

# LABORATORIUM PROJEKTOWANIE I OBSŁUGA SIECI KOMPUTEROWYCH II

**Data wykonania  
ćwiczenia:**

27.04.2023

**Rok studiów:**

3

**Semestr:**

6

**Grupa studencka:**

2

**Grupa laboratoryjna:**

2B

**Ćwiczenie nr.**

13

**Temat:** Packet Tracer - Rozwiązywanie problemów z siecią korporacyjną

**Osoby wykonujące ćwiczenia:**

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

# Packet Tracer - Rozwiązywanie problemów z siecią korporacyjną

To ćwiczenie wykorzystuje różne technologie, które napotkałeś podczas studiów CCNA, w tym routing IPv4, routing IPv6, zabezpieczenia portów, EtherChannel, DHCP i NAT. Twoim zadaniem jest przejrzanie wymagań, wyodrębnienie i rozwiązywanie wszelkich problemów, a następnie udokumentowanie kroków podjętych w celu weryfikacji wymagań.

Firma wymieniła routery R1 i R3, aby umożliwić połączenie światłowodowe między lokalizacjami. Konfiguracje z poprzednich routerów z połączeniami szeregowymi zostały zmodyfikowane i zastosowane jako konfiguracja początkowa. Protokół IPv6 jest testowany na niewielkiej części sieci i wymaga weryfikacji.

## Część 1: Weryfikacja technologii przełączania

a. Konfiguracja zabezpieczeń portu jest ustawiona tak, aby tylko PC1 miał dostęp do interfejsu F0/3 na S1. Wszystkie naruszenia powinny wyłączyć interfejs.

Wydadaj polecenie na S1, aby wyświetlić bieżący stan zabezpieczeń portu.

```
S1# show port-security
```

b. Wejdź w tryb konfiguracji interfejsu dla interfejsu F0/3 i skonfiguruj zabezpieczenia portu.

```
S1(config)# interface f0/3  
S1(config-if)# switchport port-security  
S1(config-if)# switchport port-security mac-address sticky
```

c. Urządzenia w sieci LAN na S1 powinny znajdować się w VLAN 10. Wyświetl aktualny stan konfiguracji VLAN.

```
S1#show vlan
```

Które porty są obecnie przypisane do VLAN 10?

F0/3, F0/4

d. PC1 powinien otrzymać adres IP od routera R1.

Czy PC aktualnie ma przypisany adres IP?

Nie, ma tylko adres APIPA

e. Zauważ, że interfejs G0/1 na R1 nie znajduje się w tej samej sieci VLAN co PC1. Zmień interfejs G0/1, aby był członkiem VLAN 10 i ustaw portfast na interfejsie.

```
S1(config-if)# int G0/1
S1(config-if)# switchport access vlan 10
S1(config-if)# spanning-tree portfast
```

f. Zresetuj adres interfejsu na PC1 z poziomu interfejsu graficznego lub za pomocą wiersza polecenia i polecenia ipconfig /renew. Czy PC1 ma teraz adres? Tak, IP to 192.168.10.10 Jeśli nie, sprawdź jeszcze raz kroki. Przetestuj łączność z serwerem TFTP. Ping powinien być udany.

g. Sieć LAN podłączona do R3 miała dodany dodatkowy przełącznik do topologii. Skonfigurowano agregację łączy za pomocą EtherChannel na S2, S3 i S4. Linki EtherChannel powinny być ustawione jako trunk. Linki EtherChannel powinny być ustawione tak, aby tworzyły kanał bez użycia protokołu negocjacji. Wydadź polecenie na każdym przełączniku, aby sprawdzić, czy kanał działa poprawnie.

```
S2# show etherchannel summary
```

Czy były jakieś problemy z EtherChannel?

S3 pokazuje Po1 jako down (SD)

h. Zmień S3, aby zawierał porty F0/1 i F0/2 jako port kanałowy 1.

```
S3(config)# interface range f0/1-2
S3(config-if-range)# channel-group 1 mode on
```

Sprawdź status EtherChannel na S3. Powinien być teraz stabilny. Jeśli nie, sprawdź poprzednie kroki.

i. Zweryfikuj status trunka na wszystkich przełącznikach.

```
S3# show int trunk
```

Czy były jakieś problemy z trunkingiem?

