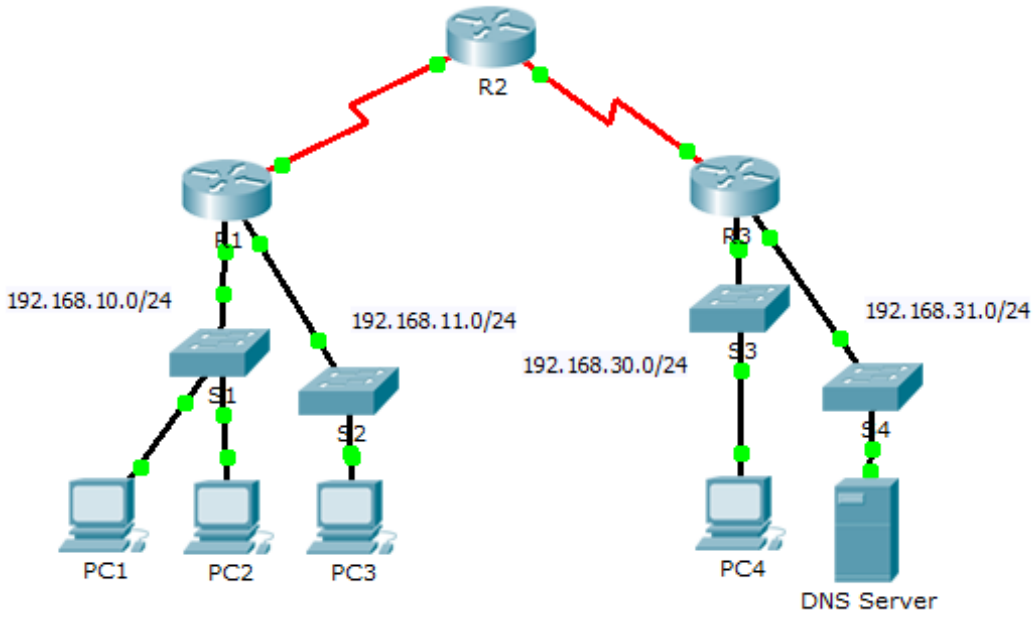
Packet Tracer – Demonstrație Access Control List (ACL)

Topologie



Obiective

Partea 1: Verificați Conectivitatea Locală și Testați ACL

Partea 2: Ștergeți ACL și Repetați Testul

Context

În această activitate, veți observa cum o listă de control al accesului (ACL) poate fi folosită pentru a împiedica o comandă ping de ajunge la gazde din rețele la distanță. După ce se elimină ACL din configurație, comenzile ping se vor realiza cu succes.

Part 1: Verificați Conectivitatea Locală și Testați ACL

Step 1: Dați ping la rețeaua locală pentru a verifica conectivitatea.

a. Din ecranul de comandă al lui **PC1**, dați ping la **PC2**.

b. Din ecranul de comandă al lui **PC1**, dați ping la **PC3**.

De ce s-au realizat comenzile ping cu succes?

Step 2: Dați ping la echipamente din rețele remote pentru a testa funcționalitatea ACL.

a. Din ecranul de comandă al lui **PC1**, dați ping la **PC4**.

b. Din ecranul de comandă **al lui** PC1, dați ping la serverul DNS.

De ce ping-urile au eșuat? (Indiciu: Folosiți modul de simulare sau vizualizați configărirle routerului pentru a investiga.) Ping-urile eșuează deoarece R1 este configurat cu un ACL pentru a împiedica orice ping din interfața serială 0/0/0 de ieșire.

Part 2: Ștergeți ACL și Repetați Testul

Step 1: Folosiți comenzile show pentru a investiga configurarea ACL.

a. Folosiți comenzile **show run** și **show access-lists** pentru a vizualiza ACL-urile curente configurate. Pentru a vizualiza rapid ACL-urile curente, folosiți show access-lists. Introduceți comanda **show access-lists** urmată de un spațiu și un semn de întrebare pentru a vizualiza opțiunile disponibile:

```
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  <cr>
```

Dacă știți numărul sau numele de ACL, puteți filtra rezultatul comenzii show. În **orice** caz, R1 are doar un ACL; așadar, comanda **show** access-lists va fi suficientă.

```
R1#show access-lists
Extended IP access list 101
    deny icmp any any echo
    permit ip any any
```

Prima linie din ACL împiedică echo-uri (interogări ping) ICMP (Internet Control Message Protocol) de la orice sursă către orice destinație. A doua linie din ACL permite orice trafic ip de la orice sursă către orice destinație.

b. Pentru ca un ACL să aibă impact asupra funcționării routerului, trebuie aplicat în altă parte. În acest scenariu, ACL este utilizat pentru a filtra traficul pe o interfață. Deși puteți vizualiza informația IP folosind comanda **show ip**, în anumite situații poate fi mai eficient să utilizați doar comanda show run. Folosind una sau ambele comenzi, la care interfață interfață este ACL aplicat?

Step 2: Îndepărtați lista de acces 101 din configurare

Puteți îndepărta ACL-urile din configurare lansând comanda **no access list [număr ACL**] Comanda **no access-list** șterge toate ACL-urile cofnigurate pe router, comanda **no access-list [număr ACL]** *șterge doar un* anumit ACL.

a. În modul de configurare global, ștergeți ACL introducând următoarea comandă:

```
R1(config)# no access-list 101
```

b. Verificați dacă **PC1** poate da acum ping la serverul DNS.

Rubrica Scorului Sugerat

Locația Întrebării	Puncte Posibile	Puncte Obținute
Partea 1, Pasul 1 b.	50	
Partea 1, Pasul 2 b.	40	
Partea 2, Pasul 2 b.	10	
Scor Total	**100**	