

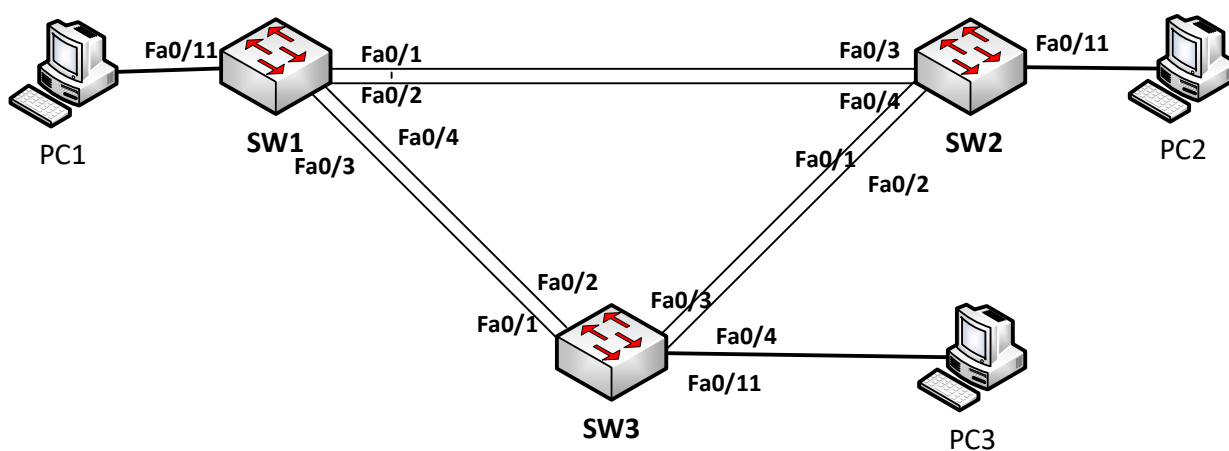
Ćwiczenie Spanning Tree Protocol

Teoria:)

Protokół Spanning Tree Protocol (STP) stosowany jest w sieciach Ethernet w celu zapobiegania pętlom na poziomie warstwy 2, a także w celu wyboru optymalnych ścieżek przesyłania danych. W protokole STP koszt ścieżki (ang. path cost) odgrywa kluczową rolę w wyborze optymalnego drzewa rozpinającego. Wartość kosztu ścieżki zależy od prędkości łącza.

Zadanie 1

W Packet Tracer zaimplementuj sieć zgodnie z topologią pokazaną na rysunku 1.



Rysunek 1. Topologia sieci

W Packet Tracer zaimplementuj sieć zgodnie z topologią pokazaną na rysunku 1, lub wykorzystaj plik z wdrożoną topologią sieci: *cw_10_STP_topologia.pkt*

W tabeli 1 przedstawiono adresację dla poszczególnych urządzeń a w tabeli 2 przydziel portów do odpowiednich VLAN'ów.

Tabela 1. Adresacja komputerów i przełączników (interface vlan99)

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
SW1	VLAN 99	172.30.99.1	255.255.255.0	-
SW2	VLAN 99	172.30.99.2	255.255.255.0	-
SW3	VLAN 99	172.30.99.3	255.255.255.0	-
PC1	NIC	172.30.10.1	255.255.255.0	172.30.10.254
PC2	NIC	172.30.20.1	255.255.255.0	172.30.20.254
PC3	NIC	172.30.30.1	255.255.255.0	172.30.30.254

Tabela 2. Przynależność portów do VLAN'wo

Porty	VLAN
SW1 F0/11	VLAN 10
SW2 F0/11	VLAN 20
SW3 F0/11	VLAN 30

Celem ćwiczenia jest skonfigurowanie sieci VLAN oraz połączenia **trunk** pomiędzy przełącznikami, sprawdzenie i skonfigurowanie pierwszorzędnych i drugorzędnych mostów głównych protokołu STP, następnie zoptymalizowanie topologii przełączników za pomocą **Rapid PVST**, **PortFast** i **BPDU guard**.

Wykonaj następujące czynności:

- Nazwij przełączniki zgodnie z rysunkiem 1.
- Utwórz na wszystkich przełącznikach następujące VLAN'y: 10, 20, 30 i 99.

```
SW1(config)# vlan 10
SW1(config-vlan)# vlan 20
SW1(config-vlan)# vlan 30
SW1(config-vlan)# vlan 99
```

*Te same czynności należy powtórzyć na **Sw2** i **Sw3***

- Ustaw na przełącznikach port **fa0/11** na tryb dostępu i przypisz port przełącznika do sieci VLAN zgodnie z tabela 2.2 następnie zweryfikuj konfigurację.

```
SW1(config)# interface f0/11
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
```

```
SW2(config)# interface f0/11
SW2(config-if)# switchport mode access
SW2(config-if)# switchport access vlan 20
```

```
SW3(config)# interface f0/11
SW3(config-if)# switchport mode access
SW3(config-if)# switchport access vlan 30
```

