIC		
	NIC		
	NIC		
	NIC		

Cerințe

Informațiile lipsă vor fi introduse în tabelul de adrese.

Se va da numele tuturor dispozitivelor.

Se vor folosi parole așa cum au fost alocate în laboratoare pentru toate liniile.

Vor fi criptate toate parolele text simplu.

Se vor configura bannere adecvate pentru modul motd și login.

Se va configura adresarea IPv4 și IPv6 pentru dispozitive conform cunoștințelor.

Se vor documenta interfețele cu descrieri, inclusiv interfața VLAN 1.

Se vor salva configurațiile.

Se va verifica conectivitatea între toate dispozitivele. Toate dispozitivele ar trebui să poată trimite ping la toate celelalte dispozitive cu IPv4 și IPv6.

Se va face depanarea și documentarea oricăror probleme.

Se vor implementa soluțiile necesare pentru a activa și a verifica conectivitatea completă end-to-end.

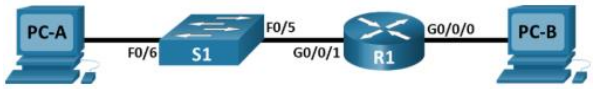
EXERCITIUL 2. Configurarea unei Retele LAN cu un Switch si un Router

Obiective

Partea 1: Topologia de configurat.

Partea 2: Dispozitivele configurate și verificată conectivitatea.

Partea 3: Afișarea informațiilor despre dispositive.



Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/0	192.168.0.1 /24	N/A
		2001:db8:acad::1/64	
		fe80::1	
	G0/0/1	192.168.1.1 /24	N/A
		2001:db8:acad:1::1/64	
		fe80::1	
S1	VLAN 1	192.168.1.2/24	192.168.1.1
PC-A	NIC	192.168.1.12/24	192.168.1.1
		2001:db8:acad:1::1/64	fe80::1
PC-B	NIC	192.168.0.12/24	192.168.0.1
		2001:db8:acad::3/64	fe80::1

Instrucțiuni

Partea 1: Configurarea topologiei

a. Se va muta ruterul și comutatorul necesar, de la Raft în Rack.

b. Se vor muta PC-urile necesare de la Raft la Masă.

c. Dispozitivele vor fi conectate, așa cum se arată în Topologie și Tabelul de Adresări.

d. Vor fi alimentate itoate dispozitivele.

Partea 2: Se vor configura dispozitivele și se va verifica conectivitatea. În această parte, se va configura topologia rețelei și se vor configura setările de bază, cum ar fi adresele IP ale interfeței, accesul la dispozitiv și parolele. Se va consulta Topologia și Tabelul de Adresări de la începutul acestei activități pentru numele dispozitivelor și informații despre adrese.

Pasul 1: Se va atribui IP static, cu informații către interfețele PC-ului.

a. Pe PC-A, vor fi configurate adresa IP, masca de subrețea și setările implicite ale gateway-ului.

b. Pe PC-B, vor fi configurate adresa IP, masca de subrețea și setările implicite ale gateway-ului.

c. Dintr-o fereastră de prompt de comandă de pe PC-A, se va da ping la PC-B.

Întrebare:*De ce nu au avut succes ping-urile?*

Pasul 2: La acest pas va fi configurat routerul.

a. Va fi configurat cablul consolei în router și va fi activat modul EXEC privilegiat.

Va fi deschisă fereastra de configurare

b. Se va intra în modul de configurare.

c. Va fi atribuit numele dispozitivului routerului.

d. Vor fi atribuite parole în același mod în care lucrăm în laborator pentru modul EXEC privilegiat.

e. Se va atribui parola în același mod în care lucrăm în laborator pentru linia de consolă și va fi activată autentificarea.

f. Se va atribui parola în același mod în care lucrăm în laborator pentru liniile vty și se va activa autentificarea.

g. Vor fi criptate parolele din text simplu.

h. Se va crea un banner care avertizează pe oricine care accesează dispozitivul că accesul neautorizat este interzis.

i. Vor fi configurate și activate ambele interfețe gigabitethernet pe router.

j. Se va configura o descriere a interfeței pentru fiecare interfață, indicând ce dispozitiv este conectat la aceasta.

k. Pentru a activa rutarea IPv6, va fi introdusă comanda ***IPv6 unicast-routing***.

l. Se va salva configurația care rulează în fișierul de configurare de pornire.

m. Va fi setat ceasul pe router.

Fereastra de configurare va fi închisă.

n. Dintr-o fereastră de prompt de comandă de pe PC-A, se va da ping la PC-B.

Întrebare: *Au avut succes ping-urile?* Explicație.

Pasul 3: La acest pas va fi configurat Switch-ul, ceea ce înseamnă că va fi configurat numele de gazdă, interfața VLAN 1 și gateway-ul implicit.

Va fi deschisă fereastra de configurare.

a. Va fi configurat cablul consolei în Switch și va fi activat modul EXEC privilegiat.

b. Se va intra în modul de configurare.

c. Se va atribui un nume de dispozitiv comutatorului.

d. Va fi configurată și activată interfața VLAN pe comutatorul S1.

e. Se va configura gateway-ul implicit pentru comutatorul S1.

f. Se va salva configurația care rulează în fișierul de configurare de pornire.

Pasul 4: Se va verifica conectivitatea de la capăt la capăt.

a. De la PC-A, se va da ping la PC-B.

b. De la S1, se va da ping la PC-B.

Toate ping-urile trebuie să aibă succes.

Fereastra de configurare va fi închisă.

Partea 3: Se vor afișa informații despre dispozitiv. În partea 3, se vor folosi comenzile ***show*** pentru a prelua informații despre interfață și rutare de la router și comutator.

Pasul 1. Va fi afișat tabelul de rutare pe router.

a. Se va folosi comanda ***show ip route*** de pe R1 pentru a răspunde la următoarele întrebări.

Se va deschide fereastra de configurare.

Întrebări:

Ce cod este folosit în tabelul de rutare pentru a indica o rețea conectată direct?

Câte intrări de rutare sunt codificate cu un cod C în tabelul de rutare?

Ce tipuri de interfețe sunt asociate rutelor codificate C?

b. Se va folosi comanda ***show ipv6 route*** pe R1 pentru a afișa rutele IPv6.

Pasul 2: Vor fi afișate informații despre interfețe pe R1.

a. Se va folosi comanda ***show interface g0/0/1*** pentru a răspunde la următoarele întrebări.

Întrebări:

Care este starea operațională a interfeței G0/0/1?

Care este adresa Media Access Control (MAC) a interfeței G0/1?

Cum este afișată adresa de internet în această comandă?

b. Pentru informațiile IPv6, va fi introdusă comanda ***show ipv6 interface***.

Pasul 3: Va fi afișată o listă rezumată a interfețelor de pe router și comutator.

Există mai multe comenzi care pot fi folosite pentru a verifica configurația unei interfețe. Una dintre cele mai utile este comanda ***show ip interface brief***. Ieșirea comenzii afișează o listă rezumată a interfețelor de pe dispozitiv și oferă feedback imediat despre starea fiecărei interfețe.

a. Va fi introdusă comanda ***show ip interface brief*** pe R1.

R1# show ip interface brief

b. Se va introduce comanda ***show ipv6 interface brief*** pe R1 pentru a vedea informațiile despre interfața IPv6.

R1# show ipv6 interface brief

Fereastra de configurare va fi închisă.

c. Va fi introdusă comanda ***show ip interface brief*** pe S1.

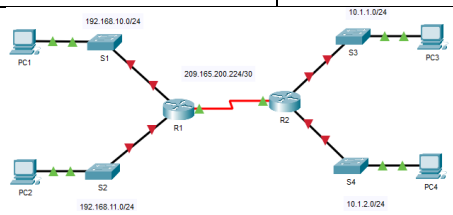
Va fi deschisă fereastra de configurare

S1# show ip interface brief

EXERCITIUL 3. Conectarea unui Router la un LAN

Tabel de Adresare

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	209.165.200.225	255.255.255.252	N/A
R2	G0/0	10.1.1.1	255.255.255.0	N/A
	G0/1	10.1.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.226	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1



Obiective

Partea 1: Se vor afișa informații despre router.

Partea 2: Se vor configura interfețele routerului.

Partea 3: Se va verifica configurația.

Partea 1: Se vor afișa informații despre router

Pasul 1: Vor fi afișate informații despre interfață pe R1.

Notă: Se va face clic pe un dispozitiv și apoi pe fila CLI pentru a accesa direct linia de comandă. Parola consolei este Cisco. Parola EXEC privilegiată este clasa.

Întrebări:

a. *Ce comandă afișează statisticile pentru toate interfețele configurate pe un router?*

b. Ce comandă afișează doar informațiile despre interfața Serial 0/0/0?

c. Se va introduce comanda pentru a afișa statisticile pentru interfața Serial 0/0/0 pe R1 și va răspunde la următoarele întrebări:

1) Care este adresa IP configurată pe R1?

2) Care este lățimea de bandă pe interfața Serial 0/0/0?

d. Se va introduce comanda pentru a afișa statisticile pentru interfața GigabitEthernet 0/0 și va răspunde la următoarele întrebări:

1) Care este adresa IP pe R1?

2) Care este adresa MAC a interfeței GigabitEthernet 0/0?

3) Care este lățimea de bandă (BW) a interfeței GigabitEthernet 0/0?

Pasul 2: Se va afișa o listă rezumată a interfețelor de pe R1.

Întrebări:

a. *Care comandă afișează un scurt rezumat al interfețelor curente, al stării interfeței și al adreselor IP care le sunt atribuite?*

b. Se va introduce comanda pe fiecare router și se va răspunde la următoarele întrebări:

1) Câte interfețe seriale există pe R1 și R2?

2) Câte interfețe Ethernet există pe R1 și R2?

3) Sunt toate interfețele Ethernet de pe R1 la fel? Dacă nu, să se explice diferența (diferențele).

Pasul 3: Se va afișat tabelul de rutare pe R1.

Întrebări:

a. Ce comandă afișează conținutul tabelului de rutare?

b. Se va introduce comanda pe R1 și se va răspunde la următoarele întrebări:

1) Câte rute conectate există (folosește codul C)?

2) Ce traseu este listat?

3) Cum gestionează un router un pachet destinat unei rețele care nu este listată în tabelul de rutare?

Partea 2: Se vor configura interfețele routerului

Pasul 1: Se va configura interfața GigabitEthernet 0/0 pe R1.

a. Se vor introduce următoarele comenzi pentru a adresa și a activa interfața GigabitEthernet 0/0 pe R1:

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

b. Este o practică bună să fie configurată o descriere pentru fiecare interfață pentru a ajuta la documentarea rețelei. Se va configura o descriere a interfeței care indică dispozitivul la care este conectat.

```
R1(config-if)# description LAN connection to S1
```

c. De la R1 ar trebui să se poată da acum ping la PC1.

```
R1(config-if)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# ping 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/8 ms
```

Pasul 2: La acest pas vor fi configurate interfețele Gigabit Ethernet rămase pe R1 și R2.

a. Se vor folosi informațiile din tabelul de adrese pentru a finaliza configurațiile interfeței pentru R1 și R2. Pentru fiecare interfață, se procedează în felul următor:

1) Se va introduce adresa IP și se va activa interfața.

2) Se va configura o descriere adecvată.

b. Se vor verifica configurațiile interfeței.

Pasul 3: Se va face backup pentru configurații în NVRAM.

Întrebare:

Salvați fișierele de configurare de pe ambele routere în NVRAM. Ce comanda este folosită ?

Fereastra de configurare va fi închisă.

Partea 3: Se va verifica configurația

Pasul 1: Se vor folosi comenzi de verificare pentru a verifica configurațiile interfeței.

a. Se va utiliza comanda ***show ip interface brief*** atât pe R1, cât și pe R2 pentru a verifica rapid dacă interfețele sunt configurate cu adresa IP corectă și sunt active.

Întrebări:

Câte interfețe de pe R1 și R2 sunt configurate cu adrese IP și în starea „up” și „up”?

Ce parte a configurației interfeței NU este afișată în ieșirea comenzii?

Ce comenzi se pot folosi pentru a verifica această parte a configurației?

b. Se va utiliza comanda ***show ip route*** atât pe R1, cât și pe R2 pentru a vizualiza tabelele de rutare curente și pentru a răspunde la următoarele întrebări:

1) Câte rute conectate (folosesc codul C) vor vedea pe fiecare router?

2) Câte rute OSPF (folosesc codul O) vor vedea pe fiecare router?

3) Dacă routerul cunoaște toate rutele din rețea, atunci numărul de rute conectate și de rute învățate dinamic (OSPF) ar trebui să fie egal cu numărul total de rețele LAN și WAN. Câte rețele LAN și WAN sunt în topologie?

4) Acest număr se potrivește cu numărul de rute C și O afișate în tabelul de rutare?

Notă: Dacă răspunsul este „nu”, atunci lipsește o configurație necesară. Se vor revizui pașii din partea 2.

Pasul 2: Se va testată conectivitatea end-to-end în rețea.

Ar trebui acum să se poată face ping de pe orice computer pe orice alt computer din rețea. În plus, ar trebui să se poată face ping la interfețele active de pe routere. De exemplu, următoarele teste ar trebui să aibă succes:

Din linia de comandă de pe PC1, se va da ping la PC4.

Din linia de comandă de pe R2, se va da ping la PC2.

EXERCITIUL 4. Verificarea aAdresarii IPv4 și IPv6.

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
		IPv6 Address/Prefix		
R1	G0/0	10.10.1.97	255.255.255.224	N/A
		2001:DB8:1:1::1/64		N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:DB8:1:2::2/64		N/A
	Link-local	FE80::1		N/A
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:DB8:1:2::1/64		N/A
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:DB8:1:3::1/64		N/A
	Link-local	FE80::2		N/A
R3	G0/0	10.10.1.17	255.255.255.240	N/A
		2001:DB8:1:4::1/64		N/A
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:DB8:1:3::2/64		N/A
	Link-local	FE80::3		N/A
PC1	NIC			
PC2	NIC			

Obiective

Partea 1: Se va completa documentația tabelului de adrese.

Partea 2: Conectivitate va fi testată folosind Ping.

Partea 3: Ruta va fi descoperită urmărind traseul.

Partea 1: Se va completa documentația tabelului de adrese.

Pasul 1: Se va folosi ipconfig pentru a verifica adresa IPv4.

a. Se va face clic pe PC1 și pe fila Desktop > Prompt de comandă.

b. Se va introduce comanda ***ipconfig /all*** pentru a colecta informațiile IPv4. Va fi completat Tabelul de adrese cu adresa IPv4, masca de subrețea și gateway-ul implicit.

c. Se va face clic pe PC2 și pe fila Desktop > Linie de comandă.

d. Se va introduce comanda ***ipconfig /all*** pentru a colecta informațiile IPv4. Va fi completat Tabelul de adrese cu adresa IPv4, masca de subrețea și gateway-ul implicit.

Pasul 2: Se va folosi ***ipv6config*** pentru a verifica adresa IPv6.

a. Pe PC1, va fi introdusă comanda ***ipv6config /all*** pentru a colecta informațiile IPv6. Se va completa Tabelul de adrese cu adresa IPv6, prefixul de subrețea și gateway-ul implicit.

b. Pe PC2, va fi introdusă comanda ***ipv6config /all*** pentru a colecta informațiile IPv6. Se va completa Tabelul de adrese cu adresa IPv6, prefixul de subrețea și gateway-ul implicit.

Partea 2: Conectivitate va fi testată folosind Ping.

Pasul 1: Se va folosi ping pentru a verifica conectivitatea IPv4.

a. De la PC1, se va da ping la adresa IPv4 pentru PC2. Rezultatul a fost cu succes?

b. De la PC2, se va da ping la adresa IPv4 pentru PC1. Rezultatul a fost cu succes?

Pasul 2: Se va folosi ping pentru a verifica conectivitatea IPv6.

a. De la PC1, se va da ping la adresa IPv6 pentru PC2. Rezultatul a fost cu succes?

b. De la PC2, se va da ping la adresa IPv6 a PC1. Rezultatul a fost cu succes?

Partea 3: Se va descoperi Ruta urmărind traseul.

Pasul 1: Se va folosi Tracert pentru a descoperi calea IPv4.

a. De la PC1, se va urmări traseul către PC2.

PC> **tracert 10.10.1.20**

Ce adrese au fost întâlnite de-a lungul căii?

Cu ce interfețe sunt asociate cele patru adrese?

b. De la PC2, se va urmări traseul către PC1.

Ce adrese au fost întâlnite de-a lungul căii?

Cu ce interfețe sunt asociate cele patru adrese?

Pasul 2: Se va folosi Tracert pentru a descoperi calea IPv6.

a. De la PC1, va fi urmărită ruta către adresa IPv6 pentru PC2.

PC> **tracert 2001:DB8:1:4::A**

Ce adrese au fost întâlnite de-a lungul căii?

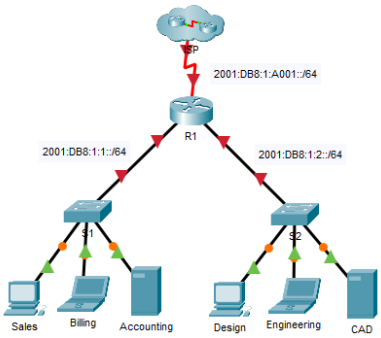
Cu ce interfețe sunt asociate cele patru adrese?

b. De la PC2, va fi urmărită ruta către adresa IPv6 pentru PC1.

Ce adrese au fost întâlnite de-a lungul căii?

Cu ce interfețe sunt asociate cele patru adrese?

EXERCITIUL 5. Configurarea adresei IPv6.



Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	G0/0	2001:DB8:1:1::1/64	N/A
	G0/1	2001:DB8:1:2::1/64	N/A
	S0/0/0	2001:DB8:1:A001::2/64	N/A
	Link-local	FE80::1	N/A
Sales	NIC	2001:DB8:1:1::2/64	FE80::1
Billing	NIC	2001:DB8:1:1::3/64	FE80::1
Accounting	NIC	2001:DB8:1:1::4/64	FE80::1
Design	NIC	2001:DB8:1:2::2/64	FE80::1
Engineering	NIC	2001:DB8:1:2::3/64	FE80::1
CAD	NIC	2001:DB8:1:2::4/64	FE80::1

Obiective

Partea 1: Se va configura adresa IPv6 pe router.

Partea 2: Se va configura adresa IPv6 pe servere.

Partea 3: Se va configura adresarea IPv6 la clienți.

Partea 4: Se va testa și se va verifica conexiunea la rețea.

Partea 1: Se va configura adresa IPv6 pe router.

Pasul 1: Routerul va fi activat să transmită pachete IPv6.

a. Va fi introdusă comanda de configurare globală ***ipv6 unicast-routing***. Această comandă trebuie configurată pentru a permite routerului să redirecționeze pachete IPv6.

R1(config)# **ipv6 unicast-routing**

Pasul 2: Se va configura adresa IPv6 pe GigabitEthernet0/0.

a. Se va face clic pe R1 și apoi pe fila CLI. Se va apăsa Enter.

b. Se va intra în modul EXEC privilegiat.

c. Se vor introduce comenzile necesare pentru a trece la modul de configurare a interfeței pentru GigabitEthernet0/0.

d. Se va configura adresa IPv6 cu următoarea comandă:

R1(config-if)# **ipv6 address 2001:DB8:1:1::1/64**

e. Se va configura adresa IPv6 de legătură locală cu următoarea comandă:

R1(config-if)# **ipv6 address FE80::1 link-local**

f. Se va activa interfața.

Pasul 3: Se va configura adresa IPv6 pe GigabitEthernet0/1.

a. Se vor introduce comenzile necesare pentru a trece la modul de configurare a interfeței pentru GigabitEthernet0/1.

b. Se va consulta tabelul de adrese pentru a obține adresa IPv6 corectă.

c. Se va configura adresa IPv6, de link-local și se va activa interfața.

Pasul 4: Se va configura adresa IPv6 pe Serial0/0/0.

a. Se vor introduce comenzile necesare pentru a trece la modul de configurare a interfeței pentru Serial0/0/0.

b. Se va consulta tabelul de adrese pentru a obține adresa IPv6 corectă.

c. Se va configura adresa IPv6, link local și se va activa interfața.

Partea 2: Se va configura adresa IPv6 pe servere.

