Instrukcja laboratoryjna z przedmiotu: Sieci komputerowe

Ćwiczenie 13: Troubleshooting. Poszukiwanie podstawowych błędów w sieciach komputerowych

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

05.2022

I. Wprowadzenie

Skuteczne poszukiwanie i naprawianie błędów w sieciach komputerowych (wynikających zarówno z błędnej konfiguracji sieci, jak i uszkodzeń powstałych w wyniku eksploatacji) jest niezwykle ważną umiejętnością, którą musi posiadać administrator sieciowy.

Błędy powstające w wyniku normalnej eksploatacji często dotyczą warstwy fizycznej — uszkodzeniu ulegają złącza RJ-45, skrętki ulegają przetarciu. Tego typu błędy po stronie użytkownika objawiają się albo pogorszeniem jakości łącza (przerywaniem Internetu, obniżeniem prędkości łącza) lub w skrajnych przypadkach nawet utratę dostępu do Internetu. O występowaniu problemów tego typu można się przekonać poprzez wyświetlenie statystyk portu (*show interface fa0/0*) i zaobserwowanie błędów w transmisji, np. CRC, kolizji, niepełnych ramek, a także braku obecności danego adresu MAC w tablicy MAC adresów przełącznika (*show mac address-table*).

Błędy dotyczące warstwy sieciowej (adresacji IP, tras statycznych) pojawiają się najczęściej podczas konfigurowania urządzenia (lub zmiany konfiguracji w sieci). Błędnie przypisane adresy IP na stacjach roboczych lub interfejsach urządzeń sieciowych, np. ustawienie adresów niebędących w ramach jednej podsieci tam, gdzie komunikacja powinna odbywać się lokalnie może poskutkować zupełnym brakiem komunikacji z danym urządzeniem.

Błędna konfiguracja bramy domyślnej powoduje, że dane urządzenie będzie w stanie komunikować się z urządzeniami jedynie w swojej podsieci, a urządzenia z innych podsieci będą dla takiego urządzenia nieosiągalne. Konfigurację IP warto weryfikować komendą *show ip interface brief*.

Skonfigurowanie niepoprawnych tras statycznych (błędne dane o sieci czy wyjściowym interfejsie) lub brak trasy ostatniej szansy, przy wyłączonych protokołach routingu, może doprowadzić do tego, że urządzenia z sieci obsługiwanych przez dany router nie będą w stanie skomunikować się z urządzeniami z sieci podłączonych do jakiegokolwiek innego routera. Konfigurację tras na routerze można sprawdzić komendą *show ip route*.

II. Cel ćwiczenia

Celem niniejszego ćwiczenia jest zdobycie umiejętności poszukiwania podstawowych błędów istniejących w sieciach komputerowych i ich naprawiania:

- błędy związane z adresacją IP,
- błędnie skonfigurowane trasy statyczne.

III. Stanowisko laboratoryjne

Do wykonania ćwiczenia niezbędne jest stanowisko laboratoryjne składające się z komputera z zainstalowanym programem Cisco Packet Tracer.

