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

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

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

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

1. ***Configurarea protocolului de rutare RIP utilizând protocolul RIP***

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

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

Pașii pentru configurarea rutării dinamice RIP sunt:

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



***Figura 3.1. Configurarea rutării dinamice utilizând GUI***

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

**Tabelul 3.1. Adresele IP de rețea ale interfețelor routerului**

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

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

Dacă s-a efectuat pasul 5 din rutarea statică, se va observa apariția unei erori, deoarece nu s-au introdus manual rute alternative pentru fiecare rețea în fiecare router pentru a preveni pierderea conectivității dintre routere. Aceasta este o caracteristică semnificativă a rutelor dinamice.

1. ***Configurarea protocolului de rutare RIP utilizând CLI***

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

1. Se utilizează aceleași comenzi ca și în exemplul de configurare a rutării statice cu linia de comandă pentru a atribui adresele IP ale interfeței routerului.
2. Apoi se revine la modul de configurare globală și se utilizează următoarea comandă pentru a trece la modul router RIP:

R1(config)#router rip

1. Pentru a afla adresa IP a rețelei, se utilizează comanda *network.* Urmeaza următoarele comenzi pentru Router R1:

R1(config-router)#network 192.168.10.0

R1(config-router)#network 192.168.20.0

1. Se configurează toate routerele în mod identic. Apoi, pentru a efectua un test de conectivitate, se utilizează instrumentul PDU convențional.

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

1. ***Tabelul de rutare***

Tabelul de rutare include o listă a tuturor rutelor preferate pe care routerele le сunosc. Tabelul de rutare poate fi vizualizat în două moduri. Pentru unul dintre ele se utilizează butonul Inspect Instrument, iar pentru celălalt se utilizează comanda Cisco IOS *show ip route*. Apare un tabel format din mai multe coloane și informații în ele. În continuare se va afișa ce anume este inclus în tabel:

R1#show ip route

C 192.168.10.0/24 is directly connected, FastEthernet0/0

C 192.168.20.0/24 is directly connected, FastEthernet0/1

R 192.168.30.0/24 [120/1] via 192.168.10.2, 00:00:13,

FastEthernet0/0

R 192.168.40.0/24 [120/1] via 192.168.20.2, 00:00:22,

FastEthernet0/1

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

A doua coloană indică rețeaua de destinație.

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

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

Adresa gateway-ului, care este următorul router ce se îndreaptă către rețeaua de destinație, este adresa IP scrisă după cuvântul „via”. Un cronometru de reținere sau holddown timer este marca temporală scrisă la sfârșitul unei rute dinamice. În plus, orice protocol de rutare trimite mesajele la un interval specific, cum ar fi „Hello timer”. Când vine vorba de protocolul RIP, acesta este de 30 de secunde. Dacă routerul nu primește mesaje despre o rută în timpul a trei intervale Hello (180 s sau Holddown timer), această rută este eliminată din tabelul de rutare și se caută o rută alternativă.

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

1. ***Distribuția sarcinii***

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

1. **Echilibrarea sarcinii în protocolul RIP**

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

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

R4(config)#interface loopback 0

R4(config-if)#ip address 192.168.100.1 255.255.255.0

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

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

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



***Figura 3.2. Utilizarea instrumentului Complex PDU***

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

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

Router>show ip route

R 192.168.30.0/24 [120/1] via 192.168.10.2, 00:00:12,  
FastEthernet0/0

R 192.168.40.0/24 [120/1] via 192.168.20.2, 00:00:14,  
FastEthernet0/1

R 192.168.100.0/24

[120/2] via 192.168.20.2, 00:00:08, FastEthernet0/1

[120/2] via 192.168.10.2, 00:00:08, FastEthernet0/0

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

1. **Echilibrarea sarcinii pentru rutele statice**

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

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

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

1. Se configurează două rute către 192.168.100.0/24 pe routerul R1. Routerului trebuie să i se explice că există două moduri pentru a ajunge la interfața loopback a routerului R4. Pentru a realiza acest lucru, se utilizează comenzile următoare:

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

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

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

1. ***Protocol gateway extern BGP (Border Gateway Protocol)***

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

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

1. **Ce este BGP?**

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

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

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

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



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



***Figura 3.4. Opțiuni cu dublă localizare (Dual homed)***

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



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



***Figura 3.6. Opțiuni dual multihomed (Dual multihomed)***

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

Există două tipuri de BGP:

1. BGP extern (External BGP, eBGP);

2. BGP intern (iBGP).

1. **BGP extern**

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

1. **BGP intern**

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

1. ***BGP ca protocol de rutare dinamic***

Deși BGP și alte protocoale de rutare dinamice funcționează la fel, există câteva diferențe între protocoalele de rutare dinamice. Protocoalele de gateway interior IGP (Interior Gateway Protocols) precum RIP, OSPF și EIGRP au protocoale de rutare avansate. Adresa IP a rețelei este determinată de anunțul de rețea care este creat prin configurarea protocolului de rutare. Procesul de anunțare a rutării implică interfețe ale căror adrese IP se încadrează în intervalul rețelei anunțate. Anunțurile de rutare sunt difuzate sau distribuite prin intermediul acestor interfețe. Pentru ca acest lucru să funcționeze, două routere vecine trebuie să aibă o conexiune directă unul cu celălalt și trebuie să aibă procese de protocol gateway interior (IGP) care să funcționeze pe ele. Numărul de salturi, lățimea de bandă, timpul de întârziere și alți parametri sunt utilizați de protocoalele interfeței interne de protocol (IGP) pentru a alege calea optimă.

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

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

1. ***Configurarea BGP în Packet Tracer***

În primul rând, se examinează comenzile utilizate în BGP:

router bgp <asn>

De exemplu:

R1(config)# router bgp 120

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

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

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

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

bgp router-id X.X.X.X

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

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

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

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

De exemplu:

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

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

Pentru protocolul BGP extern se vor utiliza următoarele comenzi:

R1(config)#router bgp 120

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

Pentru protocolul BGP intern se va utiliza următoarea formă:

R1(config)#router bgp 120

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

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

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

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

R1(config-router)#network 10.20.20.0 mask 255.255.255.0

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

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

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



***Figura 3.7. Exemplu de configurare BGP în Packet Tracer***

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

**Tabelul 3.2. Adresele IP ale interfețelor routerului**

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

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

1. Configurarea începe de la routerele de producție:

Enterprise1(config)#router bgp 10200

Enterprise1(config-router)#bgp router-id 0.0.0.1

Enterprise1(config-router)#neighbor 10.0.0.2 remote-as 30200

Enterprise1(config-router)#neighbor 10.0.0.10 remote-as 50300

Enterprise1(config-router)#network 20.30.0.0 mask 255.255.0.0

Enterprise2(config)#router bgp 3400

Enterprise2(config-router)#bgp router-id 0.0.0.2

Enterprise2(config-router)#neighbor 10.0.0.6 remote-as 30200

Enterprise2(config-router)#neighbor 10.0.0.14 remote-as 50300

Enterprise2(config-router)#network 40.30.0.0 mask

255.255.0.0

1. În continuare, se configurează routerele ISP:

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

1. Când configurarea este corectă, vor apărea mesaje de consolă despre stabilirea vecinătății:

%BGP-5-ADJCHANGE: neighbor 10.0.0.9 Up

%BGP-5-ADJCHANGE: neighbor 10.0.0.13 Up

1. Ping la interfața loopback a routerului Enterprise2 de la routerul Enterprise1:

Enterprise1>ping 40.30.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 40.30.0.1, timeout is 2

seconds:

.....