Pasul 1: Se va configura adresa IPv6 pe serverul de contabilitate.

a. Se va face clic pe Contabilitate și pe fila Desktop > Configurare IP.

b. Adresa IPv6 va fi setată la 2001:DB8:1:1::4 cu un prefix de /64.

c. Gateway-ul IPv6 va fi setat cu adresa link-local, FE80::1.

Pasul 2: Se va configura adresa IPv6 pe serverul CAD.

Se vor repeta pașii de la 1a la 1c pentru serverul CAD. Se va consulta tabelul de adrese pentru adresa IPv6.

Partea 3: Se va configura adresa IPv6 pe clienți

Pasul 1: Se va configura adresa IPv6 pe clienții de vânzări și facturare.

a. Se va face clic pe Facturare și apoi se va selecta fila Desktop urmată de Configurare IP.

b. Adresa IPv6 va fi setată la 2001:DB8:1:1::3 cu un prefix de /64.

c. Gateway-ul IPv6 va fi setat la adresa link-local, FE80::1.

d. Se vor repeta pașii de la 1a la 1c pentru vânzări. Se va consulta tabelul de adrese pentru adresa IPv6.

Pasul 2: Se va configura adresa IPv6 pe clienții de la secțiile inginerie și proiectare.

a. Se va face clic pe Inginerie și apoi se va selecta fila Desktop urmată de Configurare IP.

b. Adresa IPv6 va fi setată la 2001:DB8:1:2::3 cu un prefix de /64.

c. Gateway-ul IPv6 va fi setat la adresa link-local, FE80::1.

d. Se vor repeta pașii de la 1a la 1c pentru proiectare. Se va consulta tabelul de adrese pentru adresa IPv6.

Partea 4: Se va testa și se va verifica conexiunea la rețea

Pasul 1: Se vor deschide paginile web ale serverului de la clienți.

a. Se va face clic pe Vânzări și pe fila Desktop. Se va închide fereastra Configurare IP, dacă este necesar.

b. Se va face clic pe Browser web. Se va introduce 2001:DB8:1:1::4 în caseta URL și se va face clic pe Go. Ar trebui să apară site-ul de contabilitate.

c. Se va introduce 2001:DB8:1:2::4 în caseta URL și se va face clic pe Go. Ar trebui să apară site-ul web CAD.

d. Se vor repeta pașii de la 1a la 1d pentru restul clienților.

Pasul 2: Se va da ping la ISP.

a. Se va deschide orice fereastră de configurare a computerului client făcând clic pe pictogramă.

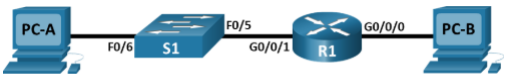
b. Se va face clic pe fila Desktop > Command Prompt.

c. Se va testa conexiunea la ISP prin introducerea următoarei comenzi:

PC> **ping 2001:DB8:1:A001::1**

d. Se va repeta comanda ping pentru toți clienții până când conectivitatea este verificată complet.

EXERCITIUL 6. Configurarea unei Adrese IPv6 pe Dispozitivele de Retea cu Conectivitate în Mod Fizic.



Obiective

Partea 1: Se va configura topologia și se vor configura setările de bază ale routerului și comutatorului.

Partea 2: Se vor configura manual adresele IPv6.

Partea 3: Se va verifica conectivitatea end-to-end.

Instrucțiuni

Partea 1: Se va face cablarea rețelei și se vor configura setările de bază ale routerului și comutatorului. În această parte, se va cabla rețeaua, se vor alimenta dispozitivele și apoi se va configura routerul și comutatorul cu setările de bază pentru aceste dispozitive.

Pasul 1: Va fi făcută cablarea rețelei și vor alimenta dispozitivele.

Se va cabla rețeaua conform topologiei. Se vor alimenta dispozitivele după cum este necesar.

Pasul 2: Se va configura routerul. I se va atribui numele de gazdă și se vor configura setările de bază ale dispozitivului.

Pasul 3: Se va configura comutatorul. Se va atribui numele de gazdă și se vor configura setările de bază ale dispozitivului.

Partea 2: Se vor configura manual adresele IPv6. În această parte, se va configura manual adresa IPv6 pe toate dispozitivele din rețea.

Pasul 1: Se vor atribui adresele IPv6 interfețelor Ethernet de pe R1.

a. Vor fi atribuite adrese IPv6 globale unicast, listate în Tabelul de Adresări, ambelor interfețe Ethernet de pe R1.

Ser va deschide fereastra de configurare.

b. Se va verifica dacă adresa IPv6 unicast corectă este atribuită fiecărei interfețe.

Notă: Adresa link-local (fe80::) afișată se bazează pe adresarea EUI-64, care folosește automat adresa de control al accesului media (MAC) a interfeței pentru a crea o adresă link-local IPv6 pe 128 de biți.

c. Pentru a obține adresa link-local care să se potrivească cu adresa globală unicast de pe interfață, se vor introduce manual adresele link-local pe fiecare dintre interfețele Ethernet de pe R1.

Notă: Fiecare interfață de router aparține unei rețele separate. Pachetele cu o adresă link-local nu părăsesc niciodată rețeaua locală; prin urmare, se poate folosi aceeași adresă locală de legătură pe ambele interfețe.

d. Se va folosi o comandă la alegere pentru a verifica dacă adresa locală a link-ului a fost schimbată în fe80::1.

Fereastra de configurare va fi închisă.

Întrebare:

Care două grupuri multicast au fost alocate interfeței G0/0/0?

Pasul 2: Se va activa rutarea IPv6 pe R1.

a. De la promptul de comandă al hostului PC-B, va fi introdusă comanda ipconfig pentru a examina informațiile despre adresa IPv6 alocată interfeței PC.

Întrebare:

A fost atribuită o adresă IPv6 unicast cardului de interfață de rețea (NIC) de pe PC-B?

b. Se va folosi comanda IPv6 unicast-routing pentru a activa rutarea IPv6 pe R1.

Se va deschide fereastra de configurare.

c. Se va folosi o comandă pentru a verifica că noul grup multicast este alocat interfeței G0/0/0. Se va observa că grupul multicast cu toate ruterele (ff02::2) apare acum pentru interfața G0/0/0.

Notă: Acest lucru va permite computerelor să obțină automat adresa IP și informații despre gateway implicit, utilizând configurarea automată a adresei fără stare (SLAAC).

d. Acum deoarece R1 face parte din grupul de adrese multicast FF02::2 cu toate rutele, de la PC-B reemite comanda ipconfig și examinează informațiile despre adresa IPv6.

Întrebare:

De ce a primit PC-B Prefixul de rutare globală și ID-ul de subrețea care au fost configurate pe R1?

Pasul 3: Se vor atribui adrese IPv6 interfeței de gestionare (SVI) pe S1.

a. Va fi atribuită adresa IPv6 pentru S1. Se va atribui și o adresă locală de legătură pentru această interfață.

Notă: Comutatorul va primi automat adresa de gateway implicită din mesajul RA trimis de router. Va folosi adresa IPv6 sursă a mesajului RA, care este adresa locală de legătură a routerului. Cu toate acestea, este posibil ca versiunea Packet Tracer să nu accepte încă acest lucru pe comutator.

b. Se va utiliza o comandă la alegere pentru a verifica dacă adresele IPv6 sunt alocate corect interfeței de gestionare.

Fereastra de configurare va fi închisă.

Pasul 4: Se vor atribui adrese IPv6 statice computerelor.

a. Se va deschide fereastra Configurare IP pe fiecare PC și se va atribui adresa IPv6.

b. Se va verifica că ambele PC-uri au informațiile corecte despre adresa IPv6. Fiecare PC ar trebui să aibă două adrese IPv6 globale: una statică și una SLAAC.

Partea 3: Se va verifica conectivitatea end-to-end.

a. De la PC-A, se va da ping la adresa fe80::1. Aceasta este adresa locală de legătură atribuită lui G0/0/1 pe R1.

b. La PC-A, se va folosi comanda tracert pentru a verifica dacă va avea conectivitate end-to-end la PC-B.

c. De la PC-B, se va da ping la PC-A.

d. De la PC-B, se va da ping adresa locală de legătură pentru G0/0/0 pe R1.

Notă: În condițiile în care conectivitatea end-to-end nu este stabilită, se va depana atribuirea adreselor IPv6 pentru a verifica dacă adresele au fost introduse corect pe toate dispozitivele.

EXERCITIUL 7. Configurarea unui Router cu Servicii Integrate.

Obiective

Partea 1: Se va conecta un cablu direct la un router integrat.

Partea 2: Se va activa conexiunea wireless.

Partea 3: Se va configura și se va verifica accesul pentru clienții wireless.

Partea 1: Se va conecta un router integrat WRT300N cu laptopul Service cu un cablu corect.

Pasul 1: Se va stabili și se va verifica conectivitatea la routerul integrat.

a. Se va conecta cablul corespunzător de la Host-A la portul Ethernet 1 pe IR.

b. Va aștepta ca lumina de legătură să devină verde. Va fi deschis promptul de comandă pentru Host-A. Se va utiliza comanda ***ipconfig*** pentru a verifica informațiile de adresare IP primite de gazdă.

c. Se va introduce comanda ***ping 192.168.0.1*** pentru a verifica că Host-A poate accesa gateway-ul implicit.

Pasul 2: Se va accesa interfața grafică de utilizator (GUI) IR folosind un browser web.

a. Va fi deschis browserul web pe Host-A pentru a accesa GUI pe IR pentru configurare. Va fi introdusă adresa de gateway implicită a Host-A în câmpul URL.

b. Vor fi introduse acreditările admin ca nume de utilizator și parolă, pentru a accesa IR.

Partea 2: Se va activa conexiunea wireless.

Pasul 1: Se va configura IR pentru conexiunea la Internet.

Nu există conexiune la Internet în acest scenariu, dar se vor configura totuși setările pentru interfața orientată către Internet. Pentru Tip de conexiune la Internet, se va alege IP static din lista derulantă, apoi se vor introduce următoarele informații IP statice:

· *Adresă IP Internet – 198.133.219.1*

· *Mască de subrețea – 255.255.255.0*

· *Gateway implicit – 198.133.219.254*

· *DNS 1 – 198.133.219.10*

Pasul 2: Se vor configura parametrii din interiorul rețelei. Se va face o derulare în jos la secțiunea Configurare rețea și vor fi configurate următoarele informații:

· *Adresă IP – 172.31.1.1*

· *Mască de subrețea – 255.255.255.224*

· *Adresă IP de pornire – Se introduce 5 pentru ultimul octet.*

· *Număr maxim de utilizatori – 25*

Notă: Intervalul de adrese IP al pool-ului DHCP va reflecta modificările numai după ce se va face clic pe Save Settings.

Pasul 3: Se vor salva setările și se va reconecta IRul.

a. Se va derula în partea de jos a paginii și se va face clic pe Save Settings. Dacă se trece de la o filă la alta fără salvare, configurațiile se vor pierde.

b. Se va pierde conexiunea când se va face clic pe Save Settings deoarece a fost schimbată adresa IP a routerului.

c. Se face întoarcerea la promptul de comandă al Host-A. Se va introduce comanda ***ipconfig /renew*** pentru a reînnoi adresa IP.

d. Se va folosi browserul web Host-A pentru a se reconecta IRul. Va trebui să se utilizeze noua adresă implicită de gateway. Se vor verifica setările de conexiune la Internet din fila Stat. Setările ar trebui să se potrivească cu valorile configurate în Partea 2, Pasul 1. Dacă nu, se vor repeta Partea 2, Pasul 1 și Pasul 2.

Pasul 4: Se va configura conectivitatea wireless pentru dispozitivele wireless.

a. Se va face clic pe fila Wireless și se vor investiga opțiunile din lista derulantă pentru Modul de rețea.

Când se va alege opțiunea Dezactivare?

Când se va alege opțiunea Mixtă?

b. Va fi setat modul de rețea numai pentru Wireless-N.

c. Se va schimba SSID-ul în MyHomeNetwork.

d. Atunci când un client wireless cercetează zona căutând rețele wireless, detectează orice transmisie SSID. Emisiunile SSID sunt activate în mod implicit.

Dacă SSID-ul unui punct de acces nu este difuzat, cum se vor conecta dispozitivele la acesta?

e. Pentru performanțe optime într-o rețea care utilizează Wireless-N, banda radio va fi setată la Wide-40MHz.

f. Se va face clic pe Save Settings și apoi pe Continue.

Pasul 5: Se va configura securitatea wireless, astfel încât clienții să se autentifice pentru a se conecta la rețeaua wireless.

a. Se va face clic pe opțiunea Wireless Security din fila Wireless.

b. Modul de securitate va fi setat la WPA2 Personal. *Care este diferența dintre personal și întreprindere?*

c. Se va lăsa modul de criptare pe AES și se va seta passphrase la ***itsasecret***.

d. Se va face clic pe Save Settings și apoi pe Continue.

Pasul 6: Se va schimba parola implicită pentru a accesa IR pentru configurare.

a. Ar trebui să schimbe întotdeauna parola implicită pentru mai multă securitate.

Partea 3: Se va configura și se va verifica accesul la client wireless

Pasul 1: Se va configura laptopul pentru a accesa rețeaua wireless.

a. Se va face clic pe Laptop și pe Desktop > PC fără fir. Fereastra care se deschide în GUI IR client.

b. Se va face clic pe fila Conectare și pe Reîmprospătare, dacă este necesar. Ar trebui să se vadă MyHomeNetwork listat sub Numele rețelei fără fir.

c. Se va face clic pe MyHomeNetwork și pe Conectare.

d. Ar trebui acum să fie văzut MyHomeNetwork. Se va face clic pe el și apoi pe Conectare.

e. Cheia pre-partajată este parola configurată în partea 2, pasul 5c. Se va introduce parola și se va face clic pe Conectare.

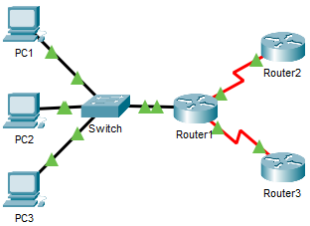
f. Se va închide interfața IR și se va face clic pe Command Prompt. Se va introduce comanda ***ipconfig*** pentru a verifica adresa IP primită de laptop.

Pasul 2: Se va verifica conectivitatea dintre laptop și Host-A.

a. Ping IR de la laptop.

b. Ping Host-A de pe laptop.

EXERCITIUL 8. Investigarea Traficului Unicast, Broadcast si Multicast.



Obiective

Partea 1: Se va genera trafic unicast.

Partea 2: Se va genera trafic Broadcast.

Partea 3: Se va investiga Traficul Multicast.

Partea 1: Se va genera trafic unicast.

Pasul 1: Se va folosi ***ping*** pentru a genera trafic.

a. Se va face clic pe PC1 și pe fila Desktop > Prompt de comandă.

b. Se va introduce comanda ***ping 10.0.3.2***. Ping-ul ar trebui să reușească.

Pasul 2: Se va intra în modul Simulare.

a. Se va face clic pe fila Simulare pentru a intra în modul Simulare.

b. Se va face clic pe Editare filtre și se va verifica dacă sunt selectate numai evenimentele ICMP și EIGRP.

c. Se va face clic pe PC1 și se va introduce comanda ***ping 10.0.3.2***.

Pasul 3: Va fi examinat traficul unicast. PDU-ul de la PC1 este o cerere de eco ICMP destinată interfeței seriale de pe Router3.

a. Se va face clic pe Captură/Redirecționare în mod repetat și se va urmări în timp ce cererea de ecou este trimisă către Router3 și răspunsul de ecou este trimis înapoi la PC1. Se va opri când primul răspuns ecou ajunge la PC1.

Prin ce dispozitive a călătorit pachetul cu transmisia unicast?

b. În secțiunea Lista de evenimente din panoul de simulare, ultima coloană conține o casetă colorată care oferă acces la informații detaliate despre un eveniment. Se va face clic pe caseta colorată din ultima coloană pentru primul eveniment. Se deschide fereastra PDU Information.

La ce strat începe această transmisie și de ce?

c. Se vor examina informațiile de nivel 3 pentru toate evenimentele. Se va observa că atât adresele IP sursă, cât și cele de destinație sunt adrese unicast care se referă la PC1 și la interfața serială de pe Router3.

Ce două modificări au loc la Layer 3 când pachetul ajunge la Router3?

d. Se va face clic pe Resetare simulare.

Partea 2: Se va genera Broadcast Traffic.

Pasul 1: Se va adăuga un PDU complex.

a. Se va face clic pe Add Complex PDU. Pictograma pentru aceasta se află în bara de instrumente din dreapta și arată un plic deschis.

b. Va fi plasat cursorul mouse-ului peste topologie, iar indicatorul se va schimba într-un plic cu semnul plus (+).

c. Se va face clic pe PC1 pentru a servi ca sursă pentru acest mesaj de testare și se deschide fereastra de dialog Creare PDU complexă. Se vor introduce următoarele valori:

· *Adresa IP de destinație: 255.255.255.255 (broadcast address)*

· *Numărul secvenței: 1*

· *Timp One Shot: 0*

În setările PDU, valoarea implicită pentru Select Application: este PING.

Care sunt cel puțin alte 3 aplicații disponibile pentru utilizare?

d. Se va face clic pe Creare PDU. Acest pachet de difuzare de test apare acum în Lista de evenimente din panoul de simulare. De asemenea, apare în fereastra PDU List. Este primul PDU pentru Scenariul 0.

e. Se va face clic pe Captură/Redirecționare de două ori. Acest pachet este trimis către comutator și apoi transmis către PC2, PC3 și Router1. Se vor examina informațiile de nivel 3 pentru toate evenimentele. Se va observa că adresa IP de destinație este 255.255.255.255, care este adresa de difuzare IP configurată la crearea PDU-ului complex.

Analizând informațiile modelului OSI, ce modificări apar în informațiile de layer 3 din coloana Out Layers la Router1, PC2 și PC3?

f. Se va face clic din nou pe Captură/Redirecționare.

PDU-ul de difuzare redirecționează vreodată către Router2 sau Router3? De ce?

g. După ce se examinează comportamentul de difuzare, se va șterge pachetul de test făcând clic pe Delete sub Scenariul 0.

Partea 3: Se va investiga Traficul Multicast.

Pasul 1: Se va examina traficul generat de protocoalele de rutare.

a. Se va face clic pe Captură/Înainte. Pachetele EIGRP se află la Router1 și așteaptă să fie transmise în mai multe interfețe.

b. Se va examina conținutul acestor pachete prin deschiderea ferestrei Informații PDU și se va face clic din nou pe Captură/Redirecționare. Pachetele sunt trimise către celelalte două routere și către comutator. Routerele acceptă și procesează pachetele, deoarece fac parte din grupul multicast. Comutatorul va redirecționa pachetele către computere.

c. Se va face clic pe Captură/Redirecționare până când pachetul EIGRP va ajunge la computere.

Ce fac gazdele cu pachetele?

Se vor examina informațiile de nivel 3 și 4 pentru toate evenimentele EIGRP.

Care este adresa de destinație a fiecărui pachet?

d. Se va face clic pe unul dintre pachetele livrate la unul dintre PC-uri.

Ce se întâmplă cu acele pachete?

Pe baza traficului generat de cele trei tipuri de pachete IP, care sunt diferențele majore de livrare?

LABORATOR 8. ADRESAREA IPv4.

În prezent, există încă o mulțime de rețele care utilizează adresa IPv4, chiar dacă organizațiile care le folosesc fac tranziția la IPv6. Prin urmare, este încă foarte important ca administratorii de rețea să știe tot ce pot despre adresarea IPv4.

Acesta include modul de segmentare a unei rețele în subrețele și cum de se creeaza o mască de subrețea cu lungime variabilă (VLSM) ca parte a unei scheme generale de adresare IPv4.

Subnetarea poate părea copleșitoare la început, dar sunt prezentae câteva trucuri care pot ajuta pe parcurs.

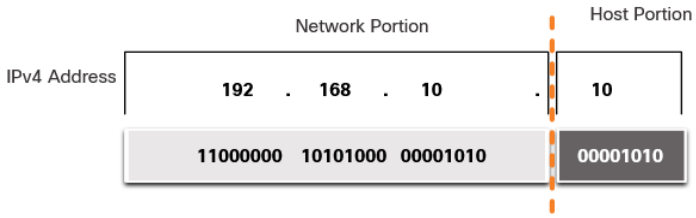
Obiective

Calcularea unei scheme de subnetare IPv4 pentru a segmenta eficient rețeaua.