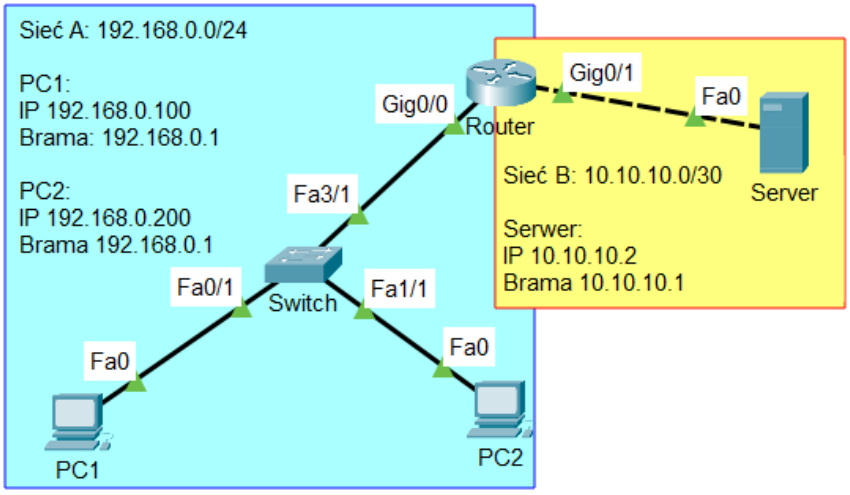
IV. Przebieg ćwiczenia

W przebiegu tego ćwiczenia masz za zadanie znaleźć błędy w konfiguracji sieci w 5 przygotowanych przypadkach. W każdym z przypadków postępuj według poniższego schematu:

1. W nowym projekcie w programie Packet Tracer umieść sieć zaprezentowaną w danym przypadku — wstaw właściwe urządzenia i połącz je odpowiednimi kablami.
2. Wprowadź podaną w ćwiczeniu konfigurację — skonfiguruj adresację IP na komputerach, przekopiuj konfigurację switchy/routerów i wklej ją, będąc w trybie konfiguracji globalnej na każdym z urządzeń.
3. Przeczytaj opis problemu i przeszukaj konfigurację urządzeń w celu jego naprawienia.
4. Napraw znaleziony błąd i przekonaj się, że sieć działa już poprawnie.

1 Problem: Niemożność skomunikowania się z serwerem

Problem: Próba połączenia się z serwerem (nawet wysłanie pinga na adres IP serwera) z komputerów PC1 i PC2 kończy się niepowodzeniem, podczas gdy komputery PC1 i PC2 komunikują się ze sobą bez przeszkód. Port, do którego podłączony jest serwer, ma status *up*.



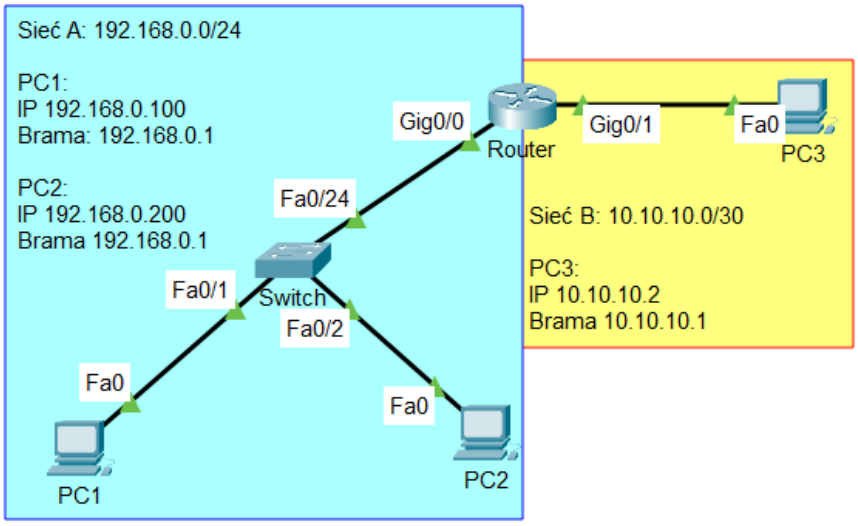
Konfiguracja routera:

```
hostname R1
enable password cisco
banner motd % Unauthorized access prohibited %
line vty 0
password cisco
login
line con 0
password cisco
login
exit
interface g0/0
ip address 10.10.10.1 255.255.255.252
no shutdown
interface g0/1
ip address 192.168.0.1 255.255.255.0
no shutdown
```

Co jest źródłem problemu?

2 Problem: Niemożność stelnetowania się na switch z zewnętrznych sieci

Problem: Próba stelnetowania się na switch z komputera PC3 kończy się niepowodzeniem, podczas gdy z komputerów PC1 i PC2 telnetowanie udaje się bez przeszkód.