Success rate is 0 percent (0/5)

1. Se observă că încercarea de testare a conectivității a eșuat.

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

Enterprise1#ping

Protocol [ip]:

Target IP address: 40.30.0.1

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 20.30.0.1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

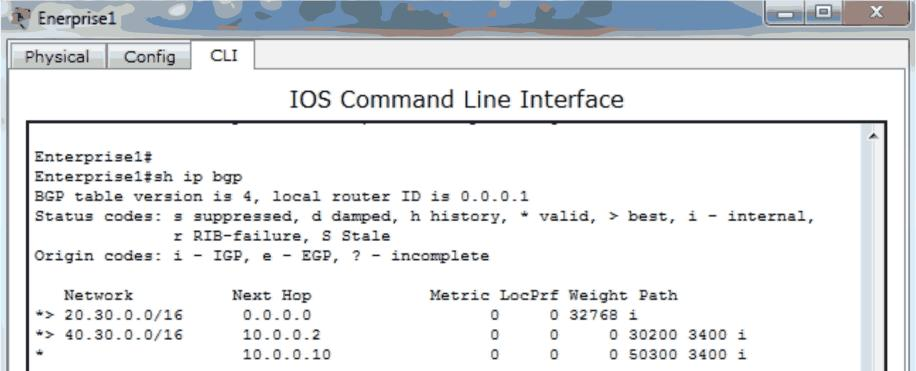
Sending 5, 100-byte ICMP Echos to 40.30.0.1, timeout is 2 seconds:

Packet sent with a source address of 20.30.0.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

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



***Figura 3.8. Rezultatul utilizării comenzii sh ip bgp***

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

Se cere proiectarea unei subrețele, având la bază topologia prezentată în figura 3.9. Rețeaua locală va fi segmentată în subrețele pentru a optimiza traficul și a spori securitatea. Fiecare router va fi responsabil pentru gestionarea subrețelelor specifice din rețea. Switch-urile vor conecta calculatoarele la subrețelele respective, asigurând conectivitatea și comunicarea eficientă. Proiectarea subrețelelor va lua în considerare numărul de calculatoare, tipul de trafic și cerințele de securitate specifice fiecărei subrețele.

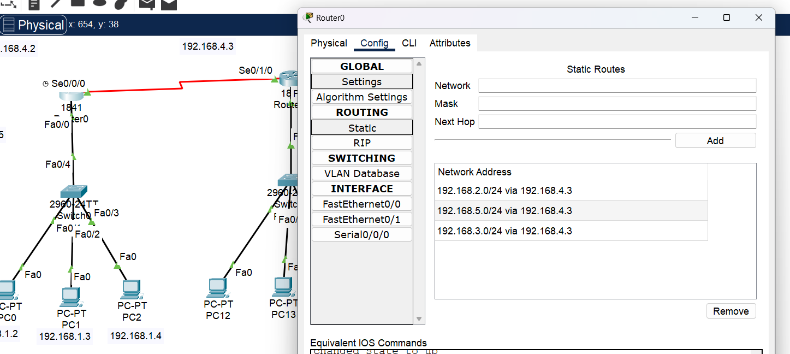


***Figura 3.9. Rețeaua locală alcătuită din 3 routere, 3 switch-uri și 9 calculatoare***

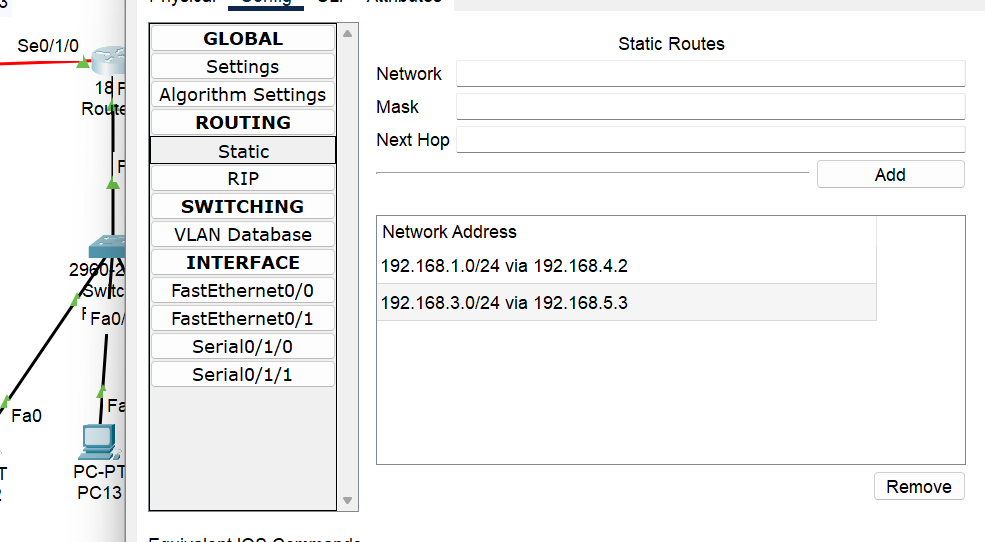
Rețeaua va fi împărțită în 3 subrețele distincte, având configurații specifice de adresare IP și mască. Subrețeaua 1 va utiliza intervalul 192.168.1.0/24 cu masca 255.255.255.0, Subrețeaua 2 va fi definită de 192.168.2.0/24 și masca 255.255.255.0, iar Subrețeaua 3 va cuprinde adresele din 192.168.3.0/24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