IPv4 Address Structure	Descrierea structurii unei adrese IPv4, inclusiv porțiunea de rețea, porțiunea gazdă și masca de subrețea.
IPv4 Unicast, Broadcast, and Multicast	Compararea caracteristicilor și utilizărilor adreselor IPv4 unicast, broadcast și multicast.
Types of IPv4 Addresses	Explain public, private, and reserved IPv4 addresses.
Network Segmentation	Explicarea modului în care subrețele segmentează o rețea pentru a permite o comunicare mai bună.
Subnet an IPv4 Network	Cum se calculează subrețele IPv4 pentru un prefix /24.
Subnet a /16 and a /8 Prefix	Cum se calculează subrețele IPv4 pentru un prefix /16 și /8.
Subnet To Meet Requirements	Având în vedere un set de cerințe pentru subrețea, cum implementăm o schemă de adresare IPv4.
Variable Length Subnet Masking	Explicarea modului de a crea o schemă de adresare flexibilă folosind mascarea subrețelei de lungime variabilă (VLSM).
Structured Design	Implementarea unei scheme de adresare VLSM.

PART 1. IPv4 Address Structure

O adresă IPv4 este o adresă ierarhică de 32 de biți care este alcătuită dintr-o porțiune de rețea și o porțiune de gazdă. Când determinați porțiunea de rețea față de porțiunea gazdă, trebuie să vă uitați la fluxul de 32 de biți, așa cum se arată în figură.

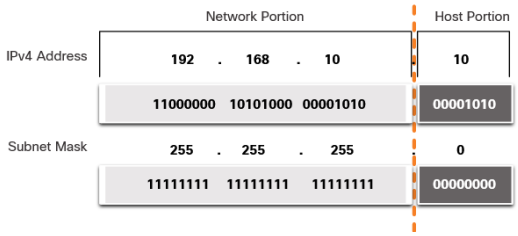


După cum se arată în figură, alocarea unei adrese IPv4 unei gazde necesită următoarele:

Adresă IPv4 - Aceasta este adresa IPv4 unică a gazdei.

Masca de subrețea - Aceasta este folosită pentru a identifica porțiunea de rețea/gazdă a adresei IPv4.

Pentru a identifica porțiunile de rețea și gazdă ale unei adrese IPv4, masca de subrețea este comparată cu adresa IPv4 bit cu bit, de la stânga la dreapta, așa cum se arată în figură.



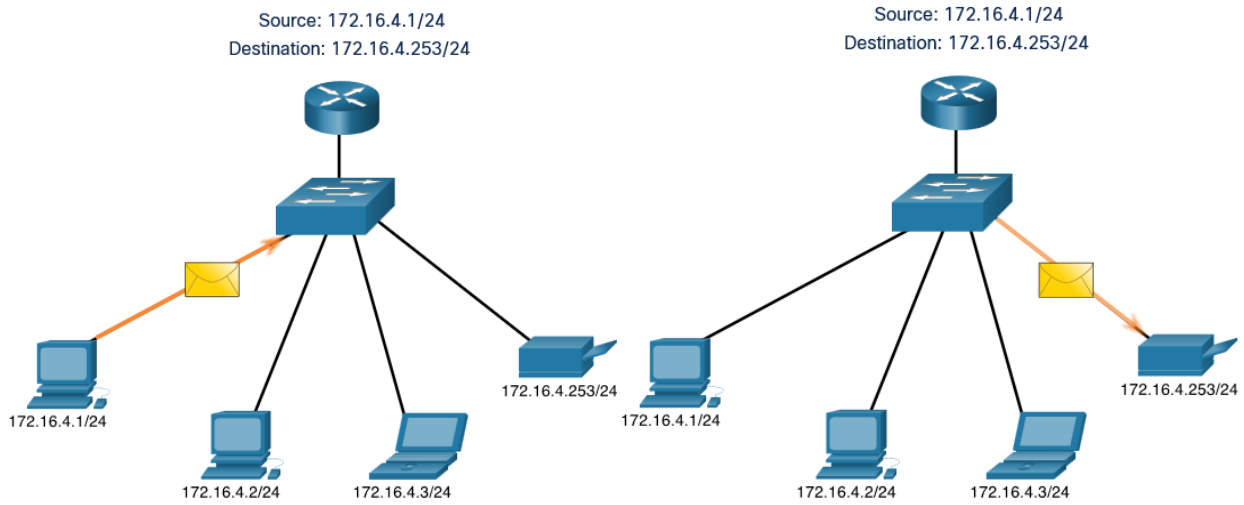
Instrucțiuni: Utilizarea procesului ANDing pentru a determina adresa de rețea (în formate binar și zecimal).

Host Address	10	105	219	81
Subnet Mask	255	255	255	252
Host Address in binary	00001010	01101001	11011011	01010001
Subnet Mask in binary	11111111	11111111	11111111	11111100
Network Address in binary				
Network Address in decimal				

PART 1. IPv4 Unicast, Broadcast, and Multicast

PASUL 1. **UNICAST** – Transmisia unicast se referă la un dispozitiv care trimite un mesaj către un alt dispozitiv în comunicații unu-la-unu.

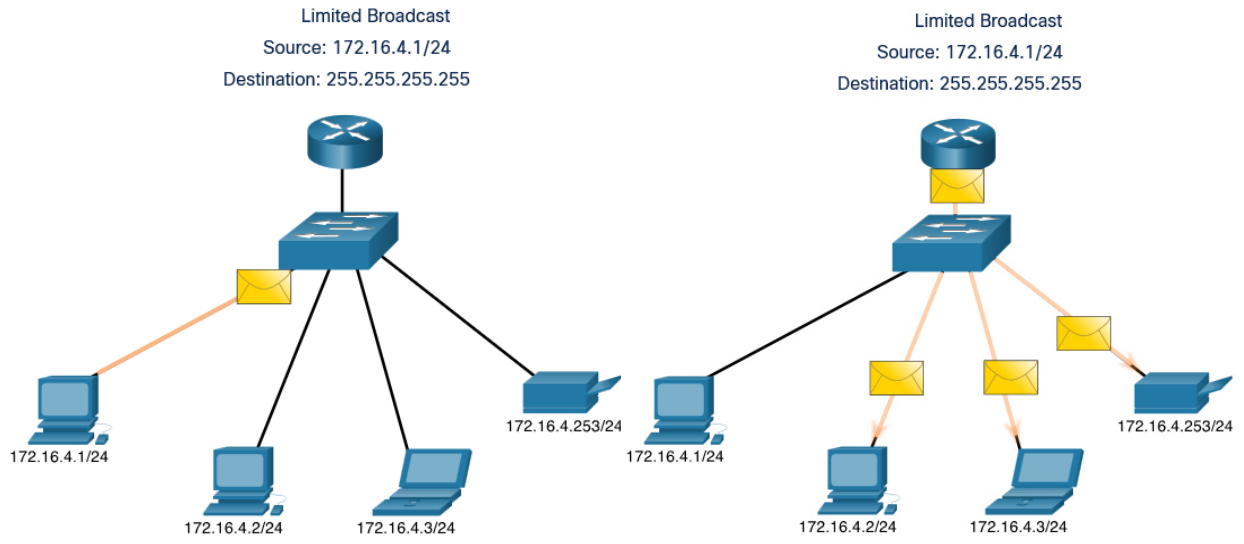
Un pachet unicast are o adresă IP de destinație care este o adresă unicast care ajunge la un singur destinatar. O adresă IP sursă poate fi doar o adresă unicast, deoarece pachetul poate proveni doar dintr-o singură sursă. Acest lucru este indiferent dacă adresa IP de destinație este unicast, broadcast sau multicast.



PASUL 2. Broadcast - Transmisia broadcast se referă la un dispozitiv care trimite un mesaj către toate dispozitivele dintr-o rețea în comunicații unu-la-toți.

Un pachet de difuzare are o adresă IP de destinație cu biți (1s) în porțiunea gazdă sau 32 de biți de un (1).

O difuzare direcționată este trimisă tuturor gazdelor dintr-o anumită rețea. De exemplu, o gazdă din rețeaua 172.16.4.0/24 trimite un pachet la 172.16.4.255. O difuzare limitată este trimisă la 255.255.255.255. În mod implicit, routerele nu transmit broadcast.



PASUL 3. Multicast - Transmisia multicast reduce traficul permițând unei gazde să trimită un singur pachet către un set selectat de gazde care sunt abonate la un grup de multicast.

Un pachet multicast este un pachet cu o adresă IP de destinație care este o adresă multicast. IPv4 a rezervat adresele de la 224.0.0.0 la 239.255.255.255 ca interval multicast.

PART 2. Tipuri de Adrese IPv4

PASUL 1. Adrese Publice

Adresele IPv4 publice sunt adrese care sunt direcționate la nivel global între routerele furnizorului de servicii de internet (ISP).

1. ***Clasa A*** (0.0.0.0/8 până la 127.0.0.0/8) - Proiectat pentru a suporta rețele extrem de mari cu peste 16 milioane de adrese gazdă. Clasa A a folosit un prefix fix /8 cu primul octet pentru a indica adresa de rețea și restul de trei octeți pentru adresele gazdei (mai mult de 16 milioane de adrese gazdă per rețea).

2. ***Clasa B*** (128.0.0.0 /16 - 191.255.0.0 /16) - Proiectat pentru a susține nevoile rețelelor de dimensiuni moderate până la mari, cu până la aproximativ 65.000 de adrese gazdă. Clasa B a folosit un prefix fix /16 cu cei doi octeți de ordin înalt pentru a indica adresa de rețea și cei doi octeți rămași pentru adresele gazdei (mai mult de 65.000 de adrese gazdă per rețea).Clasa C.

3. ***Clasa C*** (192.0.0.0 /24 - 223.255.255.0 /24) - Proiectat pentru a suporta rețele mici cu maximum 254 de gazde. Clasa C a folosit un prefix fix /24 cu primii trei octeți pentru a indica rețeaua și octetul rămas pentru adresele de gazdă (doar 254 de adrese de gazdă per rețea).

4. ***Clasa D*** în spațiul de lucru 224.0.0.0 la 239.0.0.0 bloc multicast.

5. ***Clasa E*** în spațiul de lucru 240.0.0.0 - 255.0.0.0 bloc de adrese experimental.

PARTEA 3. SUBNETAREA

Subnetarea reduce traficul general de rețea și îmbunătățește performanța rețelei. De asemenea, permite unui administrator să implementeze politici de securitate, cum ar fi subrețelele care au voie sau nu să comunice împreună. Un alt motiv este că reduce numărul de dispozitive afectate de traficul anormal de difuzare din cauza configurărilor greșite, a problemelor hardware/software sau a intențiilor rău intenționate.

Există diferite moduri de utilizare a subrețelelor pentru a ajuta la gestionarea dispozitivelor de rețea.

- *Subnetarea în funcție de locație.*
- *Subnetarea pe baza de grup sau funcție.*
- *Subnetarea dupa tip de dispozitiv.*

PASUL 1. Subnetarea unei Rețele cu IPv4.

Subnetarea este o abilitate critică pe care trebuie să o stapanim atunci când se administreaza o rețea IPv4. Este un pic descurajantă la început, dar devine mult mai ușor cu antrenament.

Subrețelele IPv4 sunt create utilizând unul sau mai mulți biți gazdă ca biți de rețea. Acest lucru se realizează prin extinderea măștii de subrețea pentru a împrumuta unii dintre biții de la porțiunea gazdă a adresei pentru a crea biți de rețea suplimentari. Cu cât sunt împrumutați mai mulți biți gazdă, cu atât mai multe subrețele pot fi definite. Cu cât sunt împrumutați mai mulți biți pentru a crește numărul de subrețele, se reduce numărul de gazde pe subrețea.

Rețelele sunt cel mai ușor de subnetat la limita octetului /8, /16 și /24. Tabelul identifică aceste lungimi de prefix, unde se poate observa că utilizarea lungimii de prefix mai mari scade numărul de gazde per subrețea.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	**255**.0.0.0	**nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh **11111111**.00000000.00000000.00000000	16,777,214
/16	**255.255**.0.0	**nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh **11111111.11111111**.00000000.00000000	65,534
/24	**255.255.255**.0	**nnnnnnnn.nnnnnnnn.nnnnnnnn**.hhhhhhhh **11111111.11111111.11111111**.00000000	254

Pentru a înțelege cum poate fi utilă subnetarea la limita octetului, se ia în considerare următorul exemplu. Presupunem că o întreprindere a ales adresa privată 10.0.0.0/8 ca adresă de rețea internă. Această adresă de rețea poate conecta 16.777.214 de gazde într-un domeniu de difuzare. Evident, a avea peste 16 milioane de gazde pe o singură subrețea nu este ideal.

Întreprinderea ar putea în continuare subneta adresa 10.0.0.0/8 la limita octetului /16, așa cum se arată în tabel. Acest lucru ar oferi întreprinderii capacitatea de a defini până la 256 de subrețele (adică, 10.0.0.0/16 - 10.255.0.0/16) cu fiecare

subrețea capabilă să conecteze 65.534 de gazde. Se poate observa cum primii doi octeți identifică porțiunea de rețea a adresei, în timp ce ultimii doi octeți sunt pentru adrese IP gazdă.

Subnetarea rețelei 10.0.0.0/8 folosind un /16

Subnet Address (256 Possible Subnets)	Host Range (65,534 possible hosts per subnet)	Broadcast
10.0.0.0/**16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/**16**	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
...	...	...
10.255.0.0/**16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Alternativ, întreprinderea ar putea alege să subneteze rețeaua 10.0.0.0/8 la granița /24 octet, așa cum se arată în tabel. Acest lucru ar permite întreprinderii să definească 65.536 de subrețele fiecare capabilă să conecteze 254 de gazde. Limita /24 este foarte populară în subrețele, deoarece găzduiește un număr rezonabil de gazde și convenabil subrețele la limita octetului.

Subnetarea rețelei 10.0.0.0/8 folosind un prefix /24.

Subnet Address (65,536 Possible Subnets)	Host Range (254 possible hosts per subnet)	Broadcast
10.0.0.0/**24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255

Subnet Address (65,536 Possible Subnets)	Host Range (254 possible hosts per subnet)	Broadcast
…	…	…
10.100.0.0/**24**	**10.100.0**.1 - **10.100.0**.254	**10.100.0**.255
...	...	...
10.255.255.0/**24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

De exemplu, o adresă de rețea /24 este în mod obișnuit subnetata folosind lungimi mai mari de prefix prin împrumutarea de biți din al patrulea octet. Acest lucru oferă administratorului flexibilitate suplimentară atunci când atribuie adrese de rețea unui număr mai mic de dispozitive finale.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

Pentru fiecare bit împrumutat în al patrulea octet, numărul de subrețele disponibile este dublat, reducând în același timp numărul de adrese gazdă per subrețea:

/25 rând - Împrumutarea a 1 bit de la al patrulea octet creează 2 subrețele care acceptă 126 de gazde fiecare.

/26 rând - Împrumutarea a 2 biți creează 4 subrețele care acceptă 62 de gazde fiecare.

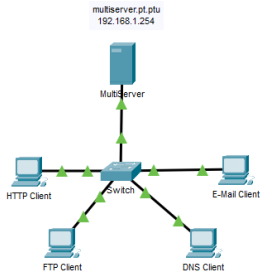
/27 rând - Împrumutarea a 3 biți creează 8 subrețele care acceptă 30 de gazde fiecare.

/28 rând - Împrumutarea a 4 biți creează 16 subrețele care acceptă 14 gazde fiecare.

/29 rând - Împrumutarea a 5 biți creează 32 de subrețele care acceptă 6 gazde fiecare.

/30 rând - Împrumutarea a 6 biți creează 64 de subrețele care acceptă 2 gazde fiecare.

LABORATOR 9. Comunicații TCP și UDP.



Obiective

Partea 1: Se va genera trafic de rețea în modul de simulare.

Partea 2: Va fi examinată funcționalitatea protocoalelor TCP și UDP.

Instrucțiuni

Partea 1: Se va genera trafic de rețea în modul de simulare și vizualizare multiplexare

Pasul 1: Se va genera trafic pentru a popula tabelele ARP (Address Resolution Protocol).

Se va efectua următoarea sarcină pentru a reduce cantitatea de trafic de rețea vizualizată în simulare.

a. Se va face clic pe MultiServer și pe fila Desktop > Prompt de comandă.

b. Se va introduce comanda ***ping -n 1 192.168.1.255***. Se va da ping la adresa de difuzare pentru LAN client. Opțiunea de comandă va trimite o singură solicitare ping, mai degrabă decât cele patru obișnuite. Acest lucru va dura câteva secunde, deoarece fiecare dispozitiv din rețea răspunde la cererea ping de la MultiServer.

c. Fereastra MultiServer va fi închisă.

Pasul 2: Va fi generat trafic web (HTTP).

a. Se va trece la modul Simulare.

b. Se va face clic pe Client HTTP și se va deschide browserul web de pe desktop.

c. În câmpul URL, se va introduce 192.168.1.254 și se va face clic pe Go. În fereastra topologiei vor apărea plicuri (PDU).

d. Se va minimiza, dar nu se va închide, fereastra de configurare a clientului HTTP.

Pasul 3: Se va genera trafic FTP.

a. Se va face clic pe Client FTP și se va deschide Linia de comandă de pe desktop

b. Se va introduce comanda ***ftp 192.168.1.254***. PDU-urile vor apărea în fereastra de simulare.

c. Se va minimiza, dar nu se va închide, fereastra de configurare a clientului FTP.

Pasul 4: Se va genera trafic DNS.

a. Se va face clic pe Client DNS și se va deschide Linia de comandă.

b. Se va introduce comanda ***nslookup multiserver.pt.ptu***. Un PDU va apărea în fereastra de simulare.

c. Se va minimiza, dar nu se va închide, fereastra de configurare a clientului DNS.

Pasul 5: Se va genera trafic de e-mail.

a. Se va face clic pe E-Mail Client și se va deschide instrumentul E-mail de pe desktop.

b. Se va face clic pe Compune și se vor introduce următoarele informații:

1) Către: user@multiserver.pt.ptu

2) Subiect: personalizare linia de subiect

3) Corpul e-mailului: va fi personalizat e-mailul

c. Se va face clic pe Trimite.

d. Se va minimiza, dar nu se va închide, fereastra de configurare a clientului de e-mail.

Pasul 6: Se va verifica dacă traficul este generat și gata pentru simulare. Ar trebui să existe acum intrări PDU în panoul de simulare pentru fiecare dintre computerele client.

Pasul 7: Va fi examinată multiplexarea pe măsură ce traficul traversează rețeaua. Acum se va folosi butonul Captură/Înainte din panoul de simulare pentru a observa diferitele protocoale care călătoresc în rețea.

Notă: butonul Captură/Înainte „ >| ‘ este o săgeată mică îndreptată spre dreapta cu o bară verticală lângă ea.

a. Se va face clic pe Captură/Redirecționare o dată. Toate PDU-urile se deplasează la comutator.

b. Se va face clic pe Captură/Redirecționare de șase ori și vor fi urmărite PDU-urile de la diferite gazde în timp ce călătoresc în rețea. Va fi de reținut că doar un singur PDU poate traversa un fir în fiecare direcție la un moment dat.

Întrebări:

Cum se numește această procedură?

Răspunsuri aici.

O varietate de PDU-uri apar în lista de evenimente din panoul de simulare. *Care este semnificația diferitelor culori?*

Răspunsuri aici.

Partea 2: Va fi examinată funcționalitatea protocoalelor TCP și UDP

Pasul 1: Se va examina traficul HTTP pe măsură ce clienții comunică cu serverul.

a. Se va face clic pe Resetare simulare.

b. Se va filtra traficul care este afișat în prezent numai pentru PDU-urile HTTP și TCP. Pentru a filtra traficul care este afișat în prezent:

1) Se va face clic pe Editare filtre și se va comuta butonul Show All/None.

