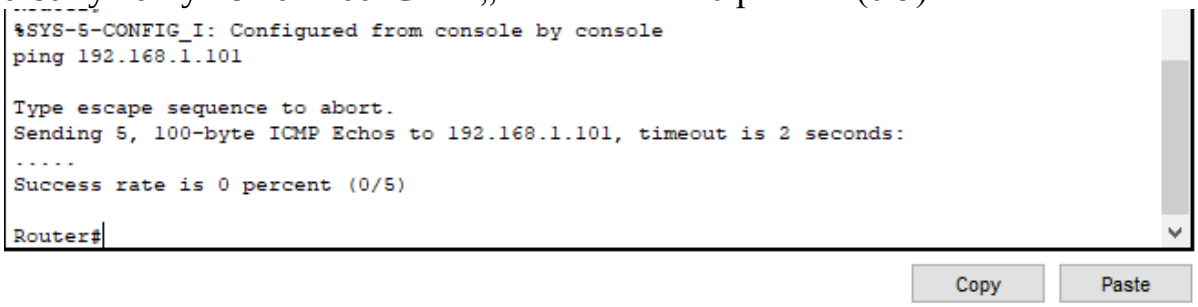
Zadanie 1:

Powód utraty komunikacji:

Utrata komunikacji wynika z tego, że RouterOS_2 został skonfigurowany jako klient DHCP na interfejsie eth2, co oznacza, że automatycznie uzyskuje adres IP od sieci lokalnej. Jednocześnie RouterOS_2 utracił domyślną bramę, co uniemożliwia mu przekazywanie ruchu między sieciami A i B.

Efekt wysłania ICMP Echo Request:

Wysłanie pakietu ICMP Echo Request z RouterOS_2 do PC1 nie powiedzie się, a otrzymamy komunikat ICMP „Succes rate is 0 percent (0/5)

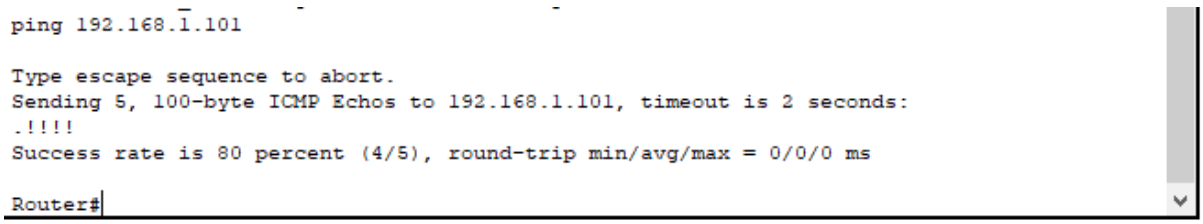


Powód braku dostępności:

Brak dostępności wynika z tego, że RouterOS_2 nie ma trasy domyślnej, a sieć A nie wie, jak dotrzeć do sieci B, ponieważ brama domyślna została usunięta.

Naprawa braku łączności:

Aby naprawić brak łączności, trzeba ponownie ustawić domyślną bramę na RouterOS_2 i skonfigurować trasę między sieciami A i B.



Dostęp do Internetu dla Sieci A:

Aby umożliwić dostęp do Internetu dla Sieci A, trzeba skonfigurować na RouterOS_2 funkcję NAT, aby przekazywał ruch między siecią lokalną a dostawcą internetu.

Zadanie 2:

NAT/PAT na RouterOS_1:

Konfigurujemy NAT/PAT na RouterOS_1

```
show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  192.168.2.1       192.168.1.1        ---                ---

Router#
```

Adres docelowy dla połączeń:

Adresem docelowym dla połączeń z zewnątrz jest adres publiczny routera, który następnie przekierowuje ruch na odpowiednie maszyny w sieci lokalnej. To adres publiczny routera jest używany do przekierowywania portów.

Zadanie 3:

Udostępnianie połączenia na Windows:

Skonfigurować udostępnianie połączenia na PC2, umożliwiając maszynie PC1 wirtualną dostęp do Internetu. Następnie, z zewnątrz, uzyskać dostęp do usługi, na przykład RDP, działającej na PC1.

Adresy IP i porty:

Adresy IP używane w tym połączeniu zależą od konfiguracji udostępniania połączenia. PC2 otrzymuje adres IP od dostawcy, a PC1 uzyskuje adres z zakresu przydzielonego przez PC2. Porty zależą od usługi, na przykład port 3389 dla RDP.

Zadanie 4:

Konfiguracja na systemie Linux:

Na systemie Linux (działającym jako router), ustawienie adresacji interfejsów, włączenie przekazywania pakietów, oraz uruchomienie maskarady dla interfejsu WAN (np. eth2). Następnie, powtórzyć polecenia takie jak w zadaniu 3, zapewniając komunikację i dostęp do Internetu dla PC1 wirtualnej maszyny.

Sprawozdanie z realizacji zadania 4:

Konfiguracja interfejsów:

Interfejsy sieciowe na systemie Linux zostały skonfigurowane w następujący sposób:

eth1: 192.168.1.1/24 (sieć wewnętrzna, PC1)

eth2: (dostęp do Internetu, np. DHCP)

Włączenie przekazywania pakietów:

Aby włączyć przekazywanie pakietów na bieżąco (bez restartowania systemu), można użyć polecenia:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

W celu ustawienia przekazywania pakietów po restarcie systemu, można zmodyfikować plik /etc/sysctl.conf dodając lub odkomentowując linię:

```
net.ipv4.ip_forward=1
```

Następnie, aby załadować nową konfigurację, użyj polecenia:

```
sysctl -p
```

Włączenie maskarady (NAT) na interfejsie WAN (eth2):

Aby włączyć maskaradę (Network Address Translation) na interfejsie WAN (eth2), można użyć narzędzia iptables. Przykładowe polecenie:

```
iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE
```

Powyższe polecenie dodaje regułę do tabeli NAT, która przekierowuje pakiety z interfejsu eth2 (wychodzące na Internet) i zmienia ich źródłowy adres IP na adres interfejsu eth2.

Dodatkowe kroki:

Konfiguracja ręczna tras w systemie Linux może być konieczna w przypadku bardziej zaawansowanych scenariuszy sieciowych.

W przypadku serwera DHCP na interfejsie WAN (eth2), system powinien automatycznie uzyskiwać adres IP.

Podsumowanie:

Po powyższej konfiguracji, PC1 powinien uzyskać dostęp do Internetu dzięki udostępnianiu połączenia przez system Linux.

Dostęp do Internetu z PC1 powinien być również testowany, na przykład poprzez przeglądarkę internetową lub polecenie ping.

Sprawdzenie połączenia z PC1:

Sprawdź połączenie z PC1, używając na przykład polecenia ping na adres zewnętrzny:

ping 8.8.8.8

Podsumowanie ogólne:

Sprawozdanie zawiera informacje dotyczące konfiguracji, kroków podjętych do umożliwienia dostępu do Internetu dla PC1, oraz testów poprawności działania konfiguracji.

Dokładna analiza i wytłumaczenie zastosowanych komend iptables, konfiguracji interfejsów, oraz przekazywania pakietów pomagają zrozumieć procesy zachodzące w systemie.