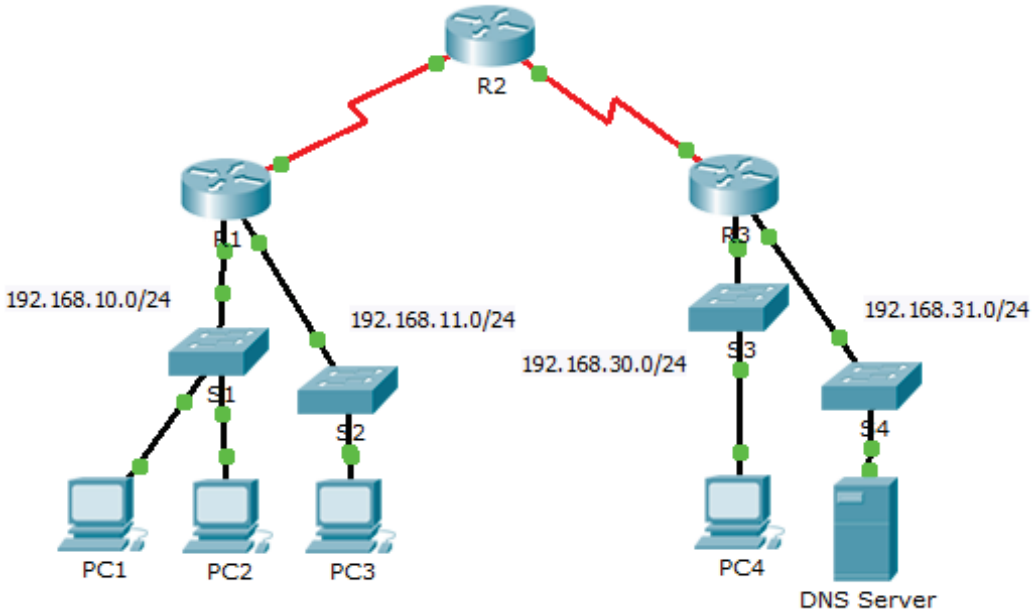
Packet Tracer – Demonstracja działania listy kontroli dostępu

Topologia



Cele

Część 1: Weryfikacja lokalnego połączenia i testowanie listy kontroli dostępu

Część 2: Usuwanie listy kontroli dostępu i ponowne testowanie

Wprowadzenie

Niniejsze ćwiczenie demonstruje użycie listy kontroli dostępu (ACL) w celu zablokowania komunikatów ping tak, by nie dotarł on do hostów znajdujących się w zdalnych sieciach. Po usunięciu listy ACL z konfiguracji, komunikaty ping nie będą blokowane.

Część 1: Weryfikacja lokalnego połączenia i testowanie listy kontroli dostępu

Krok 1: Użyj komendy ping do urządzeń znajdujących się w sieci lokalnej, aby sprawdzić komunikację.

a. W wierszu poleceń komputera **PC1** wykonaj ping do komputera **PC2**.

b. W wierszu poleceń komputera **PC1**, wykonaj ping do komputera **PC3**.

Dlaczego komendy ping zakończyły się pomyślnie? .

Krok 2: Użyj komendy ping do urządzeń znajdujących się w sieciach zdalnych by sprawdzić działanie ACL.

a. W wierszu poleceń komputera **PC1**, wykonaj ping do komputera **PC4**.

b. W wierszu poleceń komputera **PC1**, wykonaj ping do **Serwer DNS**.

Dlaczego testy ping zakończą się niepowodzeniem? (Wskazówka: aby znaleźć przyczynę użyj trybu symulacji lub wyświetl konfigurację routera)

Część 2: Usuwanie listy kontroli dostępu i ponowne testowanie

Krok 1: Aby zbadać konfigurację ACL, użyj komend show.

a. Użyj komend **show run** i **show access-lists,** aby wyświetlić aktualnie skonfigurowane listy ACL. Użyj komendy **show access-lists**, aby szybko wyświetlić aktualne listy ACL. Wpisz komendę **show access-lists** a następnie spację i znak zapytania (?), aby wyświetlić dostępne opcje:

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

Jeżeli znasz numer lub nazwę listy ACL, to możesz filtrować wyjście komendy **show**. Aczkolwiek **R1** ma tylko jedną listę ACL; w związku z tym komenda **show access-lists** jest wystarczająca.

```
R1#show access-lists
Extended IP access list 101
denyicmp any any echo
permitip any any
```

Pierwsza linia ACL odrzuca żądania (Echo Requests) protokołu Internet Control Message Protocol (ICMP) pochodzące z **dowolnego** źródła i kierowane do **dowolnego** miejsca przeznaczenia. Druga linia ACL akceptuje wszystkie inne pakiety **ip** pochodzące z **dowolnego** źródła i kierowane do **dowolnego** miejsca przeznaczenia.

b. Aby lista ACL działała w routerze, musi zostać skojarzona z interfejsem. W tym scenariuszu lista ACL jest używana do filtrowania ruchu na interfejsie. Można wyświetlić informacje dotyczące protokołu IP za pomocą komendy **show ip interface** , ale lepsze jest po prostu użycie polecenia **show run** . Do którego interfejsu jest przyporządkowana lista ACL (użyj jednej lub obu powyższych komend)?

Krok 2: Usuń listę ACL 101 z konfiguracji

Do usuwania list ACL z konfiguracji służy komenda **no access list** [*number of the ACL*]. Komenda **no access-list** usuwa wszystkie listy ACL z routera, natomiast komenda **no access-list** [*numer ACL*] usuwa konkretną listę ACL.

a. Aby usunąć listę ACL, w trybie konfiguracji globalnej wpisz następującą komendę:

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

b. Upewnij się, że ping z komputera **PC1**do**Serwer DNS** kończy się powodzeniem.

Tabela sugerowanej punktacji

Lokalizacja pytania	Maksymalna liczba punktów do uzyskania	Uzyskana liczba punktów
Część 1, krok 1 b.	50	
Część 1, krok 2 b.	40	
Część 2, krok 2 b.	10	
Wynik łączny	**100**	