2) Se vor selecta HTTP și TCP. Se va face clic pe „x” roșu din colțul din dreapta sus al casetei Filtre editate pentru a o închide. Evenimentele vizibile ar trebui să afișeze acum numai PDU-uri HTTP și TCP.

c. Se va deschide browserul pe HTTP Client și se va introduce 192.168.1.254 în câmpul URL. Se va face clic pe Go pentru a fi conectat la server prin HTTP. Se va minimiza fereastra HTTP Client.

d. Se va face clic pe Captură/Redirecționare până când apare un PDU pentru HTTP. Va fi de reținut că acum culoarea plicului din fereastra de topologie se potrivește cu codul de culoare pentru HTTP PDU din panoul de simulare.

Întrebare:

De ce a durat atât de mult până când PDU-ul HTTP să apară?

Răspunsuri aici.

e. Se va face clic pe plicul PDU pentru a afișa detaliile PDU. Se va face clic pe fila Outbound PDU Details și se va derula în jos de la a doua până la ultima secțiune.

Care este secțiunea etichetată?

Răspunsuri aici.

Sunt aceste comunicări considerate a fi de încredere?

Răspunsuri aici.

Se vor înregistra valorile SRC PORT, DEST PORT, SEQUENCE NUM și ACK NUM.

Răspunsuri aici.

f. Va fi analizată valoarea din câmpul Flags, care se află lângă câmpul Window. Valorile din dreapta „b” reprezintă steaguri TCP care sunt setate pentru această etapă a conversației de date. Fiecare dintre cele șase locuri corespunde unui steag. Prezența unui „1” în orice loc indică faptul că steagul este setat. Mai mult de un steag poate fi setat la un moment dat. Valorile steagurilor sunt prezentate mai jos.

Flag Place	6	5	4	3	2	1
Value	URG	ACK	PSH	RST	SYN	FIN

Ce steaguri TCP sunt setate în această PDU?

Răspunsuri aici.

g. Se va închide PDU-ul și se va face clic pe Captură/Redirecționare până când un PDU cu bifă revine la clientul HTTP.

h. Se va face clic pe plicul PDU și se selectează Inbound PDU Details.

Întrebare:

Cum diferă porturile și numerele de secvență față de înainte?

Răspunsuri aici.

i. Se va face clic pe HTTP PDU pe care Clientul HTTP a pregătit-o să o trimită către MultiServer. Acesta este începutul comunicării HTTP. Se va face clic pe acest al doilea plic PDU și se selectează Outbound PDU Details.

Întrebare:

Ce informații sunt listate acum în secțiunea TCP?

Cum sunt diferite porturile și numerele de secvență din precedentele două PDU-uri?

Răspunsuri aici.

j. Va fi resetata simularea.

Pasul 2: Se va examina traficul FTP pe măsură ce clienții comunică cu serverul.

a. Va fi deschis promptul de comandă pe desktopul clientului FTP. Se va iniția o conexiune FTP introducând ***ftp 192.168.1.254***.

b. În panoul de simulare, se va modifica Editarea filtrelor pentru a afișa numai FTP și TCP.

c. Se va face clic pe Captură/Înainte. Se va face clic pe al doilea plic PDU pentru a-l deschide. Se va face clic pe fila Outbound PDU Details și derulează în jos la secțiunea TCP.

Întrebare:

Sunt aceste comunicări considerate a fi de încredere?

Răspunsuri aici.

d. Se vor înregistra valorile SRC PORT, DEST PORT, SEQUENCE NUM și ACK NUM.

Întrebare:

Care este valoarea în câmpul steag?

e. Se va închide PDU-ul și se va face clic pe Capture/Forward până când un PDU se întoarce la clientul FTP cu o bifă.

f. Se va face clic pe plicul PDU și se selectează Inbound PDU Details.

Întrebare:

Cum diferă porturile și numerele de secvență față de înainte?

Răspunsuri aici.

g. Se va face clic pe fila Outbound PDU Details.

Întrebare:

Cum diferă porturile și numerele de secvență față de rezultatele anterioare?

Răspunsuri aici.

h. Se va închide PDU-ul și se va face clic pe Capture/Forward până când un al doilea PDU se întoarce la clientul FTP. PDU-ul este de altă culoare.

i. Va fi deschis PDU-ul și va fi selectat Inbound PDU Details. Va fi derulat în jos dincolo de secțiunea TCP.

Întrebare:

Care este mesajul de la server?

Răspunsuri aici.

j. Se va face clic pe Resetare simulare.

Pasul 3: Se va examina traficul DNS pe măsură ce clienții comunică cu serverul.

a. Se vor repeta pașii din partea 1 pentru a crea trafic DNS.

b. În panoul de simulare, se va modifica Editarea filtrelor pentru a afișa numai DNS și UDP.

c. Se va face clic pe plicul PDU pentru a-l deschide.

d. Se vor analiza detaliile modelului OSI pentru PDU de ieșire.

Întrebare:

Care este protocolul Layer 4?

Răspunsuri aici.

Sunt aceste comunicări considerate a fi de încredere?

Răspunsuri aici.

e. Va fi deschisă fila Outbound PDU Details și va găsi secțiunea UDP a formatelor PDU. Se vor înregistra valorile SRC PORT și DEST PORT.

Întrebare:

De ce nu există numere de ordine și de confirmare?

Răspunsuri aici.

f. Se va închide PDU-ul și se va face clic pe Captură/Redirecționare până când un PDU cu o bifă revine la Clientul DNS.

g. Se va face clic pe plicul PDU și se selectează Inbound PDU Details.

Întrebare:

Cum diferă porturile și numerele de secvență față de cele precedente?

Răspunsuri aici.

Cum se numește ultima secțiune a PDU? Care este adresa IP pentru numele multiserver.pt.ptu?

Răspunsuri aici.

h. Se va face clic pe Resetare simulare.

Pasul 4: Se va examina traficul de e-mail pe măsură ce clienții comunică cu serverul.

a. Se vor repeta pașii din partea 1 pentru a trimite un e-mail la ***user@multiserver.pt.ptu***.

b. În panoul de simulare, se va modifica Editarea filtrelor pentru a afișa numai POP3, SMTP și TCP.

c. Se va face clic pe primul plic PDU pentru a-l deschide.

d. Se va face clic pe fila Outbound PDU Details și derulează în jos până la ultima secțiune.

Întrebări:

Ce protocol de nivel transport folosește traficul de e-mail?

Răspunsuri aici.

Sunt aceste comunicări considerate a fi de încredere?

Răspunsuri aici.

e. Se înregistrează valorile SRC PORT, DEST PORT, SEQUENCE NUM și ACK NUM. *Care este valoarea câmpului steag*?

f. Se va închide PDU-ul și se va face clic pe Captură/Redirecționare până când un PDU se întoarce la clientul de e-mail cu o bifă.

g. Se va face clic pe plicul TCP PDU și se selectează Inbound PDU Details.

Întrebare:

Cum diferă porturile și numerele de secvență față de precedentele?

Răspunsuri aici.

h. Se va face clic pe fila Outbound PDU Details.

Întrebare:

Cum diferă porturile și numerele de secvență față de cele două rezultate anterioare?

Răspunsuri aici.

i. Există un al doilea PDU de o culoare diferită pe care E-Mail Client a pregătit-o să o trimită către MultiServer. Acesta este începutul comunicării prin e-mail. Se va face clic pe acest al doilea plic PDU și se selectează Outbound PDU Details.

Întrebări:

Cum diferă porturile și numerele de secvență față de cele două PDU-uri anterioare?

Răspunsuri aici.

Ce protocol de e-mail este asociat cu portul TCP 25?

Ce protocol este asociat cu portul TCP 110?

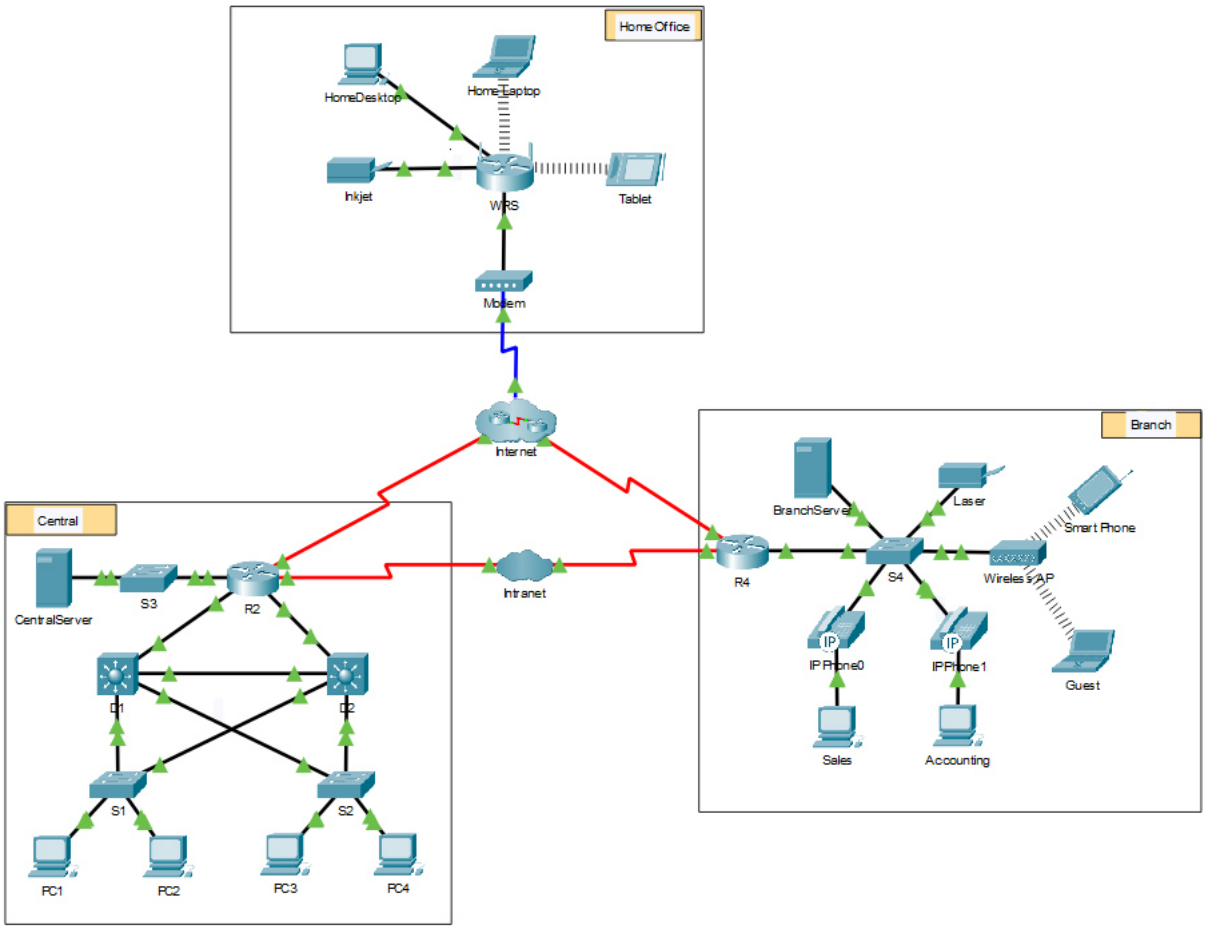
LABORATOR 10. APLICAȚII

EXERCIȚIUL 1. Servere DHCP și DNS.

Obiective

Partea 1: Se va configura adresa IPv4 statică.

Partea 2: Se configuta serviciul DNS și vor verifica înregistrările DNS.



Partea 1: Se va configura adresa IPv4 statică.

Pasul 1: Se va configura imprimanta cu jet de cerneală cu adresa IPv4 statică.

Calculatoarele de la biroul de casă trebuie să cunoască adresa IPv4 a imprimantei pentru a-i trimite informații. Prin urmare, imprimanta trebuie să utilizeze o adresă IPv4 statică (nu se schimbă).

a. Se va face clic pe Inkjet și pe fila Configurare, care afișează Setările globale.

b. Va fi atribuită adresa statică pentru Default Gateway ca 192.168.0.1 și adresa serverului DNS ca 64.100.8.8.

c. Se va face clic pe FastEthernet0 și se va atribui static adresa IP ca 192.168.0.2 și adresa Subnet Mask ca 255.255.255.0.

d. Se va închide fereastra Inkjet.

Pasul 2: Se va configura WRS pentru a furniza servicii DHCP.

a. Se va face clic pe WRS și pe fila GUI și să maximizeze fereastra.

b. Se afișează, implicit, fereastra Configurare de bază. Se vor configura următoarele setări în secțiunea Configurare rețea:

1) Se va schimba adresa IP la 192.168.0.1.

2) Va fi setată Masca de subrețea la 255.255.255.0.

3) Va fi activat serverul DHCP.

4) Va fi setată adresa Statică, DNS 1 la 64.100.8.8.

5) Se va derula în partea de jos și se va face clic pe Salvare.

c. Se va închide fereastra WRS.

Pasul 3: Se va solicita adresare DHCP pentru laptopul de casă.

Această activitate se concentrează pe biroul de casă. Clienții care vor fi configurați cu DHCP sunt Home Laptop și Tablet.

a. Se va face clic pe Home Laptop și pe fila Desktop > IP Configuration.

b. Se va face clic pe DHCP și se așteaptă până când solicitarea DHCP are succes.

c. Laptopul de casă ar trebui să aibă acum o configurație IP completă. Dacă nu, se va reveni la Pasul 2 și se vor verifica configurațiile pe WRS.

d. Se va închide fereastra Configurare IP și apoi se va închide fereastra Laptop de casă.

Pasul 4: Se va solicita adresare DHCP pentru tabletă.

a. Se va face clic pe Tabletă și pe fila Desktop > Configurare IP.

b. Se va face clic pe DHCP și se așteaptă până când solicitarea DHCP are succes.

c. Tableta ar trebui să aibă acum o configurație IP completă. Dacă nu, se va reveni la Pasul 2 și se vor verifica configurațiile pe WRS.

Pasul 5: Va fi testat accesul la site-uri web.

a. Se va închide fereastra Configurare IP și apoi se va face clic pe Browser web.

b. În caseta URL, va fi introdusă adresa 10.10.10.2 (pentru site-ul CentralServer) sau 64.100.200.1 (pentru site-ul BranchServer) și se va face clic pe Go. Ar trebui să apară ambele site-uri.

c. Se va redeschide browserul web. Vor fi testate numele pentru aceleași site-uri web introducând centralserver.pt.pka și ranchserver.pt.pka. Se va face clic pe Fast Forward Time din bara galbenă de sub topologie pentru a accelera procesul.

Partea 2: Înregistrările vor fi configurate pe serverul DNS

Pasul 1: Va fi configurat famous.dns.pka cu înregistrări pentru CentralServer și BranchServer.

De obicei, înregistrările DNS sunt înregistrate la companii, dar în scopul acestei activități va fi controlat serverul famous.dns.pka de pe Internet.

a. Se va face clic pe cloud de Internet. Se afișează o nouă rețea.

b. Se va face clic pe famous.dns.pka și pe fila Servicii > DNS.

c. Se vor adăuga următoarele înregistrări de resurse:

Resource Record Name	Ipv4 Address
centralserver.pt.pka	10.10.10.2
branchserver.pt.pka	64.100.200.1

d. Fereastra famous.dns.pka va fi închisă.

e. Se va face clic pe Back pentru a ieși din cloud-ul de internet.

Pasul 2: Se va verifica capacitatea computerelor client de a utiliza DNS.

Acum că am configurat înregistrările DNS, laptopul și tableta de casă ar trebui să poată accesa site-urile web folosind numele în loc de adresele IP. În primul rând, se va verifica dacă clientul DNS funcționează corect și apoi se verifică accesul la site.

a. Se va face clic pe Home Laptop sau Tabletă.

b. Dacă browserul web este deschis, va fi închis și va fi selectat Command Prompt.

Se va verifica adresa IPv4 prin introducerea comenzii ***ipconfig /all***. Ar trebui să se vadă adresa IP a serverului DNS.

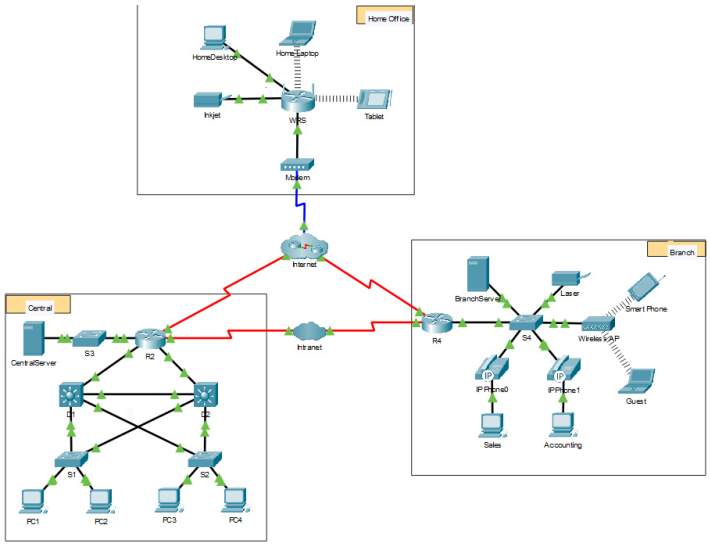
c. Se va da Ping la serverul DNS la cu adresa ipv4 64.100.8.8 pentru a verifica conectivitatea.

Notă: Primele două sau trei ping-uri pot eșua, deoarece Packet Tracer simulează toate procesele diferite care trebuie să aibă loc pentru o conexiune de succes la o resursă de la distanță.

Se va testa funcționalitatea serverului DNS prin introducerea comenzilor ***nslookup centralserver.pt.pka*** și ***nslookup branchserver.pt.pka***. Ar trebui să se obțină o rezoluție de nume care să arate adresa IP pentru fiecare.

d. Se va închide fereastra Prompt de comandă și se va face clic pe Browser web. Se va verifica dacă Home Laptop sau Tableta pot accesa acum paginile web pentru CentralServer și BranchServer.

EXERCIȚIUL 2. Serviciile de WEB și E-MAIL.



Partea 1: Vor fi configurate și vor fi verificate Serviciile Web

Pasul 1: Vor fi configurate serviciile web pe CentralServer și BranchServer.

a. Se va face clic pe CentralServer și pe fila Servicii > HTTP.

b. Se va face clic pe On pentru a activa HTTP și HTTP Secure (HTTPS).

c. Opțional. Se va personaliza codul HTML.

d. Se va repeta Pasul 1a – 1c pe BranchServer.

Pasul 2: Se vor verifica serverele web accesând paginile web.

Există multe dispozitive terminale în această rețea, dar în scopul acestui pas, se va folosi PC3.

a. Se va face clic pe PC3 și pe fila Desktop > Browser web.

b. În caseta URL, se va introduce 10.10.10.2 ca adresă IP și se va face clic pe Go. Se afișează site-ul web CentralServer.

c. În caseta URL, se va introduce 64.100.200.1 ca adresă IP și se va face clic pe Go. Se afișează site-ul web BranchServer.

d. În caseta URL, se va introduce centralserver.pt.pka și se va face clic pe Go. Se afișează site-ul web CentralServer.

e. În caseta URL, se va introduce branchserver.pt.pka și se va face clic pe Go. Se afișează site-ul web BranchServer.

f. Ce protocol translatează numele centralserver.pt.pka și branchserver.pt.pka în adrese IP?

Partea 2: Vor fi configurate și vor fi verificate Serviciile de e-mail pe servere.

Pasul 1: Va fi configurat CentralServer pentru a trimite (SMTP) și a primi (POP3) e-mail.

a. Se va face clic pe CentralServer, apoi se va selecta fila Servicii urmată de butonul E-MAIL.

b. Se va face clic pe On pentru a activa SMTP și POP3.

c. Va fi setat numele de domeniu la centralserver.pt.pka și se va face clic pe Set.

d. Va fi creat un utilizator numit central-user cu parola cisco. Se va face clic pe + pentru a adăuga utilizatorul.

Pasul 2: BranchServer va fi configurat pentru a trimite (SMTP) și a primi (POP3) e-mail.

a. Se va face clic pe BranchServer și pe fila Servicii > EMAIL.

b. Se va face clic pe On pentru a activa SMTP și POP3.

c. Numele de domeniu va fi setat la branchserver.pt.pka și se va face clic pe Set.

d. Va fi creat un utilizator numit branch-user cu parola cisco. Se va face clic pe + pentru a adăuga utilizatorul.