S2 używa VLAN 1 jako domyślną sieć VLAN na interfejsie G0/1.

j. Popraw problemy z trunkingiem na S2.

```
S2(config)# int g0/1
S2(config-if)# switchport trunk native vlan 99
```

k. Protokół drzewa rozpinającego powinien być ustawiony na PVST+ na S2, S3 i S4. S2 powinien być skonfigurowany jako główny most dla wszystkich sieci VLAN. Wydadz polecenie, aby wyświetlić status drzewa rozpinającego na S2.

```
S2# show spanning-tree summary totals
```

Wynik polecenia pokazuje, że S2 nie jest głównym mostem dla żadnych sieci VLAN. Popraw status drzewa rozpinającego na S2.

l. Korekta statusu drzewa rozpinającego na S2.

```
S2(config)# spanning-tree vlan 1-1005 root primary
```

m. Sprawdź status drzewa rozpinającego na S2, aby zweryfikować zmiany.

```
S2# show spanning-tree summary totals
```

## Część 2: Weryfikacja DHCP

R1 jest serwerem DHCP dla sieci LAN R1.

R3 jest serwerem DHCP dla wszystkich 3 sieci LAN podłączonych do R3.

a. Sprawdź adresację komputerów.

Czy wszystkie mają poprawną adresację?

Nie, PC3 i PC4 mają nieprawidłowe bramy

b. Sprawdź ustawienia DHCP na R3. Filtrowanie wyjścia z polecenia show run, aby rozpocząć od konfiguracji DHCP.

```
R3# sh run | begin dhcp
```

Czy są jakiegokolwiek problemy z konfiguracją DHCP?

Ustawienie default-router jest nieprawidłowe w LAN40 i LAN50.

c. Dokonaj ewentualnych poprawek i zresetuj adresy IP na komputerach. Sprawdź łączność ze wszystkimi urządzeniami.

R

```
3(config)#ip dhcp pool LAN40
R3(dhcp-config)#network 192.168.40.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.40.1
R3(dhcp-config)#ip dhcp pool LAN50
R3(dhcp-config)#network 192.168.50.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.50.1
```

Zresetuj adres interfejsu na PC3, PC4 z poziomu interfejsu graficznego lub za pomocą wiersza polecenia i polecenia `ipconfig /renew`.

Czy udało się zpingować wszystkie adresy IPv4?

PC1, PC2, PC3 i PC4 powinny mieć pełną łączność dla IPv4 wewnętrznie. Hosty nie mogą pingować na zewnątrz. Ten problem zostanie rozwiązany w Części 3.

## Część 3: Weryfikacja routingu

Zweryfikuj, czy spełniono następujące wymagania. Jeśli nie, uzupełnij konfigurację.

Wszystkie routery są skonfigurowane z procesem OSPF ID 1 i nie należy wysyłać aktualizacji routingu przez interfejsy, które nie mają podłączonych routerów.

```
R3(config)#router ospf 1
R3(config-router)#passive-interface g0/1.30
R3(config-router)#passive-interface g0/1.40
R3(config-router)#passive-interface g0/1.50
```

R2 jest skonfigurowany z domyślną trasą IPv4 wskazującą na ISP i przekształca domyślną trasę w dziedzinie OSPFv2.

R2 jest skonfigurowany z pełną domyślną trasą IPv6 wskazującą na ISP i przekształca domyślną trasę w dziedzinie OSPFv3.

NAT jest skonfigurowany na R2 i żadne adresy nieprzetłumaczone nie są dozwolone w internecie.

a. Sprawdź tabele routingu na wszystkich routerach.

```
R3# show ip route ospf
```

Czy wszystkie sieci są obecne na wszystkich routerach?

Wszystkie sieci znajdują się w tabelach routingu. Jednak domyślna trasa nie jest propagowana do R1 i R3, więc istnieje łączność tylko z zewnątrz z R2.

b. Zpinguj Zewnętrzny Host z R2.

Czy ping był udany?