Konfiguracja routera:

```
hostname R1
enable password cisco
banner motd % Unauthorized access prohibited %
line vty 0
password cisco
login
line con 0
password cisco
login
exit
interface g0/0
ip address 192.168.0.1 255.255.255.0
no shutdown
interface g0/1
ip address 10.10.10.1 255.255.255.252
no shutdown
```

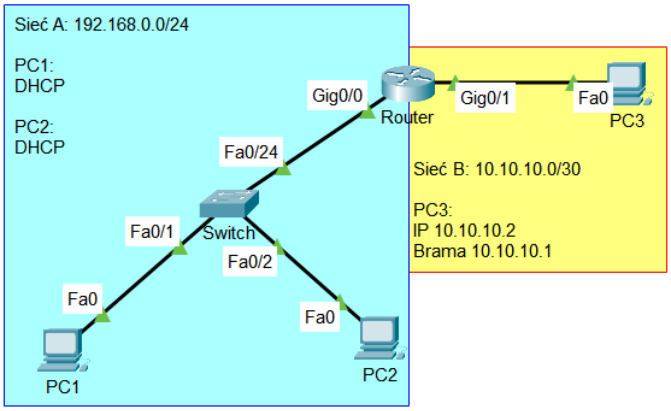
Konfiguracja switcha:

```
hostname SW
enable password cisco
banner motd % Unauthorized access prohibited %
line vty 0
password cisco
login
line con 0
password cisco
login
exit
interface vlan1
ip address 192.168.0.254 255.255.255.0
no shutdown
```

Co jest źródłem problemu?

3 Problem: Niedziałający serwer DHCP

Problem: Próba uzyskania adresów IP automatycznie (przez DHCP) przez komputery PC1 i PC2 kończy się niepowodzeniem.



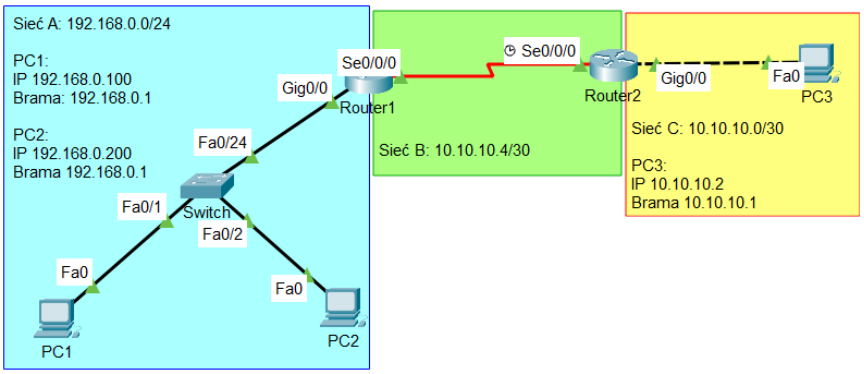
Konfiguracja routera:

```
hostname R1
enable password cisco
banner motd % Unauthorized access prohibited %
line vty 0
password cisco
login
line con 0
password cisco
login
exit
interface g0/0
ip address 192.168.0.1 255.255.255.0
no shutdown
interface g0/1
ip address 10.10.10.1 255.255.255.252
no shutdown
exit
ip dhcp excluded-address 192.168.0.1
ip dhcp excluded-address 192.168.0.254
ip dhcp pool Pula
network 192.168.0.128 255.255.255.128
default-router 192.168.0.1
```

Co jest źródłem problemu?

4 Problem: Brak połączenia z hostami z dalszych sieci

Problem: Próba połączenia pomiędzy hostami z sieci A a hostami z sieci C nie udaje się.