Pasul 3: Se va configura PC3 pentru a utiliza serviciul de e-mail CentralServer.

a. Se va face clic pe PC3 și pe fila Desktop > E-mail.

b. Se vor introduce următoarele valori în câmpurile respective:

1) Nume: Utilizator central

2) Adresă de e-mail: central-user@centralserver.pt.pka

3) Server de e-mail de intrare: 10.10.10.2

4) Server de e-mail de ieșire: 10.10.10.2

5) Nume utilizator: central-user

6) Parola: cisco

c. Se va face clic pe Salvare. Va fi afișată fereastra Browser de e-mail.

d. Se va face clic pe Primire. Dacă totul a fost configurat corect atât pe client, cât și pe server, fereastra Browser de e-mail afișează mesajul de confirmare Receive Mail Success.

Pasul 4: Se vor configura dispozitivele Sales pentru a utiliza serviciul de e-mail al BranchServer.

a. Se va face clic pe Sales și apoi pe fila Desktop > E-mail.

b. Se vor introduce următoarele valori în câmpurile respective:

1) Nume: Utilizator sucursală

2) Adresă de e-mail: branch-user@branchserver.pt.pka

3) Server de e-mail de intrare: 172.16.0.3

4) Server de e-mail de ieșire: 172.16.0.3

5) Nume de utilizator: branch-user

6) Parola: cisco

c. Se va face clic pe Salvare. Va fi afișată fereastra browserului de e-mail.

d. Se va face clic pe Primire. Dacă totul a fost configurat corect atât pe client, cât și pe server, fereastra Browser de e-mail afișează mesajul de confirmare Receive Mail Success.

e. Nu se va închide fereastra de configurare a vânzărilor sau fereastra Browser de e-mail.

Pasul 5: Se va trimite un e-mail de la clientul de vânzări și clientul PC3.

a. Din fereastra Sales Mail Browser, se va face clic pe Compune.

b. Se vor introduce următoarele valori în câmpurile respective:

1) Către: central-user@centralserver.pt.pka

2) Subiect: Personalizarea liniei de subiect.

3) Corpul e-mailului: Personalizarea e-mailului.

c. Se va face clic pe Trimite.

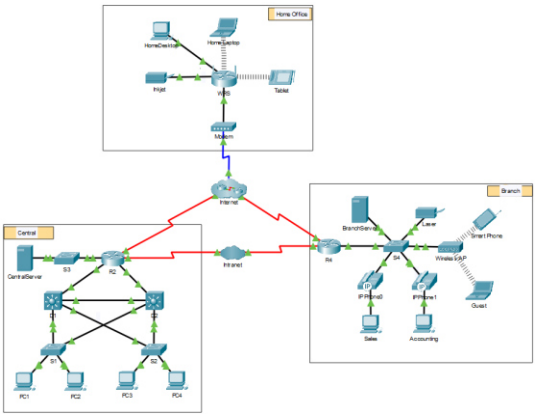
d. Se va verifica dacă PC3 a primit e-mailul. Se va face clic pe PC3. Dacă fereastra Browser de e-mail este închisă, se va face clic pe E-mail.

e. Se va face clic pe Primire. Se afișează un e-mail de la Sales. Se va face dublu clic pe e-mail.

f. Se va face clic pe Răspuns, se va personaliza un răspuns și se va face clic pe Trimite.

g. Se va verifica dacă Sales a primit răspunsul.

EXERCIȚIUL 3. Servere FTP.



Obiective

Partea 1: Se vor configura serviciile FTP pe servere.

Partea 2: Se va încărca un fișier pe serverul FTP.

Partea 3: Se va descărca un fișier de pe serverul FTP.

Partea 1: Se vor configura serviciile FTP pe servere.

Pasul 1: Se va configura serviciul FTP pe CentralServer.

a. Se va face clic pe CentralServer > fila Servicii > FTP.

b. Se va face clic pe On pentru a activa serviciul FTP.

c. În Configurare Utilizator, se vor crea următoarele conturi de utilizator, făcând clic pe Add pentru a adăuga contul:

Username	Password	Permissions
anonymous	anonymous	limited to Read and List
administrator	cisco	full permission

d. Se va face clic pe contul implicit de utilizator Cisco și se va face clic pe Remove pentru a-l șterge. Se va închide fereastra de configurare CentralServer.

Pasul 2: Se va configura serviciul FTP pe BranchServer.

Se va repeta Pasul 1 pe BranchServer.

Partea 2: Se va încărca un fișier pe serverul FTP

Pasul 1: Se va transfera fișierul README.txt de pe laptopul de acasă la CentralServer.

În calitate de administrator de rețea, va trebui să plaseze o notificare pe serverele FTP. Documentul a fost creat pe laptopul de acasă și trebuie încărcat pe serverele FTP.

a. Se va face clic pe Home Laptop și pe fila Desktop > Editor de text.

b. Se va deschide fișierul README.txt și se va revizui. Editorul de text va fi închis când va fi finalizată sarcina.

c. În fila Desktop, se va deschide fereastra Prompt de comandă și se vor efectua următorii pași:

1) Va fi tastat ***ftp centralserver.pt.pka***. Va fi așteptat câteva secunde în timp ce clientul se conectează.

Notă: Deoarece Packet Tracer este un sistem de simulare, poate dura până la 30 de secunde pentru ca FTP să se conecteze prima dată.

2) Serverul solicită un nume de utilizator și o parolă. Se vor folosi acreditările pentru contul de administrator.

3) Promptul se schimbă în ftp>. Se va lista conținutul directorului tastând ***dir***. Se afișează directorul de fișiere de pe CentralServer.

4) Se va transfera fișierul README.txt: la promptul ftp>, se va tasta ***put README.txt***. Fișierul README.txt este transferat de pe laptopul de casă la CentralServer.

5) Se va verifica transferul fișierului tastând dir. Fișierul README.txt este acum listat în directorul de fișiere.

6) Se va închide clientul FTP tastând ***quit***. Promtul va reveni la PC>.

Pasul 2: Se va transfera fișierul README.txt de pe laptopul de casă pe BranchServer.

a. Se va repeta Pasul 1c pentru a transfera fișierul README.txt pe branchserver.pt.pka.

b. Se vor închide ferestrele Prompt de comandă și, respectiv, Laptop casă.

Partea 3: Se va descărca un fișier de pe serverul FTP.

Pasul 1: Se va transfera ***asa842-k8.bin*** de la CentralServer la PC2.

a. Se va face clic pe PC2 și pe fila Desktop > Linie de comandă.

1) Se va tasta ***ftp centralserver.pt.pka***.

2) Serverul solicită un nume de utilizator și o parolă. Se vor folosi acreditările pentru contul anonim.

3) Promptul se schimbă în ftp>. Se va lista conținutul directorului tastând ***dir***. Fișierul ***asa842-k8.bin*** este listat în partea de sus a listei de directoare.

4) Se descarcă fișierul ***asa842-k8.bin***: la promptul ftp>,se va tasta ***get asa842-k8.bin***. Fișierul asa842-k8.bin este transferat pe PC2.

5) Se va verifica dacă contul anonim nu are permisiunea de a scrie fișiere pe CentralServer tastând ***put asa842-k8.bin***. Se afișează următorul mesaj de eroare:

Writing file ***asa842-k8.bin*** to centralserver.pt.pka:
File transfer in progress...
%Error ftp://centralserver.pt.pka/ ***asa842-k8.bin*** (No such file or directory Or Permission denied)
550-Requested action not taken. permission denied).

6) Se va închide clientul FTP tastând ***quit***. Promptul revine la promptul PC>.

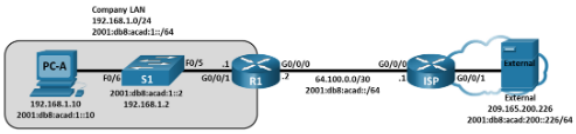
7) Se va verifica transferul fișierului pe PC2 tastând dir. ***asa842-k8.bin*** este listat în director.

8) Se va închide fereastra liniei de comandă.

Pasul 2: Se va transfera fișierul ***asa842-k8.bin*** de pe BranchServer pe Smart Phone.

Se va repeta Pasul 1 pentru Smart Phone, cu excepția descărcarii fișierului ***asa842-k8.bin*** de pe branchserver.pt.pka.

Exercițiul 4. Folosirea Utilitarelor PING și TraceRoute pentru a Testa Conectivitatea Rețelei.



Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/0	64.100.0.2 /30	N/A
		2001:db8:acad::2 /64	
		fe80::2	
	G0/0/1	192.168.1.1 /24	
		2001:db8:acad:1::1 /64	
		fe80::1	
ISP	G0/0/0	64.100.0.1 /30	N/A
		2001:db8:acad::1 /64	
		fe80::1	
	G0/0/1	209.165.200.225 /27	
		2001:db8:acad:200::225 /64	
		fe80::225	
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
		2001:db8:acad:1::2 /64	fe80::1
		fe80::2	
PC-A	NIC	2001:db8:acad:1::10 /64	fe80::1
		192.168.1.10 /24	192.168.1.1
External	NIC	209.165.200.226 /27	209.165.200.225
		2001:db8:acad:200::226 /64	fe80::225

Obiective

Partea 1: Se va folosi comanda Ping pentru testarea de bază a rețelei.

Partea 2: Se vor folosi comenzile Tracert și Traceroute pentru testarea de bază a rețelei.

Partea 3: Se va depana topologia.

Instrucțiuni

Partea 1: Se va folosi comanda Ping pentru testarea de bază a rețelei.

În această parte a activității, se va folosi comanda ping pentru a verifica conectivitatea de la end-la-end. Ping funcționează prin trimiterea de pachete de solicitare ecou ICMP (Internet Control Message Protocol) către gazda țintă și apoi așteptând un răspuns ICMP. Poate înregistra timpul dus-întors și orice pierdere de pachete sau bucle de rutare.

Pachetele IP au o durată de viață limitată în rețea. Pachetele IPv4 folosesc un Time to Live (TTL) de 8 biți. Pachetele IPv6 folosesc o valoare de câmp pentru antetul Hop Limit. TTL și Hop Limit specifică numărul maxim de hop-uri Layer 3 care pot fi parcurse pe calea către destinație. Fiecare gazdă dintr-o rețea va seta valoarea de 8 biți cu o valoare maximă de 255.

De fiecare dată când un pachet IP ajunge la un dispozitiv de rețea de nivel 3, această valoare este redusă cu unu înainte de a fi redirecționat către destinație. Dacă această valoare ajunge în cele din urmă la zero înainte de a ajunge la destinație, pachetul IP este aruncat.

Vor fi examinate rezultatele comenzii ping și opțiunile suplimentare de ping care sunt disponibile în computerele Packet Tracer și dispozitivele Cisco.

Pasul 1: Se va testa conectivitatea la rețea la R1 folosind PC-A gazdă.

Toate ping-urile de la PC-A la alte dispozitive din topologie ar trebui să aibă succes. Dacă nu sunt, se vor verifica topologia și cablarea, precum și configurația dispozitivelor Cisco și a PC-urilor.

a. De la PC-A, se va da ping gateway-ul implicit folosind adresa IPv4 (interfața GigabitEthernet 0/0/1 a R1).

```
C:\> ping 192.168.1.1
 Pinging 192.168.1.1 with 32 bytes of data:
 Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

În acest exemplu, au fost trimise patru cereri ICMP care au 32 de octeți fiecare. Răspunsurile au fost primite în mai puțin de o milisecundă, fără pierderi de pachete. Timpul de transmisie și răspuns poate crește pe măsură ce cererile și răspunsurile ICMP sunt procesate de mai multe dispozitive în timpul călătoriei către și de la destinație.

Acest lucru se poate face și folosind adresa IPv6 a gateway-ului implicit (interfața GigabitEthernet 0/0/1 a R1).

```
C:\> ping 2001:db8:acad:1::1
 Pinging 2001:db8:acad:1::1 with 32 bytes of data:
 Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
 Ping statistics for 2001:DB8:ACAD:1::1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

De la PC-A, se va da ping la adresele enumerate în tabelul următor și se va înregistra timpul mediu dus-întors și IPv4 TTL, sau IPv6 Hop Limit.

Destination	Average Round Trip Time (ms)	TTL / Hop Limit
192.168.1.10		
2001:db8:acad:1::10		
192.168.1.1 (R1)		
2001:db8:acad:1::1 (R1)		
192.168.1.2 (S1)		
2001:db8:acad:1::2(S1)		
64.100.0.2 (R1)		
2001:db8:acad::2 (R1)		

Destination	Average Round Trip Time (ms)	TTL / Hop Limit
64.100.0.1 (ISP)		
2001:db8:acad::1 (ISP)		
209.165.200.225 (ISP G0/0/1)		
2001:db8:acad:200::225 (ISP G0/0/1)		
209.165.200.226 (External)		
2001:db8:acad:200::226 (External)		

Pasul 2: Se vor efectua ping-uri de la S1 la Extern.

De la S1, se va încerca să ping la ISP și la Extern folosind adrese IPv4 și IPv6.

Întrebare:

Care sunt rezultatele ping-ului de la S1 la ISP și Extern?

Partea 2: Se vor folosi comenzile Tracert și Traceroute pentru testarea de bază a rețelei.

Comenzile pentru trasarea rutelor pot fi găsite pe computere și dispozitive de rețea. Pentru un computer bazat pe Windows, comanda tracert folosește mesaje ICMP pentru a urmări calea către destinație. Comanda traceroute folosește datagramele UDP (User Datagram Protocol) pentru a urmări rutele către destinație pentru dispozitivele Cisco și alte PC-uri asemănătoare Unix.

În această parte, se vor examina comenzile traceroute și se vor determina calea pe care o parcurge un pachet către destinație. Se va utiliza comanda tracert de pe computere și comanda traceroute de pe dispozitivele Cisco. Se vor examina, de asemenea, opțiunile disponibile pentru reglarea fină a rezultatelor traceroute.

Pasul 1: La hostul PC-A, se va folosi comanda tracert spre Extern.

a. La promptul de comandă al PC-A, va fi tastat ***tracert 209.165.200.226***.

C:\> tracert 209.165.200.226

Tracing route to 209.165.200.226 over a maximum of 30 hops:

1 * * 1 ms 192.168.1.1

2 * 0 ms 0 ms 64.100.0.1

3 0 ms * 0 ms 64.100.0.1

4 * 11 ms * Request timed out.

5 0 ms * 0 ms 64.100.0.1

C:\>

Notă: Se poate opri trace route apăsând combinația de taste Ctrl-C.

Rezultatul tracert indică că există calea de la PC-A la Extern cu legătură de la PC-A la R1 la ISP, sar nu poate ajunge la Extern. Rezultatele tracert indică o problemă la routerul ISP.

b. Se va repeta comanda tracert folosind adresa IPv6. La promptul de comandă, va fi introdus ***tracert 2001:db8:acad:200::226***.

Se va închide promptul de comandă.

Pasul 2: La S1, se va folosi comanda traceroute către Extern.

Din S1, va fi tastat ***traceroute 209.165.200.226*** sau ***traceroute 2001:db8:acad:200::226***.

S1# **traceroute 209.165.200.226**

Partea 3: Problema de conectivitate la rețea va fi corectată la ISP.

Pasul 1: Va fi accesată locația de rețea în care apare problema de conectivitate.

Din pașii anteriori, s-a stabilit că există o problemă la routerul ISP folosind comenzile ping și traceroute. Se poate avea acces SSH de la distanță la toate dispozitivele din rețea folosind numele de utilizator ***admin*** și parola ***class***.

Se va deschide promptul de comandă.

a. De la terminalul S1, se va utiliza SSH în routerul ISP folosind interfața G0/0/0 pentru a corecta problema.

C:\> ssh -l admin 64.100.0.1

b. Se vor folosi comenzile show pentru a examina configurațiile de rulare pentru routerul ISP.

Ieșirile comenzilor ***show run*** și ***show ip interface brief*** indică faptul că interfața GigabitEthernet 0/0/1 este up/up, dar este configurată cu o adresă IP incorectă.

c. Vor fi corectate problemele constatate. Din promptul de comandă de pe PC-A, va fi inserată următoarea configurație în routerul ISP pentru a corecta problema din sesiunea SSH pe routerul ISP.

configure terminal

interface g0/0/1

no ip address 192.168.8.1 255.255.255.0

ip address 209.165.200.225 255.255.255.224

no ipv6 address 2001:db8:acad:201::225/64

ipv6 address 2001:db8:acad:200::225/64

ipv6 address fe80::225 link-local

no shutdown

d. Se va ieși din sesiunea SSH când sunt terminate comenzile.

Va fi închis promptul de comandă.

Pasul 2: Se va verifica conectivitatea end-to-end.

Din promptul de comandă PC-A, se vor utiliza comenzile ping și tracert pentru a verifica conectivitatea end-to-end la serverul extern la 209.165.200.226 și 2001:db8:acad:200::226.

Partea 4: Se vor folosi comenzile Ping extinse

Pasul 1: Se vor folosi comenzi ping extinse pe PC-A. Comanda implicită ping trimite patru cereri de 32 de octeți fiecare. Așteaptă 4.000 de milisecunde (4 secunde) pentru ca fiecare răspuns să fie returnat înainte de a afișa mesajul "Request timed out". Comanda ping poate fi reglată fin pentru depanarea unei rețele.

Se va deschide promptul de comandă.

a. La promptul de comandă, se va tasta ping și se va apăsa Enter.

C:\> ping

b. Folosind opțiunea ***ping -t***, se va da ping la Extern pentru a verifica dacă Externul este accesibil. Opțiunea -t va trimite continuu ping la țintă până la oprire. Se va folosi Ctrl+c pentru a opri secvența ping.

C:\> **ping –t 209.165.200.226**

Pentru a ilustra rezultatele când o gazdă nu este accesibilă, interfața GigabitEthernet 0/0/1 de pe routerul ISP va fi oprită. De la comutatorul S1, se va folosi SSH la interfața ISP G0/0/0. Se va utiliza parola ***class***.

S1# **ssh -l admin 64.100.0.1**

d. Se va folosi comanda de închidere pentru a dezactiva interfața GigabitEthernet 0/0/1 pe routerul ISP.

În timp ce rețeaua funcționează corect, comanda ping poate determina dacă destinația a răspuns și cât timp a durat să primească un răspuns de la destinație. Dacă există o problemă de conectivitate la rețea, comanda ping afișează un mesaj de eroare.

e. Va fi reactivată interfața GigabitEthernet 0/0/1 pe routerul ISP (folosind comanda ***no shutdown***) înainte de a trece la pasul următor. După aproximativ 30 de secunde, ping-ul ar trebui să aibă succes din nou.

f. Se va apăsa Ctrl+c pentru a opri comanda ping.

g. Pașii de mai sus pot fi repetați pentru adresa IPv6 pentru a obține un mesaj de eroare ICMP.

Întrebare:*Ce mesaje de eroare ICMP au fost primite?*

h. Se va activa interfața GigabitEthernet 0/0/1 pe routerul ISP (folosind comanda no shutdown) înainte de a trece la pasul următor. După aproximativ 30 de secunde, ping-ul ar trebui să aibă succes din nou.

Va fi închis promptul de comandă.

Pasul 2: Se va testa conectivitatea la rețea de la rețeaua R1 folosind dispozitive Cisco.

Comanda ping este disponibilă și pe dispozitivele Cisco. În acest pas, comanda ping este examinată folosind R1 și S1.

a. De la R1, se va da ping la Extern, pe rețeaua externă, folosind adresa IP 209.165.200.226.

```
R1# ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Semnul de exclamare (!) indică faptul că ping-ul a avut succes de la R1 la Extern. Călătoria dus-întors durează în medie 1 ms fără pierderi de pachete, așa cum indică o rată de succes de 100%.

b. Deoarece o tabelă gazdă locală a fost configurată pe R1, se poate face ping la Externalv4 pe rețeaua externă folosind numele de gazdă configurat din R1.

```
R1# ping Externalv4
```

Care este adresa IP folosită?

c. În modul EXEC privilegiat, există mai multe opțiuni disponibile pentru comanda ping. La linia de comandă se va tasta ping și se va apăsa Enter. Se va folosi ipv6 ca protocol. Va fi introdus 2001:db8:acad:200::226 sau extern pentru adresa IPv6 țintă. Se va apăsa Enter pentru a accepta valoarea implicită pentru alte opțiuni.

```
R1# ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:db8:acad:200::226
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:200::226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

d. Se poate folosi un ping extins pentru a observa unde există o problemă de rețea. Va fi dată comanda ping la 209.165.200.226 cu un număr de repetări de 50000. Apoi, va fi oprită interfața GigabitEthernet 0/0/1 de pe routerul ISP.