R2 powinien móc zpingować Zewnętrzny Host.

c. Popraw propagację domyślnej trasy.

```
R2(config)# router ospf 1
R2(config-router)# default-information originate
```

d. Sprawdź tabele routingu na R1 i R3, aby upewnić się, że domyślna trasa jest obecna.

e. Przetestuj łączność IPv6 z R2 do Zewnętrznego Hosta i Serwera TFTP. Pingi powinny być udane. Rozwiąż problemy, jeśli nie.

f. Przetestuj łączność IPv6 z R2 do PC4. Jeśli ping nie powiedzie się, upewnij się, że adresowanie IPv6 odpowiada tabeli adresów.

g. Przetestuj łączność IPv6 z R3 do Zewnętrznego Hosta. Jeśli ping nie powiedzie się, sprawdź trasy IPv6 na R3. Upewnij się, że domyślna trasa pochodząca z R2 jest poprawna. Jeśli trasa nie pojawi się, zmodyfikuj konfigurację IPv6 OSPF na R2.

```
R2(config)# ipv6 router ospf 1
R2(config-rtr)# default-information originate
```

h. Sprawdź łączność z R2 do Zewnętrznego Hosta. Ping powinien być udany.

## Część 4: Weryfikacja technologii WAN

Łącze szeregowo między R1 a R2 jest używane jako łącze zapasowe w przypadku awarii i powinno przenosić ruch tylko wtedy, gdy łącze światłowodowe jest niedostępne.

Połączenie Ethernetowe między R2 a R3 to połączenie światłowodowe.

Połączenie Ethernetowe między R1 a R3 to połączenie światłowodowe i powinno być używane do przesyłania ruchu z R1.

a. Dokładnie przyjrzyj się tabeli routingu na R1.

Czy istnieją jakieś trasy wykorzystujące łącze szeregowo?

Tak. Ruch dla sieci 192.168.20.0 i domyślna trasa są przesyłane przez S0/1/0, a nie G0/0/0.

Użyj polecenia traceroute, aby zweryfikować ewentualne podejrzane trasy.

```
R1# traceroute 192.168.20.254
```

Zauważ, że ruch jest przesyłany przez interfejs S0/1/0, a nie interfejs G0/0/0.

b. Oryginalne konfiguracje z poprzednich połączeń WAN szeregowych zostały przeniesione na nowe urządzenia. Porównaj ustawienia interfejsu G0/0/0 i Serial0/1/0. Zauważ, że oba mają ustawioną wartość kosztu OSPF. Usuń ustawienie kosztu OSPF z interfejsu G0/0/0. Konieczne będzie również usunięcie ustawienia na łączu na R3, które łączy się z R1.

```
R1(config)# int g0/0/0
R1(config-if)# no ip ospf cost 648
R3(config)# int g0/1/0
R3(config-if)# no ip ospf cost 648
```

c. Ponownie wydaj polecenie traceroute z R1, aby zweryfikować zmianę trasy.

d. Zmiana została dokonana, aby skierować ruch przez szybsze łącze, jednak trzeba przetestować trasę zapasową. Wyłącz interfejs G0/2/0 na R3 i przetestuj łączność z serwerem TFTP i Zewnętrznym Hostem.

Czy pingi były udane?

Serwer TFTP jest osiągalny; jednak Zewnętrzny Host nie jest osiągalny. Studenci powinni zastanowić się nad innymi przyczynami braku łączności. W tym przypadku jest to problem z brakiem ustawienia NAT jako wewnętrznego na interfejsie szeregowym na R2.

e. R2 musi wykonywać NAT dla wszystkich sieci wewnętrznych. Sprawdź translacje NAT na R2.

```
R2# show ip nat translations
```

f. Zauważ, że lista jest pusta, jeśli próbowałeś tylko zpingować z R1. Spróbuj zpingować z R3 do Zewnętrznego Hosta i ponownie sprawdź translacje NAT na R2. Wydaj polecenie wyświetlające bieżące statystyki NAT, które również dostarczą informacje o interfejsach zaangażowanych w NAT.

```
R2# show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/0
Inside Interfaces: GigabitEthernet0/1 , GigabitEthernet0/1/0
Hits: 17 Misses: 27
Expired translations: 17
Dynamic mappings:
```

g. Ustaw interfejs szeregowy 0/0/0 jako wewnętrzny, aby przekładać adresy.

```
R2(config)# int s0/0/0
R2(config-if)# ip nat inside
```

h. Przetestuj łączność ze Zewnętrznym Hostem z R1. Ping powinien teraz być udany. Ponownie włącz interfejs G0/2/0 na R3.