Pentru a facilita comunicarea între subrețele, se vor configura rute statice pe cele 3 routere. Primul router va deține rute statice către subrețelele 2, 3 și 4, utilizând interfața de ieșire 192.168.4.3. Al doilea router va fi configurat cu rute statice către subrețelele 1 și 3, având ca interfață de ieșire 192.168.4.2. Al treilea router va completa schema prin configurarea de rute statice către subrețelele 1, 2 și 4, cu interfața de ieșire 192.168.5.2.

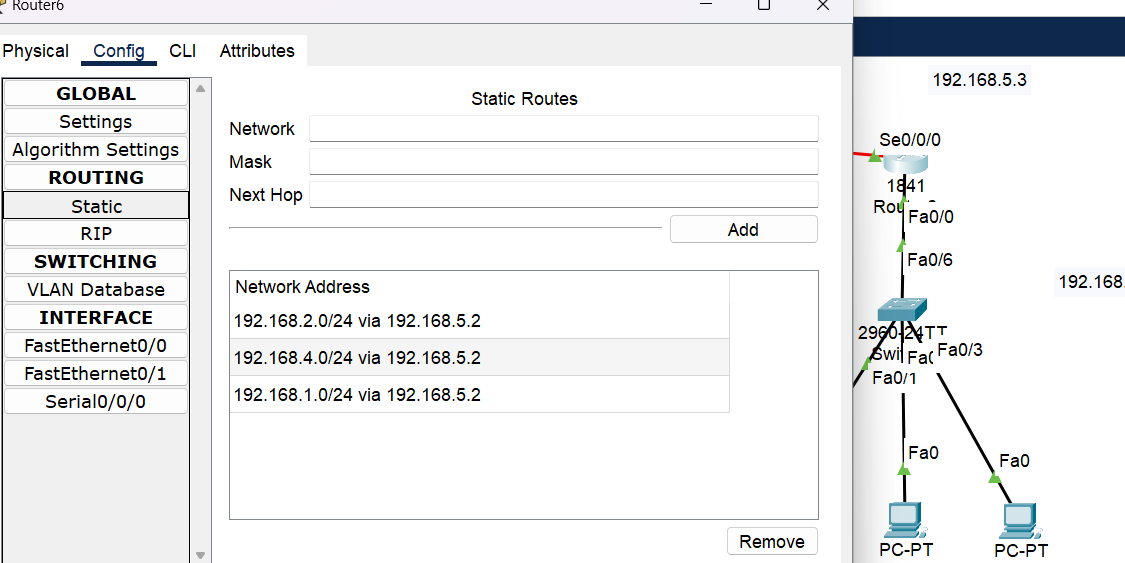
Switch-urile vor juca un rol esențial în conectarea calculatoarelor la subrețelele respective, asigurând comunicarea eficientă între dispozitivele din rețea. Segmentarea rețelei în subrețele va optimiza traficul și va spori semnificativ nivelul de securitate prin limitarea accesului la anumite segmente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