De la sesiunea SSH la ISP pe comutatorul S1, va fi dezactivată interfața GigabitEthernet 0/0/1 pe ISP.

e. Din sesiunea SSH, va fi activată interfața GigabitEthernet 0/0/1 pe ISP după ce semnele de exclamare (!) au fost înlocuite cu litera U și puncte (.). După aproximativ 30 de secunde, ping-ul ar trebui să aibă succes din nou. Se va apăsa Ctrl+Shift+6 pentru a opri comanda ping.

R1# ping

Protocol [ip]:

```
Target IP address: 209.165.200.226

Repeat count [5]: 50000

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]:

Sweep range of sizes [n]:

Sending 500, 100-byte ICMP Echos to 209.165.200.226, timeout is 2
seconds:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

<output omitted>

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
U.U.U.

U.U...............!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

<output omitted>

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!

Success rate is 99 percent (9970/10000), round-trip min/avg/max =
1/1/10 ms
```

Litera U din rezultate indică faptul că o destinație este inaccesibilă. R1 a primit o eroare PDU. Fiecare punct (.) din ieșire indică faptul că ping-ul a expirat în timp ce se aștepta un răspuns de la Extern. În acest exemplu, 1% din pachete s-au pierdut în timpul întreruperii rețelei simulate.

Fereastra de configurare va fi închisă.

Comanda ping este extrem de utilă atunci când se dorește depanarea conectivității la rețea. Cu toate acestea, ping-ul nu poate indica

locația unei probleme atunci când un ping nu are succes. Comanda tracert (sau traceroute) poate afișa informații despre latența și calea rețelei.

LABORATORUL 11. Proiectarea și Construirea unei Rețele Mici

EXERCIȚIUL 1. Construirea unei Rețele.

Obiective

Explicarea modului în care este creată, configurată și verificată o rețea mică de segmente conectate direct.

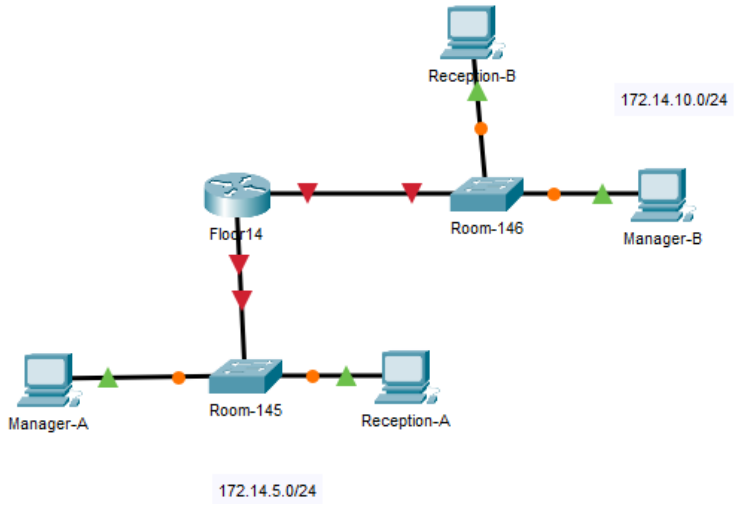
În această activitate Packet Tracer Physical Mode (PTPM), se va proiecta și construi o rețea de la zero. Designul trebuie să includă cel puțin un router Cisco 4321, două switch-uri Cisco 2960 și două PC-uri. Rețeaua va fi configurată complet și va fi utilizată cu IPv4/IPv6 (subrețea trebuie inclusă ca parte a schemei de adresare). Se va verifica rețeaua folosind cel puțin cinci comenzi show. Rețeaua va fi securizată folosind SSH, parole securizate și parole pentru consolă (minimum).

Întrebări de reflecție

1. Care este cea mai dificilă parte a acestei activități?

2. Documentația rețelei este atât de importantă pentru această activitate și în lumea reală?

EXERCIȚIUL 2. Provocarea de Integrare a Cunoștințelor Dobândite.



Obiective

Partea 1. Se va finaliza documentația de rețea.

Partea 2. Se vor efectua configurații de bază ale dispozitivului pe un router și un switch.

Partea 3. Se va verifica conectivitatea și se va rezolva orice problemă.

Device	Interface	IP Address	Subnet Mask	Default Gateway
Floor14	G0/0	172.14.5.1	255.255.255.0	N/A
	G0/1	172.14.10.1	255.255.255.0	N/A
Room-145	VLAN 1	172.14.5.35	255.255.255.0	
Room-146	VLAN 1	172.14.10.35	255.255.255.0	
Manager-A	NIC	172.14.5.50	255.255.255.0	
Reception-A	NIC	172.14.5.60	255.255.255.0	
Manager-B	NIC	172.14.10.50	255.255.255.0	
Reception-B	NIC	172.14.10.60	255.255.255.0	

Cerințe

· Vor fi furnizate informațiile lipsă în Tabelul de Adresări.

· Se va da numele routerului Floor14 iar pentru al doilea comutator Room-146. Nu se va putea accesa Camera-145.

· Se va folosi cisco ca parolă EXEC de utilizator pentru toate liniile.

· Se va folosi class ca parolă EXEC privilegiată.

· Vor fi criptate toate parolele text simplu.

· Vor fi configurate un bannere adecvate.

· Se va configura adresarea pentru toate dispozitivele conform Tabelului de Adresări.

· Se vor documenta interfețe cu descrieri, inclusiv interfața Room-146 VLAN 1.

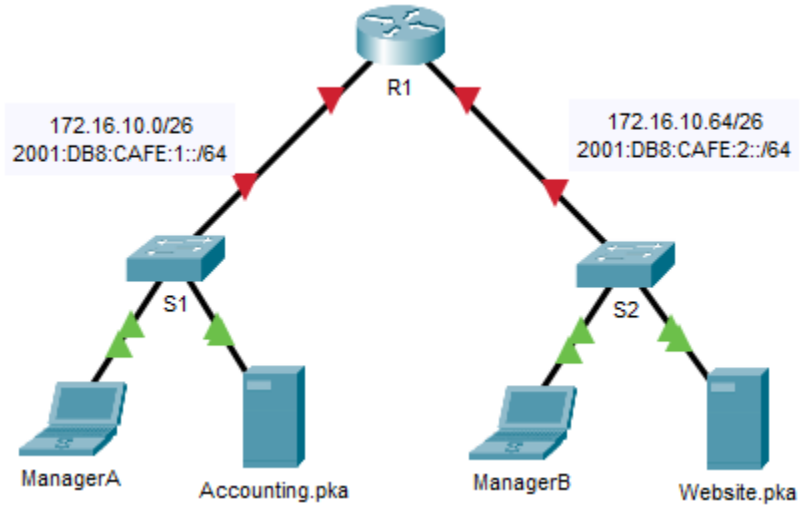
· Se vor salva configurațiile.

· Se va verifica conectivitatea între toate dispozitivele. Toate dispozitivele ar trebui să poată trimite ping la orice alt dispozitiv.

· Trebuie să se depaneze și să se documenteze orice probleme.

· Se vor implementa soluțiile necesare pentru a activa și a verifica conectivitatea completă end-to-end.

EXERCIȚIUL 3. Provocarea de Integrare a Cunoștințelor Dobândite.



Device	Interface	IPv4 Address / IPv6 Address/Prefix	Subnet Mask	Default Gateway
R1	G0/0	172.16.10.1	255.255.255.192	N/A
		2001:DB8:CAFE:1::1/64		N/A
	G0/1	172.16.10.65	255.255.255.192	N/A
		2001:DB8:CAFE:2::1/64		N/A
	Link-local	FE80::1		N/A
S1	VLAN1	172.16.10.62	255.255.255.192	172.16.10.1
S2	VLAN1	172.16.10.126	255.255.255.192	172.16.10.65
ManagerA	NIC	172.16.10.3	255.255.255.192	
		2001:DB8:CAFE:1::3/64		
Accounting.pka	NIC	172.16.10.2	255.255.255.192	
		2001:DB8:CAFE:1::2/64		
ManagerB	NIC	172.16.10.67	255.255.255.192	
		2001:DB8:CAFE:2::3/64		
Website.pka	NIC	172.16.10.66	255.255.255.192	
		2001:DB8:CAFE:2::2/64		

Cerințe

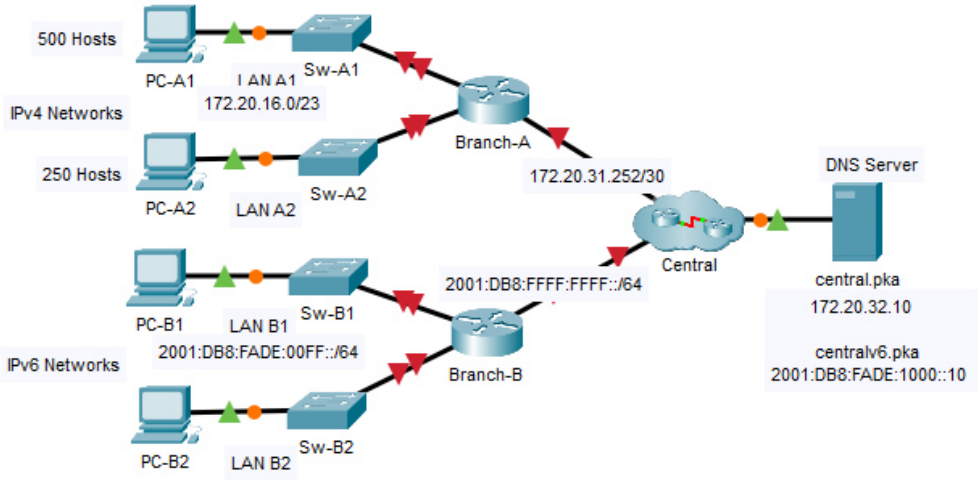
- Se va completa documentația tabelului de adrese.
- Se va configura R1 cu adresare IPv4 și IPv6.

· Se va configura S1 cu adresare IPv4.

· Se va configura ManagerA cu adresare IPv4 și IPv6. Restul clienților sunt deja configurați.

· Se va verifica conectivitatea. Toți clienții ar trebui să poată să facă ping reciproc și să acceseze site-urile web de pe Accounting.pka și Website.pka.

EXERCIȚIUL 4. Provocarea de Integrare a Cunoștințelor Dobândite.



Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
		IPv6 Address/Prefix		
Branch-A	G0/0			N/A
	G0/1			N/A
	G0/2	172.20.31.254	255.255.255.252	N/A
Branch-B	G0/0			N/A
	G0/1			N/A
	G0/2	2001:DB8:FFFF:FFFF::2/64		N/A
PC-A1	NIC			
PC-A2	NIC			
PC-B1	NIC			
PC-B2	NIC			

Cerințe

· Se vor configura setările inițiale pentru Branch-A și Branch-B, inclusiv numele gazdei, bannerul, liniile și parolele. Se va folosi

cisco ca parolă EXEC a utilizatorului și class ca parolă EXEC privilegiată. Se va cripta toate parolele.

· LAN A1 utilizează subrețeaua 172.20.16.0/23. Se va atribui următoarea subrețea disponibilă la LAN A2 pentru maximum 250 de gazde.

· LAN B1 utilizează subrețeaua 2001:DB8:FADE:00FF::/64. Va fi atribuită următoarea subrețea disponibilă la LAN B2.

· Se va termina de documentat schema de adresare în Tabelul de adrese, folosind următoarele îndrumări:

- Se va atribui prima adresă IP pentru LAN A1, LAN A2, LAN B1 și LAN B2 interfeței routerului.

- Pentru rețelele IPv4, se va atribui ultima adresă IPv4 computerelor.

- Pentru rețelele IPv6, va fi atribuită a 16-a adresă IPv6 computerelor.

· Se va configura adresarea routerelor conform documentatiei. Se va include o descriere adecvată pentru fiecare interfață de router. Branch-B folosește FE80::B ca adresă locală de legătură.

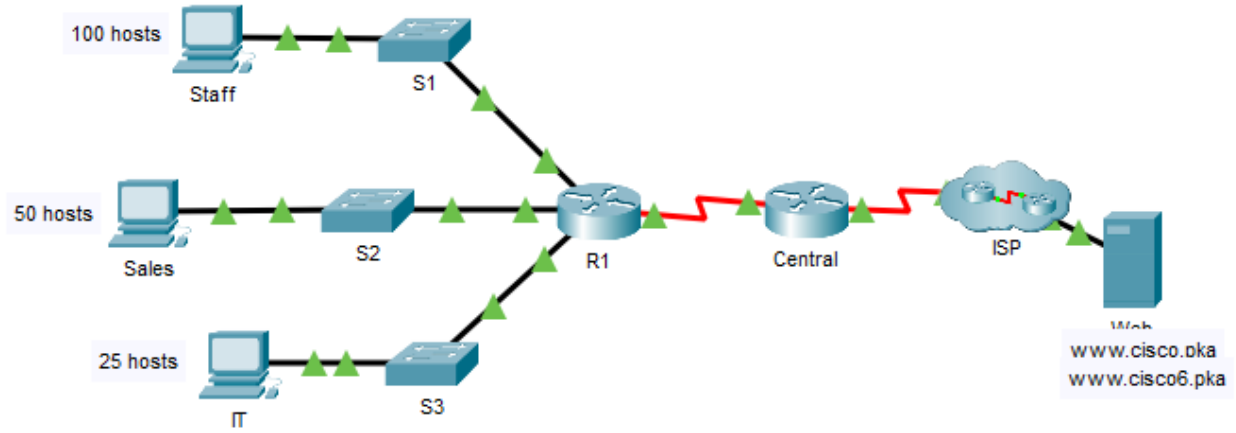
· Vor fi configurate PC-uri cu adresare conform documentației. Adresele serverului DNS pentru IPv4 și IPv6 sunt afișate în topologie.

· Se va verifica conectivitatea între PC-urile IPv4 și între PC-urile IPv6.

· Se va verifica dacă PC-urile IPv4 pot accesa pagina web la central.pka.

· Se va verifica dacă PC-urile IPv6 pot accesa pagina web la centralv6.pka.

EXERCIȚIUL 5. Provocarea de Integrare a Cunoștințelor Dobândite.



Device	Interface	IPv4 Address / IPv6 Address/Prefix	Subnet Mask / IPv6 Link-local	Default Gateway
R1	G0/0			N/A
		2001:DB8:ACAD::1/64	FE80::1	N/A
	G0/1			N/A
		2001:DB8:ACAD:1::1/64	FE80::1	N/A
	G0/2			N/A
		2001:DB8:ACAD:2::1/64	FE80::1	N/A
	S0/0/1	172.16.1.2	255.255.255.252	N/A
		2001:DB8:2::1/64	FE80::1	N/A
Central	S0/0/0	209.165.200.226	255.255.255.252	N/A
		2001:DB8:1::1/64	FE80::2	N/A
	S0/0/1	172.16.1.1	255.255.255.252	N/A
		2001:DB8:2::2/64	FE80::2	N/A
S1	VLAN 1			
S2	VLAN 1			
S3	VLAN 1			
Staff	NIC			

		2001:DB8:ACAD::2/64	FE80::2	FE80::1
Sales	NIC			
		2001:DB8:ACAD:1::2/64	FE80::2	FE80::1
IT	NIC			
		2001:DB8:ACAD:2::2/64	FE80::2	FE80::1
Web	NIC	64.100.0.3	255.255.255.248	64.100.0.1
		2001:DB8:CAFE::3/64	FE80::2	FE80::1

Cerințe

Adresare IPv4

· Se vor crea subrețele care îndeplinesc cerințele gazdei folosind 192.168.0.0/24.

o Staff: 100 gazde

o Sales: 50 gazde

o IT: 25 gazde

o Rețea de oaspeți care va fi adăugată mai târziu: 25 de gazde

· Vor fi documentate adresele IPv4 atribuite în Tabelul de Adresări.

· Se va înregistra subrețeaua pentru rețeaua pentru invitați:

Vor fi configurate PC-urile.

· Se vor configura adresa IPv4 atribuită, masca de subrețea și setările implicite ale gateway-ului pe PC-urile pentru Staff, Sales și IT folosind schema de adresare.

· Se va atribui IPv6 unicast și se va conecta adresele locale și gateway-ul implicit către rețelele ţStaffţ, ţSalesţ și IT conform Tabelului de Adresări.

R1 va fi configurat.

· Numele dispozitivului va fi configurat conform Tabelului de Adresări.

· Se va dezactiva căutarea DNS.

· Se va atribui Ciscoenpa55 ca parolă criptată pentru modul EXEC privilegiat.

· Se va atribui Ciscoconpa55 ca parolă pentru consolă și se va activa conectarea.

· Va fi necesar ca pentru toate parolele să fie utilizate minim 10 caractere.

· Vor fi criptate toate parolele text simplu.

· Se va crea un banner care avertizează pe oricine care accesează dispozitivul că accesul neautorizat este interzis. Se va asigura că va conține cuvântul Avertisment în banner.

· Se vor configura toate interfețele Gigabit Ethernet.

o Vor fi configurate adresele IPv4 conform schemei de adresare.

o Vor fi configurate adresele IPv6 conform Tabelului de Adresări.

· Se va configura SSH pe R1:

o Va fi setat numele de domeniu la CCNA-lab.com

o Va fi generată o cheie RSA de 2048 de biți.

o Se vor configura liniile VTY pentru acces SSH.

o Se vor folosi profilurile de utilizator locale pentru autentificare.

o Va fi creat un utilizator Admin1 cu un nivel de privilegii de 15 folosind parola criptată pentru Admin1pa55.

· Se va configura consola și liniile VTY pentru a se deconecta după cinci minute de inactivitate.

· Va fi blocat oricine timp de trei minute care nu reușește să se conecteze după patru încercări într-o perioadă de două minute.

Vor fi configurate Switch-uri.

· Numele dispozitivului va fi configurat conform Tabelului de Adresări.

· Se va configura interfața SVI cu adresa IPv4 și masca de subrețea conform schemei de adresare.

· Se va configura gateway-ul implicit.

· Se va dezactiva căutarea DNS.

· Se va atribui Ciscoenpa55 ca parolă criptată pentru modul EXEC privilegiat.

· Se va atribui Ciscoconpa55 ca parolă pentru consolă și se va activa conectarea.

· Se va configura consola și liniile VTY pentru a se deconecta după cinci minute de inactivitate.

· Vor fi criptate toate parolele text simplu.

Se va verifica conectivitatea

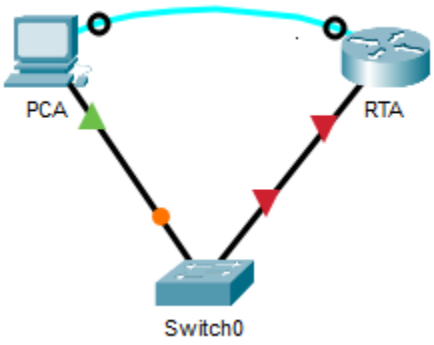
· Folosind browserul web de la Staff, Sales și PC-uri IT, va fi navigat la www.cisco.pka.

· Folosind browserul web de la Staff, Sales și PC-uri IT, va fi navigat la www.cisco6.pka.

· Toate PC-urile ar trebui să poată face ping la toate dispozitivele.

LABORATOR 12. Securizarea Dispozitivelor de Retea.

EXERCIȚIUL 1. Configurarea SSH și a parolelor securizate.



Tabel de Adresare

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0	192.168.10.1	255.255.255.0	N/A
PCA	NIC	192.168.10.2	255.255.255.0	192.168.10.1

Cerințe

· Configurarea adresei IP pe PCA conform Tabelului de Adresări.

· Conectare prin consolă la RTA de la Terminalul de pe PC-A.

· Configurarea adresei IP pe RTA și activarea interfeței.

· Configurarea numelui de gazdă ca RTA.

· Criptarea tuturor parolelor de text simplu în clar.

· Setarea unei parole secrete puternice, la fel ca în laboratoare.

· Setarea numelui de domeniu la RTA.com (se face distincția între majuscule și minuscule).

· Crearea unui utilizator de administrare cu o parolă puternică.

· Generarea de chei RSA pe 1024 de biți.

Notă: Se va reține că în Packet Tracer, va fi introdusă comanda crypto key generate rsa și se va apăsa Enter pentru a continua.

