Packet Tracer – Rozwiązywanie problemów z konfiguracją NAT

Topologia

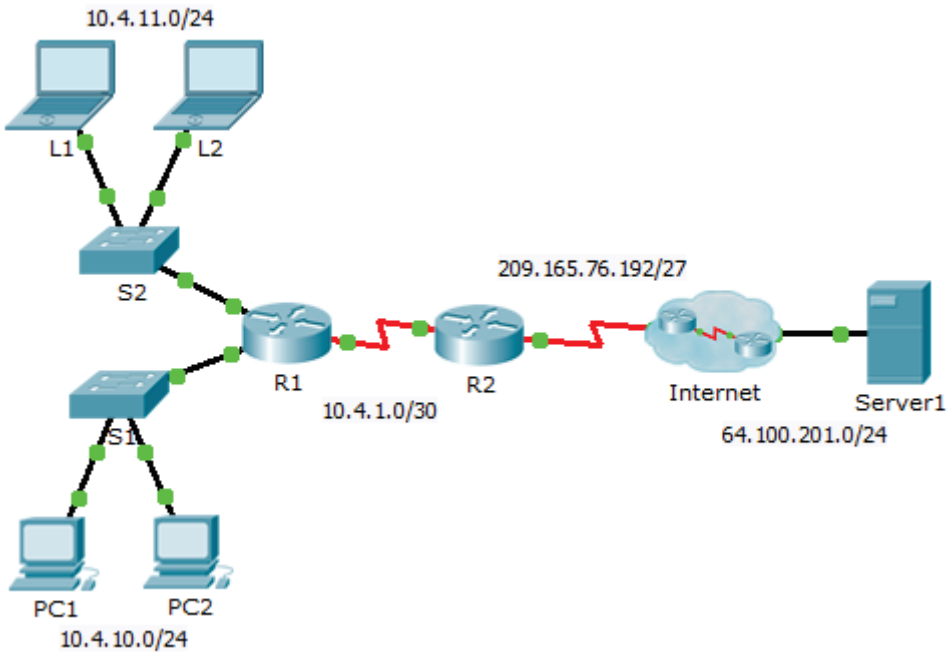

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0	10.4.10.254	255.255.255.0	Nie dotyczy
	G0/1	10.4.11.254	255.255.255.0	Nie dotyczy
	S0/0/1	10.4.1.2	255.255.255.252	Nie dotyczy
R2	S0/0/0	209.165.76.194	255.255.255.224	Nie dotyczy
	S0/0/1	10.4.1.1	255.255.255.252	Nie dotyczy
Server1	Karta sieciowa	64.100.201.5	255.255.255.0	64.100.201.1
PC1	Karta sieciowa	10.4.10.1	255.255.255.0	10.4.10.254
PC2	Karta sieciowa	10.4.10.2	255.255.255.0	10.4.10.254
L1	Karta sieciowa	10.4.11.1	255.255.255.0	10.4.11.254
L2	Karta sieciowa	10.4.11.2	255.255.255.0	10.4.11.254

Cele

Część 1: Identyfikowanie problemu

Część 2: Rozwiązywanie problemów z konfiguracją NAT

Część 3: Weryfikacja połączeń

Scenariusz

Serwisant przywrócił starą konfigurację routera z uruchomioną translacją NAT. Jednakże w międzyczasie sieć została zmieniona: po wykonaniu kopii zapasowej starej konfiguracji dodano do topologii nową podsieć. Twoim zadaniem jest ponowne przywrócenie sprawności sieci.

Część 1: Identyfikowanie problemu

Z hostów **PC1**, **PC2**, **L1**, **L2** oraz **R2** wykonaj ping do **Server1**. Zanotuj każdy ping zakończony sukcesem. Wykonaj ping do dowolnego innego hosta, jeśli wystąpi taka konieczność.

Część 2: Rozwiązywanie problemów z konfiguracją NAT

Krok 1: Przejrzyj odwzorowania NAT na R2.

Jeśli NAT działa prawidłowo, powinny istnieć wpisy w tablicy odwzorowań.

Krok 2: Wyświetl bieżącą konfigurację routera R2.

Port oznaczony jako NAT inside powinien być powiązany z adresami sieci prywatnej, natomiast port NAT outside powinien być przypisany do adresów publicznych (globalnych).

Krok 3: Popraw konfigurację interfejsów.

Przypisz komendy **ipnat inside** oraz **ipnat outside** do właściwych portów.

Krok 4: Z hostów PC1, PC2, L1, L2 oraz R2 wykonaj ping do Server1.

Zapisz wynik każdego polecenia ping zakończonego sukcesem. Wykonaj ping do dowolnego innego hosta, jeśli jest to konieczne.

Krok 5: Przejrzyj odwzorowania NAT na R2.

Jeśli NAT działa prawidłowo, powinny istnieć wpisy w tablicy odwzorowań.

Krok 6: Wyświetl listę ACL 101 na R2.

Maska odwrotna powinna obejmować obie sieci: 10.4.10.0 oraz 10.4.11.0.

Krok 7: Popraw listę ACL.

Usuń listę ACL 101, a następnie zastąp ją nową listą o podobnej składni. Jedyną różnicą będzie maska odwrotna.

Część 3: Weryfikacja połączeń

Krok 1: Sprawdź połączenie z serwerem Serwer1.

Zapisz wynik każdego polecenia ping zakończonego sukcesem. Z każdego hosta powinno być możliwe wysłanie pakietów ping do **Server1**, **R1**, oraz **R2**. Jeżeli sprawdzenie za pomocą ping nie dało pomyślnego rezultatu, wyszukaj i rozwiąż problemy aż osiągniesz pomyślne rozwiązanie.

Krok 2: Wyświetl odwzorowania NAT na R2.

Jeśli NAT działa prawidłowo, powinny istnieć wpisy w tablicy odwzorowań.