***Figura 3.10. Configurarea routingului static la primul router***



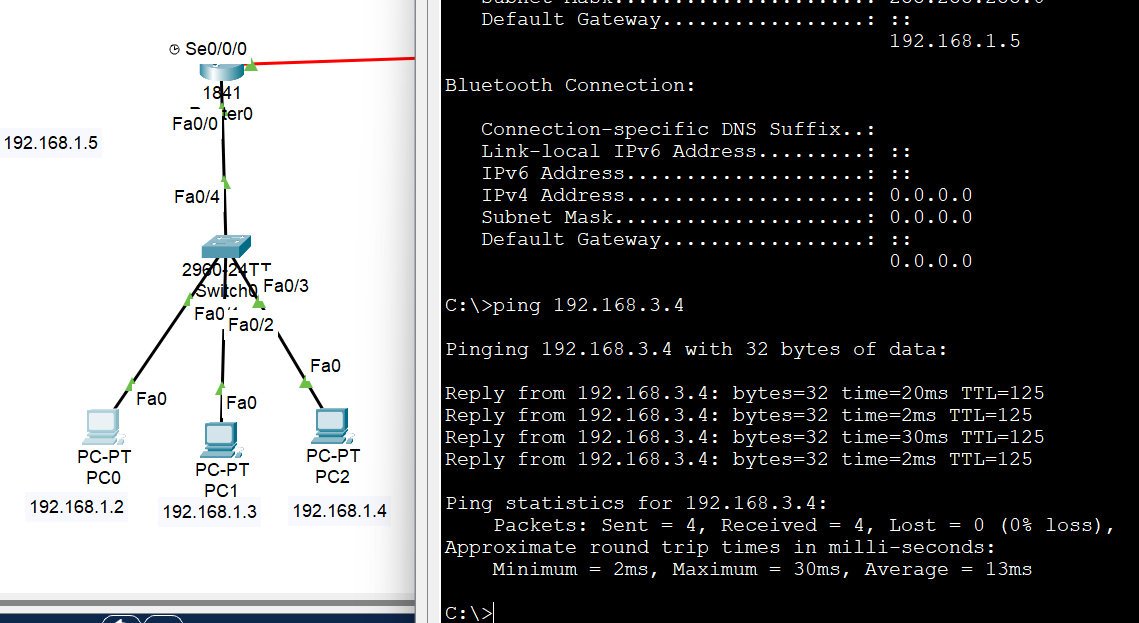
***Figura 3.11. Configurarea routingului static la al doilea router***



***Figura 3.12. Configurarea routingului static la al treilea router***

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

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



***Figura 3.13. Legătura primului calculator cu ultimul prin***

***comanada ping***

1. **Conținutul raportului**
2. Introducere:
3. Scopul și obiectivele lucrării de laborator.
4. Descrierea generală a rețelei locale și a necesității utilizării algoritmilor de routing.
5. Descrierea rețelei locale:
6. Prezentarea topologiei rețelei: routere, switch-uri, calculatoare etc.
7. Configurarea inițială a dispozitivelor din rețea: setarea adreselor IP, configurarea interfețelor de rețea etc.
8. Algoritmii de routing utilizați:
9. Explicarea conceptelor și principiilor de bază ale algoritmilor de routing: static, RIP, OSPF etc.
10. Descrierea modului de funcționare a fiecărui algoritm în cadrul rețelei locale proiectate.
11. Configurarea algoritmilor de routing:
12. Configurarea și setarea algoritmilor de routing pe dispozitivele din rețea.
13. Descrierea pașilor specifici necesari pentru fiecare algoritm.
14. Verificarea funcționării algoritmilor de routing:
15. Utilizarea comenzilor specifice pentru a verifica starea și funcționarea algoritmilor de routing pe dispozitivele din rețea.
16. Testarea conectivității între diferitele subrețele, utilizând algoritmii de routing configurați.
17. Concluzie:
18. Rezultatele obținute în cadrul lucrării de laborator.
19. Observații și concluzii privind eficiența și performanța algoritmilor de routing utilizați.
20. Bibliografie:
21. Sursele bibliografice utilizate pentru a înțelege conceptele și principiile algoritmilor de routing.
22. Anexe:
23. Capturi de ecran cu configurările și interacțiunile din cadrul laboratorului, dacă este necesar.

**Întrebări de control**

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

**Bibliografie**

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