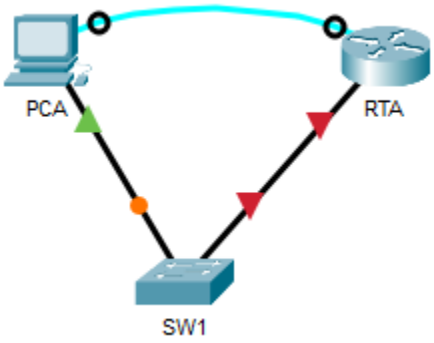
· Blocarea timp de trei minute a oricărei persoane care nu se conectează după patru încercări într-o perioadă de două minute.

· Configurarea liniilor VTY pentru acces SSH și utilizarea profilurilor locale de utilizator pentru autentificare.

· Salvarea configurației în NVRAM.

· În acest fel putem să demonstrăm că am stabilit accesul SSH de la PCA la RTA.

EXERCIȚIUL 2. Configurarea SSH și a parolelor securizate.



Tabel de Adresare

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0	172.16.1.1	255.255.255.0	N/A
PCA	NIC	172.16.1.10	255.255.255.0	172.16.1.1
SW1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1

Instrucțiuni

Pasul 1: Configurarea securității de bază pe router

Deschiderea unui prompt de comandă

a. Configurarea adresei IP pe PCA conform Tabelului de Adresări.

Închiderea unui prompt de comandă.

Deschiderea ferestrei de configurare.

b. Conectare prin consolă la RTA de la terminalul de pe PC-A.

c. Configurarea numelui de gazdă ca RTA.

d. Configurarea adresei IP pe RTA și activarea interfeței.

e. Criptarea tuturor parolelor text simplu.

f. Setarea lungimii minime a parolei la 10 caractere.

g. Setarea unei parole secrete puternice,așa cum se face în laboratoare.

h. Se dezactivează căutarea DNS.

i. Setarea numelui de domeniu la CCNA.com (se face distincția între majuscule și minuscule).

j. Crearea unui utilizator pentru administrare cu o parolă puternică criptată.

k. Se generează chei RSA pe n-biți.

Notă: Va trebui să ne amintim că în Packet Tracer, va fi introdusă comanda crypto key generate rsa și se va apăsa Enter pentru a continua.

Numele cheilor va fi: RTA.CCNA.com

Se va alege dimensiunea modulului cheie în intervalul de la 360 la 2048, dar punem valoare ca în laboratoare.

Câți biți în modulul [512]: 2048

l. Blocarea timp de trei minute a oricărei persoane care nu se conectează după patru încercări într-o perioadă de două minute.

m. Configurarea tuturor liniilor VTY pentru acces SSH și utilizarea profilurilor locale de utilizator pentru autentificare.

n. Setarea timpului de expirare a modului EXEC la 6 minute pe liniile VTY.

o. Salvarea configurației în NVRAM.

Se închide fereastra de configurare.

p. Accesarea promptului de comandă de pe desktopul PCA pentru a stabili o conexiune SSH la RTA.

Deschiderea unui prompt de comandă

Utilizare: ssh -l nume utilizator adresa IP țintă.

Pasul 2: Configurarea securității de bază pe switch

Configurarea comutatorului SW1 cu măsurile de securitate corespunzătoare. Se vor consulta pașii de configurare pe router dacă va fi nevoie de asistență suplimentară.

a. Se va conecta SW1 prin cablu de consolă și se selectează fila CLI, din terminal.

Deschiderea unei ferestre de configurare

b. Configurarea numelui de gazdă ca SW1.

c. Configurarea adresei IP pe SW1 VLAN1 și activarea interfeței.

d. Configurarea adresei gateway implicite.

e. Se vor dezactiva toate porturile de comutare neutilizate.

Notă.: Pe un comutator, este o bună practică de securitate să fie dezactivate porturile neutilizate. O metodă de a face acest lucru este pur și simplu să fie închis fiecare port cu comanda „shutdown”. Acest lucru ar necesita accesarea fiecărui port individual. Există o metodă de comandă rapidă pentru a face modificări la mai multe porturi simultan, utilizând comanda pentru toate interfețele.

f. Criptarea tuturor parolelor care sunt în text simplu.

g. Setarea unei parole secrete puternice, ca în laboratoare.

h. Se dezactivează căutarea DNS.

i. Setarea numelui de domeniu la CCNA.com (se face distincția între majuscule și minuscule).

j. Crearea unui utilizator pentru administrare cu o parolă puternică criptată.

k. Se generează chei RSA pe 2048 de biți.

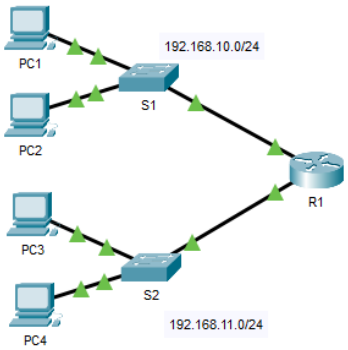
l. Configurarea tuturor liniilor VTY pentru acces SSH și utilizarea profilurilor locale de utilizator pentru autentificare.

m. Setarea timpului de expirare a modului EXEC la 16 minute pe toate liniile VTY.

n. Salvarea configurației în NVRAM.

LABORATOR 13. TROUBLESHOOTING.

EXERCIȚIUL 1. Depanarea problemelor cu Gateway-ul Implicit.



Tabel de Adresare.

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
S1	VLAN 1	192.168.10.2	255.255.255.0	
S2	VLAN 1	192.168.11.2	255.255.255.0	
PC1	NIC	192.168.10.10	255.255.255.0	
PC2	NIC	192.168.10.11	255.255.255.0	
PC3	NIC	192.168.11.10	255.255.255.0	
PC4	NIC	192.168.11.11	255.255.255.0	

Obiective

Partea 1: Verificarea documentației de rețea și izolarea problemelor

Partea 2: Implementarea, verificarea și documentarea soluțiilor.

INSTRUCȚIUNI

Partea 1: Verificarea documentației de rețea și izolarea problemelor. În partea 1 a acestei activități, se va completa documentația și se vor efectua teste de conectivitate pentru a descoperi probleme. În plus, se va determina o soluție adecvată pentru implementare în partea 2.

Pasul 1: Se va verifica documentația de rețea și se vor izola orice probleme.

a. Înainte de a putea testa în mod eficient o rețea, trebuie să existe o documentație completă. În Tabelul de Adresări se va observa că unele informații lipsesc. Va trebui completat Tabelul de adrese prin completarea informațiilor lipsă despre gateway implicite pentru switch-uri și PC-uri.

b. Se va testa conexiunea la dispozitivele din aceeași rețea. Izolând și corectând orice probleme de acces local, se va putea testa mai bine conectivitatea de la distanță, doar după ce este verificat faptul că există conectivitate locală și că aceasta este operațională.

Un plan de verificare poate fi la fel de simplu ca o listă de teste de conectivitate. Se vor folosi următoarele teste pentru a verifica conectivitatea locală și pentru a izola orice probleme de acces. Prima problemă este deja documentată, dar va trebui implementată și verificată soluția în timpul părții 2.

Documentație de testare și verificare.

Test	**Successful?**	**Issues**	**Solution**	**Verified**
PC1 to PC2	**No**	**IP address on PC1**	**Change PC1 IP address**	
PC1 to S1				
PC1 to R1				

Notă: Tabelul este un exemplu; trebuie să fie creat propriul document. Se poate folosi hârtie și creion pentru a desena un tabel sau se poate folosi un editor de text sau o foaie de calcul.

c. Se va testa conectivitatea la dispozitive la distanță (cum ar fi: ping de la PC1 la PC4) și se va documenta orice problemă. Aceasta este denumită frecvent conectivitate end-to-end. Aceasta înseamnă că toate dispozitivele dintr-o rețea au conectivitatea completă permisă de politica de rețea.

Notă: Este posibil ca testarea conectivității de la distanță să nu fie posibilă încă, deoarece va trebui mai întâi să se rezolve problemele de conectivitate locală. După ce vor fi rezolvate aceste probleme, se va reveni la acest pas și se va testa conectivitatea între rețele.

Pasul 2: Se va determina o soluție adecvată pentru problemă.

a. Folosind cunoștințele despre modul în care funcționează rețelele și abilitățile de configurare a dispozitivului, va fi căutată cauza problemei. De exemplu, S1 nu este cauza problemei de conectivitate între PC1 și PC2. Luminile de legătură sunt verzi și nicio configurație pe S1 nu ar face ca traficul să nu treacă între PC1 și PC2. Deci problema trebuie să fie cu PC1, PC2 sau ambele.

b. Se va verifica adresa dispozitivului pentru a se asigura că se potrivește cu documentația rețelei. De exemplu, adresa IP pentru PC1 este incorectă, așa cum a fost verificată cu comanda ipconfig.

c. Se va sugera o soluție gândită că va rezolva problema și va fi documentată. De exemplu, se va schimba adresa IP pentru PC1 pentru a se potrivi cu documentația.

Notă: Adesea există mai multe soluții. Cu toate acestea, implementarea și verificarea unei singure soluții la un moment dat este o bună practică de depanare. Implementarea mai multor soluții ar putea introduce probleme suplimentare într-un scenariu mai complex.

Partea 2: Implementarea, verificarea și documentarea soluțiilor

În Partea 2 a acestei activități, vor fi implementate soluțiile identificate în Partea 1. Se va verifica apoi soluția funcțională. Poate fi necesar să se revină la partea 1 pentru a termina izolarea tuturor problemelor.

Pasul 1: Se vor implementa soluții la problemele de conectivitate.

Se va consulta documentația din Partea 1. Se va alege prima problemă și se va implementa soluția sugerată. De exemplu, adresa IP de pe PC1 va fi corectă.

Pasul 2: Se va verifica dacă problema este acum rezolvată.

a. Se va verifica că soluția a rezolvat problema prin efectuarea testului utilizat pentru a identifica problema. *De exemplu, poate PC1 să dea acum ping la PC2?*

b. Dacă problema este rezolvată, acest lucru va fi indicat în documentație. De exemplu, în tabelul de mai sus, o simplă bifă ar fi suficientă în coloana „Verificat”.

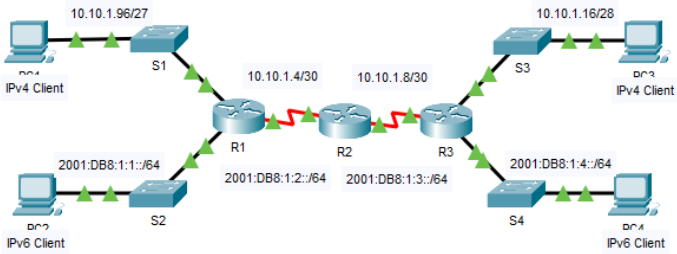
Pasul 3: Se va verifica dacă toate problemele sunt rezolvate.

a.Dacă în continuare este o problemă nerezolvată cu o soluție care nu a fost încă implementată, se va reveni la Partea 2, Pasul 1.

b. Dacă toate problemele curente sunt rezolvate, vor fi rezolvate și orice probleme de conectivitate la distanță (cum ar fi poate da PC1 ping la PC4)? Dacă răspunsul este nu, se va reveni la partea 1, pasul 1c pentru a testa conectivitatea de la distanță.

EXERCIȚIUL 2. Ping și Tracert pentru a testa calea.

Tabel de Adresare



Device	Interface	IPv4 Address / IPv6 Address/Prefix	Subnet Mask	Default Gateway
R1	G0/0	2001:DB8:1:1::1/64		N/A
	G0/1	10.10.1.97	255.255.255.224	N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:DB8:1:2::2/64		N/A
	Link-local	FE80::1		N/A
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:DB8:1:2::1/64		N/A
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:DB8:1:3::1/64		N/A
	Link-local	FE80::2		N/A
R3	G0/0	2001:DB8:1:4::1/64		N/A
	G0/1	10.10.1.17	255.255.255.240	N/A
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:DB8:1:3::2/64		N/A
	Link-local	FE80::3		N/A
PC1	NIC			
PC2	NIC			
PC3	NIC			
PC4	NIC			

Obiective

Partea 1: Testarea și restaurarea conectivității IPv4.

Partea 2: Testarea și restaurarea conectivității IPv6.

Partea 1: Testarea și restaurarea conectivității IPv4.

Pasul 1: Se va folosi ipconfig și ping pentru a verifica conectivitatea.

a. Se va face clic pe PC1 și pe fila Desktop > Prompt de comandă.

b. Se va introduce comanda ***ipconfig /all*** pentru a colecta informațiile IPv4. Va fi completat Tabelul de adrese cu adresa IPv4, masca de subrețea și gateway-ul implicit.

c. Se va face clic pe PC3 și pe fila Desktop > Command Prompt.

d. Se va introduce comanda ***ipconfig /all*** pentru a colecta informațiile IPv4. Va fi completat Tabelul de adrese cu adresa IPv4, masca de subrețea și gateway-ul implicit.

e. Conectivitate va fi testată între PC1 și PC3. Ping-ul ar trebui să eșueze.

Pasul 2: Se va localiza sursa eșecului de conectivitate.

a. De la PC1, va fi introdusă comanda necesară pentru a urmări traseul către PC3. *Care este ultima adresă IPv4 reușită la care a fost atinsă?*

b. Urmărirea se va încheia în cele din urmă după 30 de încercări. Se va combinația de taste ***Ctrl+C*** pentru a opri urmărirea înainte de 30 de încercări.

c. De la PC3, va fi introdusă comanda necesară pentru a urmări traseul către PC1. *Care este ultima adresă IPv4 reușită la care a fost atinsă?*

d. Se va introduce Ctrl+C pentru a opri urmărirea.

e. Se va face clic pe R1 și apoi pe fila CLI. Se va apăsa ENTER și se va face autentificare la router.

f. Se va introduce comanda ***show ip interface brief*** pentru a lista interfețele și starea acestora. Există două adrese IPv4 pe router. Unul ar fi trebuit să fie înregistrată în Pasul 2a. *Care este celălalt?*

g. Se va introduce comanda ***show ip route*** pentru a lista rețelele la care este conectat routerul. De reținut că există două rețele conectate la interfața Serial0/0/1. *Care sunt acestea?*

h. Se va repeta pasul 2e la 2g pentru R3 și se vor înregistra răspunsurile.

Se va observa cum se schimbă interfața serială pentru R3.

i. Vor fi efectuate mai multe teste dacă ajută la vizualizarea problemei. Modul de simulare este disponibil.

Pasul 3: Se va propune o soluție pentru a rezolva problema.

a. Se vor compara răspunsurile din Pasul 2 cu documentația disponibilă pentru rețea. *Care este eroarea?*

b. *Ce soluție s-ar propune pentru a corecta problema?*

Pasul 4: Implementarea planului.

Se va implementa soluția propusă în Pasul 3b.

Pasul 5: Se va verifica dacă conectivitatea este restabilită.

a. De la PC1 va fi testată conexiunea la PC3.

b. De la PC3 va fi testată conexiunea la PC1. Este problema rezolvată?

Pasul 6: Se va documenta soluția.

Partea 2: Testarea și restaurarea conectivității IPv6.

Pasul 1: Se va folosi ipv6config și ping pentru a verifica conectivitatea.

a. Se va face clic pe PC2 și pe fila Desktop > Command Prompt.

b. Se va introduce comanda ***ipv6config /all*** pentru a colecta informațiile IPv6. Va fi completat Tabelul de adrese cu adresa IPv6, prefixul de subrețea și gateway-ul implicit.

c. Se va face clic pe PC4 și pe fila Desktop > Command Prompt.

d. Se va introduce comanda ***ipv6config /all*** pentru a colecta informațiile IPv6. Va fi completat Tabelul de adrese cu adresa IPv6, prefixul de subrețea și gateway-ul implicit.

e. Conectivitate va fi testată între PC2 și PC4. Ping-ul ar trebui să eșueze.

Pasul 2: Se va localiza sursa eșecului de conectivitate.

a. De la PC2, se va introduce comanda necesară pentru a urmări traseul către PC4. *Care este ultima adresă IPv6 reușită la care a fost atinsă?*

b. Urmărirea se va încheia în cele din urmă după 30 de încercări.

c. De la PC4, va fi introdusă comanda necesară pentru a urmări traseul către PC2. *Care este ultima adresă IPv6 reușită la care a fost atinsă?*

d. Se va introduce Ctrl+C pentru a opri urmărirea.

e. Se va face clic pe R3 și apoi pe fila CLI. Se va apăsa ENTER și se va face autentificare la router.

f. Se va introduce comanda ***show ipv6 interface brief*** pentru a lista interfețele și starea acestora. Există două adrese IPv6 pe router. Una ar trebui să se potrivească cu adresa gateway-ului înregistrată la Pasul 1d. *Există o discrepanță?*

g. Vor fi efectuate mai multe teste dacă ajută la vizualizarea problemei. Modul de simulare este disponibil.

Pasul 3: Se va propune o soluție pentru a rezolva problema.

a. Se vor compara răspunsurile din Pasul 2 cu documentația disponibilă pentru rețea. *Care este eroarea?*

b. Ce soluție ar fi propusă pentru a corecta problema?

Pasul 4: Se va implementa planul.

Se va implementa soluția propusă în Pasul 3b.

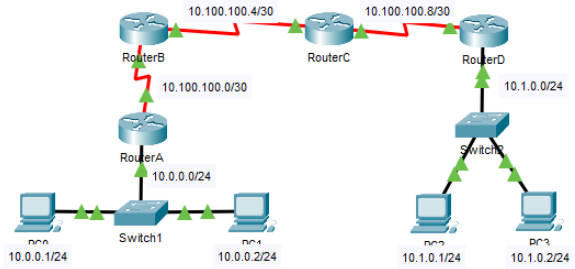
Pasul 5: Se va verifica dacă conectivitatea este restabilită.

a. De la PC2 va fi testată conexiunea la PC4.

b. De la PC4 va fi testată conexiunea la PC2. *Este problema rezolvată?*

Pasul 6: Se va documenta soluția.

EXERCIȚIUL 3. Testarea Conectivității cu Traceroute.



Obiective

Partea 1: Testarea conectivității end-to-end cu comanda tracert.

Partea 2: Comparara cu comanda traceroute de pe un router.

Partea 1: Testarea conectivității end-to-end cu comanda tracert.

Pasul 1: Se va trimite un ping de la un capăt al rețelei la celălalt capăt.

Se va face clic pe PC1 și se va deschide linia de comandă. Ping PC3 la 10.1.0.2. *Ce mesaj este afișat ca rezultat al ping-ului?*

Pasul 2: Se va urmări traseul de la PC1 pentru a determina unde eșuează conectivitatea din cale.

a. Din promptul de comandă al PC1, va fi introdusă comanda tracert 10.1.0.2.

b. Când va fi primit mesajul ***Request timed out***, se va apăsa Ctrl+C. *Care a fost prima adresă IP listată în rezultatul tracert?*

c. Se vor observa rezultatele comenzii tracert. *Care este ultima adresă atinsă cu comanda tracert?*

Pasul 3: Se va corecta problema rețelei.

Se va compara ultima adresă atinsă cu comanda tracert cu adresele de rețea enumerate în topologie. Cel mai îndepărtat dispozitiv de gazdă 10.0.0.2 cu o adresă în intervalul de rețea găsit este punctul de defecțiune. *Ce dispozitive au adrese configurate pentru rețeaua în care a avut loc defecțiunea?*

a. Se va face clic pe RouterC și apoi pe fila CLI. *Care este starea interfețelor?*

b. Se vor compara adresele IP de pe interfețe cu adresele de rețea din topologie. *Se pare că există ceva extraordinar?*

c. Se vor face modificările necesare pentru a restabili conectivitatea; totuși, nu se vor schimba subrețelele. Ce este soluția?