Konfiguracja routera R1:

```
hostname R1
enable password cisco
banner motd % Unauthorized access prohibited %
line vty 0
password cisco
login
line con 0
password cisco
login
exit
interface g0/0
ip address 192.168.0.1 255.255.255.0
no shutdown
interface s0/0/0
ip address 10.10.10.5 255.255.255.252
no shutdown
```

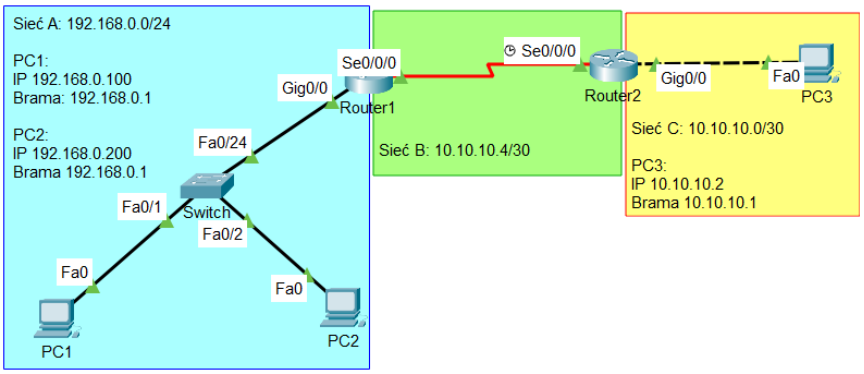
Konfiguracja routera R2:

```
hostname R2
enable password cisco
banner motd % Unauthorized access prohibited %
line vty 0
password cisco
login
line con 0
password cisco
login
exit
interface g0/0
ip address 10.10.10.1 255.255.255.252
no shutdown
interface s0/0/0
ip address 10.10.10.6 255.255.255.252
no shutdown
```

Co jest źródłem problemu?

5 Problem: Pingi do hostów z dalszych sieci skuteczne w 50%

Problem: Próba połączenia pomiędzy hostami z sieci A a hostami z sieci C udaje się w ok. 50% (niektóre pingi przechodzą, inne nie).



Konfiguracja routera R1:

```
hostname R1
enable password cisco
banner motd % Unauthorized access prohibited %
line vty 0
password cisco
login
line con 0
password cisco
login
exit
interface g0/0
ip address 192.168.0.1 255.255.255.0
no shutdown
interface s0/0/0
ip address 10.10.10.5 255.255.255.252
no shutdown
ip route 0.0.0.0 0.0.0.0 g0/0
ip route 0.0.0.0 0.0.0.0 s0/0/0
```

Konfiguracja routera R2:

```
hostname R2
enable password cisco
banner motd % Unauthorized access prohibited %
line vty 0
password cisco
login
line con 0
password cisco
login
exit
interface g0/0
ip address 10.10.10.1 255.255.255.252
no shutdown
interface s0/0/0
ip address 10.10.10.6 255.255.255.252
no shutdown
ip route 0.0.0.0 0.0.0.0 g0/0
ip route 0.0.0.0 0.0.0.0 s0/0/0
```

Co jest źródłem problemu?

V. Pytania kontrolne

1. Jakie będą konsekwencje niewłaściwego skonfigurowania tras statycznych na routerze?
2. Jakie będą konsekwencje niewłaściwego skonfigurowania bramy domyślnej na urządzeniach końcowych?
3. Wymień typowe błędy w konfiguracji urządzeń sieciowych, jakie mogą się pojawić.

Odpowiedzi:

Problem 1: Błędnie przypisane adresy IP na interfejsach routera. Na interfejsie g0/0 powinien być przypisany adres 192.168.0.1 z maską 255.255.255.0 z podsieci A, a na interfejsie g0/1 — adres 10.10.10.1 z maską 255.255.255.252 z podsieci B.

Problem 2: Brak skonfigurowanej bramy domyślnej na switchu: należałoby w trybie konfiguracji globalnej na switchu wpisać komendę *ip default-gateway 192.168.0.1*

Problem 3: Niewłaściwa maska podana przy konfiguracji puli DHCP: należy zmodyfikować pulę poleceniem *network 192.168.0.0 255.255.255.0*

Problem 4: Brak skonfigurowanych tras ostatniej szansy na routerach: w trybie konfiguracji globalnej obu routerów należałoby wydać komendę *ip route 0.0.0.0 0.0.0.0 s0/0/0*

Problem 5: Na routerach występują dwie statyczne trasy ostatniej szansy: należy usunąć niewłaściwe trasy komendą *no ip route 0.0.0.0 0.0.0.0 g0/0*