Pasul 4: Se va verifica dacă este stabilită conectivitatea end-to-end.

a. Din promptul de comandă PC1, va fi introdusă comanda tracert 10.1.0.2.

b. Se va observa rezultatul comenzii tracert. *Comanda a avut succes?*

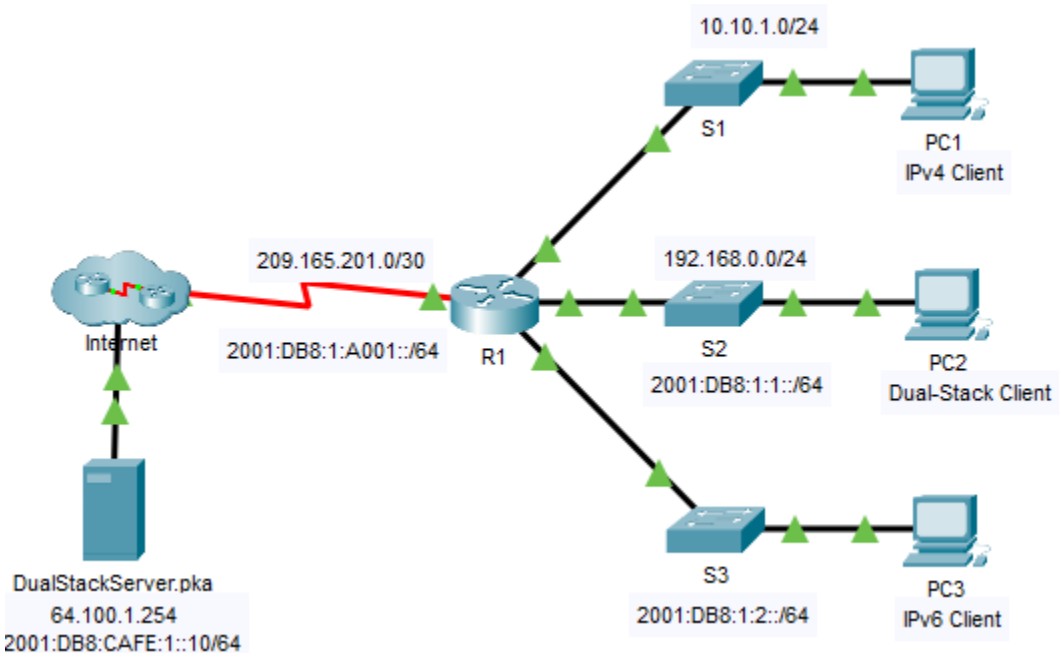
Partea 2: Va fi comparată cu comanda traceroute de pe un router

a. Se va face clic pe RouterA și apoi pe fila CLI.

b. Va fi introdusă comanda traceroute 10.1.0.2. *Comanda s-a finalizat cu succes?*

c. Se va compara ieșirea de la comanda router traceroute cu comanda PC tracert. *Ce este semnificativ diferit la lista de adrese returnate?*

EXERCIȚIUL 4. Depanarea adresei IPv4 și IPv6.



Tabel de Adresare

Device	Interface	IPv4 Address / IPv6 Address/Prefix	Subnet Mask	Default Gateway
R1	G0/0	10.10.1.1	255.255.255.0	N/A
	G0/1	192.168.0.1	255.255.255.0	N/A
		2001:DB8:1:1::1/64		N/A
	G0/2	2001:DB8:1:2::1/64		N/A
	S0/0/0	209.165.201.2	255.255.255.252	N/A
		2001:DB8:1:A001::2/64		N/A
	Link-local	FE80::1		N/A
Dual Stack Server	NIC	64.100.1.254	255.255.255.0	64.100.1.1
		2001:DB8:CAFE:1::10/64		FE80::A
DNS Server	NIC	64.100.1.254	255.255.255.0	64.100.1.1
		2001:DB8:CAFE:1::10/64		FE80::A
PC1	NIC	10.10.1.2	255.255.255.0	10.10.1.1
PC2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
		2001:DB8:1:1::2/64		FE80::1
PC3	NIC	2001:DB8:1:2::2/64		FE80::1

Obiective

Partea 1: Depanarea primei probleme.

Partea 2: Depanarea celei de-a doua probleme.

Partea 3: Depanarea celei de-a treia probleme.

Partea 1: Depanarea primei probleme.

Un client care folosește PC1 se plânge că nu poate accesa pagina web dualstackserver.pka.

Pasul 1: Se va verifica un bilet detaliat la biroul de asistență. Serviciul de asistență a colectat următoarele informații de la client, prin telefon. Se va verifica dacă este corect.

Help Desk Ticket	
Client Identifier: PC1	
Issue: Nu se poate accesa pagina web dualstackserver.pka.	
Informații detaliate despre problemă	
Test: Verificarea dacă computerul are o adresă IP utilizând **ipconfig**?	Yes
Test: Poate computerul să-și contacteze gateway-ul folosind **ping**?	Yes
Test: Poate computerul să contacteze serverul folosind **tracert**?	Yes
Test: Poate computerul să contacteze serverul folosind **nslookup**?	No
Resolution: Se trece la nivelul de asistență 2.	

Pasul 2: Se vor lua în considerare cauzele probabile ale eșecului.

a. Se vor observa testele care au fost efectuate. Dacă este posibil, vor fi discutate posibile scenarii care ar crea această situație cu colegii tehnicieni de rețea.

b. Vor fi efectuate mai multe teste dacă ajută la vizualizarea problemei.

Pasul 3: Se va propune o soluție pentru a rezolva problema.

Se va face o listă cu lucrurile care ar putea fi schimbate pentru a rezolva această problemă. Se va începe cu soluția care este cel mai probabil să funcționeze.

Pasul 4: Se va implementa planul.

Se va încerca cea mai probabilă soluție din listă. Dacă a fost deja încercată, se va trece la următoarea soluție.

Pasul 5: Se va verifica dacă soluția a rezolvat problema.

a. Vor fi repetate testele de la biletul de la biroul de asistență. *A rezolvat problema?*

b. Dacă problema încă există, se va inversa modificarea dacă nu există siguranța că este corectă și se va reveni la Pasul 4.

Pasul 6: Se va documenta soluția.

Se va înregistra soluția problemei. Dacă în viitor se va mai întâlni vreodată aceeași problemă, notițele vor fi foarte valoroase.

Partea 2: Se va depana a doua problemă.

Un client care utilizează PC2 se plânge că nu poate accesa fișierele de pe DualStackServer.pka la 2001:DB8:CAFE:1::10.

Pasul 1: Se va verifica un bilet detaliat primit de la biroul de asistență.

Serviciul de asistență a colectat următoarele informații de la client, prin telefon. Se va verifica dacă este corect.

Help Desk Ticket	
Client Identifier: PC2	
Issue: Nu se poate accesa serviciul FTP de la 2001:DB8:CAFE:1:10.	
Informații detaliate despre problemă	
Test: Verificarea : Computerul are o adresă IPv6 utilizând **ipv6config**?	Yes
Test: Poate computerul să-și contacteze gateway-ul folosind **ping**?	Yes
Test: Poate computerul să contacteze serverul folosind **tracert**?	No
Resolution: Se trece la nivelul 2 suport.	

Pasul 2: Se vor completa pașii 2 până la 5 din Partea 1 pentru această problemă.

Pasul 3: Se va documenta soluția.

Se va înregistra soluția problemei. Dacă în viitor se va mai întâlni vreodată aceeași problemă, notițele vor fi foarte valoroase.

Partea 3: Se va depana a treia problemă.

Un client care utilizează PC3 se plânge că nu poate comunica cu PC2.

Pasul 1: Se va verifica primirea unui bilet detaliat de la biroul de asistență.

Serviciul de asistență a colectat următoarele informații de la utilizator prin telefon. Se va verifica dacă este corect.

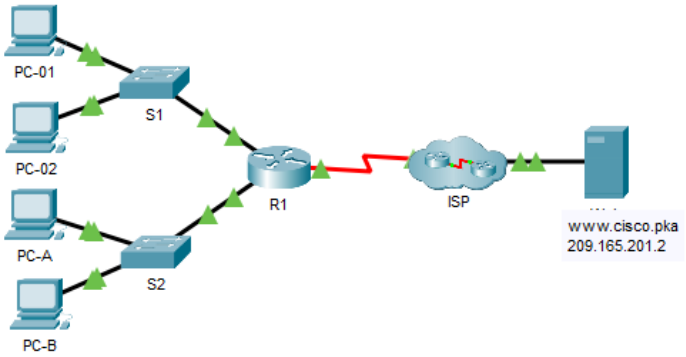
Help Desk Ticket	
Client Identifier: PC3	
Issue: Imposibil de a comunica cu PC2.	
Informații detaliate despre problemă	
Test: Se verifică dacă computerul are o adresă IP utilizând **ipconfig**?	Yes

Test: Se verifică dacă computerul are o adresă IPv6 cu **ipv6config**?	Yes
Test: Poate computerul să contacteze gateway-ul său IPv4 cu **ping**?	No
Test: Poate computerul să contacteze gateway-ul său IPv6 cu **ping**?	Yes
Test: Poate computerul să contacteze clientul IPv4 cu **tracert**?	No
Test: Poate computerul să contacteze clientul IPv6 cu **tracert**?	Yes
Resolution: Se trece la nivelul 2 suport.	

Pasul 2: Se vor completa pașii 2 până la 5 din Partea 1 pentru această problemă.

Pasul 3: Se va documenta soluția.

EXERCIȚIUL 5. Depanarea Problemelor de Conectivitate.



Tabel de Adresare

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	G0/1	172.16.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.226	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.224	N/A
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	N/A
PC-01	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-02	NIC	172.16.1.4	255.255.255.0	172.16.1.1
PC-A	NIC	172.16.2.3	255.255.255.0	172.16.2.1
PC-B	NIC	172.16.2.4	255.255.255.0	172.16.2.1
Web	NIC	209.165.201.2	255.255.255.224	209.165.201.1
DNS1	NIC	209.165.201.3	255.255.255.224	209.165.201.1
DNS2	NIC	209.165.201.4	255.255.255.224	209.165.201.1

Obiective

Obiectivul acestei activităţi Packet Tracer este de a depana şi de a rezolva problemele de conectivitate, dacă este posibil. În caz contrar, problemele ar trebui să fie clar documentate şi astfel încât să poată fi escaladate.

Pasul 1: Determinarea problemei de conectivitate între PC-01 şi serverul web.

a. Pe PC-01, va fi deschis promptul de comandă. Se va introduce comanda ipconfig pentru a verifica ce adresă IP şi gateway implicit i-au fost atribuite PC-01. Va fi corect după caz.

b. După corectarea problemelor de adresare IP pe PC-01, vor fi emise ping-urile către gateway-ul implicit, serverul web şi alte PC-uri. *Au avut succes ping-urile?* Trebuie să fie înregistrate rezultatele.

Ping la gateway-ul implicit (172.16.1.1). La serverul web (209.165.201.2).

Ping la PC-02. La PC-A. La PC-B.

c. Se va folosi browserul web pentru a accesa serverul web de pe PC-01. Se va introduce adresa URL www.cisco.pka şi apoi se va folosi adresa IP 209.165.201.2. Trebuie să fie înregistrate rezultatele.

Poate PC-01 să acceseze www.cisco.pka? folosind adresa IP a serverului web?

d. Vor fi documentate problemele şi vor fi furnizate soluţia (soluţiile). Vor fi corectate problemele dacă este posibil.

Pasul 2: Se va determina problema de conectivitate dintre PC-02 şi serverul web.

a. Pe PC-02, va fi deschis promptul de comandă. Se va introduce comanda ipconfig pentru a verifica configuraţia pentru adresa IP şi gateway-ul implicit. Va fi corectat după caz.

b. După corectarea problemelor de adresare IP pe PC-02, vor fi emise ping-urile către gateway-ul implicit, serverul web şi alte PC-uri. Au avut succes ping-urile? Trebuie să fie înregistrate rezultatele.

Ping la gateway-ul implicit (172.16.1.1). La serverul web (209.165.201.2) .

Ping la PC-01. La PC-A. La PC-B.

c. Se va naviga la www.cisco.pka folosind browserul web de pe PC-02. Trebuie să fie înregistrate rezultatele.

Poate PC-01 să acceseze www.cisco.pka? folosind adresa IP a serverului web

d. Vor fi documentate problemele și vor fi furnizate soluția (soluțiile). Problemele vor fi corectate dacă este posibil.

Pasul 3: Se va determina problema de conectivitate dintre PC-A și serverul web.

a. Pe PC-A, va fi deschis promptul de comandă. Se va introduce comanda ipconfig pentru a verifica configurația pentru adresa IP și gateway-ul implicit. Va fi corectat după caz.

b. După corectarea problemelor de adresare IP pe PC-A, vor fi emise ping-urile către gateway-ul implicit, serverul web și alte PC-uri. Au avut succes ping-urile? Trebuie să fie înregistrate rezultatele.

Ping la gateway-ul implicit (172.16.2.1). La serverul web (209.165.201.2).

Ping la PC-B. La PC-01. La PC-02.

c. Se va naviga la www.cisco.pka.net folosind browserul web de pe PC-A. Trebuie să fie înregistrate rezultatele.

Poate PC-A să acceseze www.cisco.pka? folosind adresa IP a serverului web

d. Va documenta problemele și va furniza soluția (soluțiile). Problemele vor fi corectate dacă este posibil.

Pasul 4: Determinarea problemei de conectivitate între PC-B și serverul web.

a. Pe PC-B, va fi deschis promptul de comandă. Se va introduce comanda ipconfig pentru a verifica configurația pentru adresa IP și gateway-ul implicit. Va fi corectat după caz.

b. După corectarea problemelor de adresare IP pe PC-B, vor fi emise ping-urile către gateway-ul implicit, serverul web și alte PC-uri. Au avut succes ping-urile? Trebuie să fie înregistrate rezultatele.

Ping la gateway-ul implicit (172.16.2.1). La serverul web (209.165.201.2).

Ping la PC-A. La PC-01. La PC-02.

c. Se va naviga la www.cisco.pka folosind browser-ul web. Trebuie să fie înregistrate rezultatele.

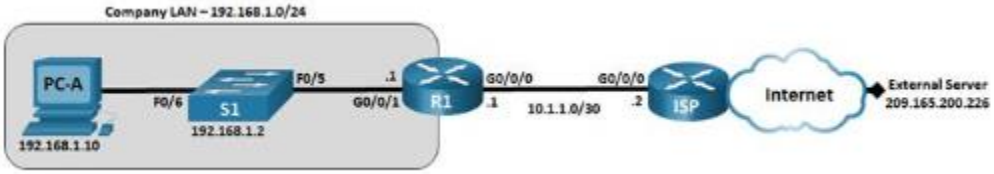
Poate PC-B să acceseze www.cisco.pka? folosind adresa IP a serverului web

d. Vor fi documentate problemele și vor fi furnizate soluția (soluțiile). Vor fi corectate problemele dacă este posibil.

Pasul 5: Se va verifica conectivitatea.

Se va verifica dacă toate PC-urile pot accesa serverul web www.cisco.pka.

EXERCIȚIUL 6. Depanarea Problemelor de Conectivitate la Modul Fizic.



Obiective

Partea 1: Identificarea problemei.

Partea 2: Implementarea modificărilor de rețea.

Partea 3: Verificarea funcționalității complete.

Partea 4: Documentarea constatărilor și modificărilor de configurare.

Instrucțiuni

Partea 1: Identificarea problemei.

Singura informație disponibilă despre problema rețelei este că utilizatorii se confruntă cu timpi de răspuns lenți și că nu pot ajunge la un dispozitiv extern pe internet la adresa IP 209.165.200.226. Pentru a determina cauzele probabile pentru aceste probleme de rețea, va fi necesar să fie utilizate comenzile și instrumentele de rețea de pe echipamentul LAN.

Notă: Numele de utilizator admin01 cu o parolă cisco12345 va fi necesar pentru conectarea la echipamentul de rețea.

Pasul 1: Depanarea rețelei.

Se vor folosi instrumentele disponibile pentru a depana rețeaua, ținând cont de faptul că cerința este de a restabili conectivitatea la serverul extern și de a elimina timpii de răspuns lenți.

Pasul 2: Documentarea cauzelor probabile.

Se vor enumera cauzele probabile ale problemelor de rețea cu care se confruntă angajații.

Partea 2: Implementarea modificărilor de rețea

Vor fi comunicate supervizorului problemele descoperite în partea 1. Dacă a aprobat aceste modificări, atunci a cerut ca acestea să fie implementate.

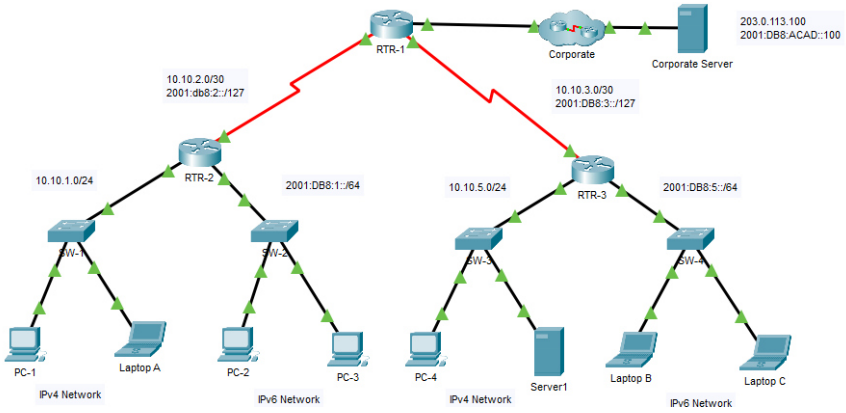
Partea 3: Verificarea funcționalității complete.

Trebuie să se verifice dacă funcționalitatea completă a fost restaurată. PC-A, S1 și R1 ar trebui să poată ajunge la serverul extern, iar răspunsurile ping de la PC-A către serverul extern nu ar trebui să prezinte variații semnificative în timpii de răspuns.

Partea 4: Documentarea constatărilor și modificărilor de configurare.

Se va folosi spațiul oferit mai jos pentru a documenta problemele găsite în timpul depanării și modificările configurațiilor făcute pentru a rezolva aceste probleme.

EXERCIȚIUL 7. Utilizarea ICMP pentru a Testa si Corecta Conexiunea la Rețea.



Tabel de Adresare

Device	Interface	Address	Mask/Prefix	Default Gateway
RTR-1	G/0/0/0	192.168.1.1	255.255.255.0	N/A
		2001:db8:4::1	/64	N/A
	S0/1/0	10.10.2.2	255.255.255.252	N/A
		2001:db8:2::2	/126	N/A
	S0/1/1	10.10.3.1	255.255.255.252	N/A
		2001:db8:3::1	/126	N/A
RTR-2	G/0/0/0	10.10.1.1	255.255.255.0	N/A
	G0/0/1	2001:db8:1::1	/64	N/A
	S0/1/0	10.10.2.1	255.255.255.252	N/A
		2001:db8:2::1	/126	N/A
RTR-3	G0/0/0	10.10.5.1	255.255.255.0	N/A
	G0/0/1	2001:db8:5::1	/64	N/A
	S0/1/0	10.10.3.2	255.255.255.252	N/A
		2001:db8:3::2	/126	N/A
PC-1	NIC	10.10.1.10	255.255.255.0	10.10.1.1
Laptop A	NIC	10.10.1.20	255.255.255.0	10.10.1.1
PC-2	NIC	2001:db8:1::10	/64	fe80::1
PC-3	NIC	2001:db8:1::20	/64	fe80::1
PC-4	NIC	10.10.5.10	255.255.255.0	10.10.5.1
Server 1	NIC	10.10.5.20	255.255.255.0	10.10.5.1
Laptop B	NIC	2001:db8:5::10	/64	fe80::1
Laptop C	NIC	2001:db8:5::20	/64	fe80::1
Corporate Server	NIC	203.0.113.100	255.255.255.0	203.0.113.1
		2001:db8:acad::100	/64	fe80::1

Obiective

În acest laborator se va folosi ICMP pentru a testa conectivitatea la rețea și a localiza problemele de rețea. De asemenea, vor fi corectate problemele simple de configurare și vor restabili conectivitatea la rețea.

· Se va folosi ICMP pentru a localiza problemele de conectivitate.

· Se vor configura dispozitivele de rețea pentru a corecta problemele de conectivitate.

Instrucțiuni

Toate gazdele ar trebui să aibă conectivitate la toate celelalte gazde și la serverul corporativ.

· Se va aștepta până când toate luminile de legătură sunt verzi.

· Se va selecta o gazdă și se va folosi ping ICMP pentru a determina ce gazde sunt accesibile de la acea gazdă.

· Dacă se găsește că o gazdă nu poate fi accesată, se va utiliza urmărirea ICMP pentru a localiza locația generală a erorilor de rețea.

· Se vor localiza erorile specifice și vor fi corectate.