Weryfikacja: na każdym przełączniku wykonaj:

```
SW1# show vlan brief
```

- Skonfiguruj porty **fa0/1-4** jako **trunk**

```
SW1(config)# interface range f0/1-4
SW1(config-if-range)# switchport mode trunk
```

```
SW2(config)# interface range f0/1-4
SW2(config-if-range)# switchport mode trunk
```

```
SW3(config)# interface range f0/1-4
SW3(config-if-range)# switchport mode trunk
```

- Skonfiguruj adres na interfejsach zarządzania na wszystkich trzech przełącznikach zgodnie z tabela 2.1

```
SW1(config)# interface vlan99
SW1(config-if)# ip address 172.30.99.1 255.255.255.0

SW2(config)# interface vlan99
SW2(config-if)# ip address 172.30.99.2 255.255.255.0

SW3(config)# interface vlan99
SW3(config-if)# ip address 172.30.99.3 255.255.255.0
```

- f. Upewnij się, że przełączniki są prawidłowo skonfigurowane poprzez sprawdzenie komunikacji pomiędzy nimi (polecenie ping). Sprawdź konfigurację **STP** na każdym z przełączników za pomocą polecenia:

```
SW1# show spanning-tree
```

Przeanalizuj status protokołu **STP**, który przełącznik jest **root primary**, a który **root secondary**? Czy dla każdego z **VLAN**ów sytuacja przedstawia się tak samo?

- g. Konfigurowanie trybu STP. Użyj polecenia `spanning-tree mode`, aby skonfigurować przełączniki tak, żeby używały Rapid PVST jako tryb STP.

```
SW1(config)# spanning-tree mode rapid-pvst
SW2(config)# spanning-tree mode rapid-pvst
SW3(config)# spanning-tree mode rapid-pvst
```

Przeanalizuj status protokołu **STP**, czy coś się zmieniło ?

- h. Konfiguracja Spanning Tree i równoważenie obciążenia.

Skonfiguruj **S1**, aby był pierwszorzędnym przełącznikiem głównym dla sieci VLAN 1, 10. Skonfiguruj **S3**, aby był pierwszorzędnym przełącznikiem głównym dla sieci VLAN 20, 30, 99.

```
SW1(config)# spanning-tree vlan 1,10 root primary
SW3(config)# spanning-tree vlan 20,30,99 root primary
```

Sprawdź konfigurację na każdym z przełączników za pomocą polecenia

```
SW1# show spanning-tree
```

- i. Konfiguracja PortFast i BPDU guard na przełącznikach.

```
SW1(config)# interface f0/11
SW1(config-if)# spanning-tree portfast
SW1(config-if)# spanning-tree bpduguard enable

SW2(config)# interface f0/11
SW2(config-if)# spanning-tree portfast
SW2(config-if)# spanning-tree bpduguard enable

SW3(config)# interface f0/11
SW3(config-if)# spanning-tree portfast
SW3(config-if)# spanning-tree bpduguard enable
```

Użyj polecenia **show running-config**, aby sprawdzić konfigurację.

Zadanie 2 - Opcjonalne

1. Zapewnij łączność pomiędzy VLAN'ami 10,20,30. Wskazówka: dodaj ruter lub przełącznik warstwy 3 i go skonfiguruj).
2. Skonfiguruj komputery PC1,PC2,PC3 i przetestuj łączność pomiędzy nimi.
3. Dodatkowo połącz przełączniki z wykorzystaniem portów GigabitEthernet, połączenia skonfiguruj jako trunk.
4. Obserwuj zachowanie sieci

Uzupełnienie teoretyczne:

PortFast

Opis działania:

- **default** w kontekście PortFast automatycznie włącza funkcję **PortFast** na wszystkich portach przełącznika skonfigurowanych jako porty dostępne (access ports).
- PortFast powoduje, że porty natychmiast przechodzą do stanu **forwarding** po aktywacji, bez przechodzenia przez standardowe fazy STP (Listening i Learning). To przyspiesza komunikację dla urządzeń końcowych, takich jak komputery, które nie uczestniczą w procesie STP.
- Ważne: PortFast nie wyłącza STP na porcie – jeśli na porcie zostaną odebrane BPDU, port nadal może uczestniczyć w STP lub zareagować zgodnie z konfiguracją BPDU Guard lub BPDU Filter.

Zastosowanie:

- Przyspiesza aktywację portów dla urządzeń końcowych.
- Jest to wygodne rozwiązanie dla portów podłączonych do hostów, które nie biorą udziału w protokole STP, takich jak komputery czy drukarki.

Konfiguracja:

- Włączenie PortFast na wszystkich portach dostępowych (access ports):

Switch(config)# spanning-tree portfast default

- Włączenie PortFast na porcie

Switch(config-if)# spanning-tree portfast

BPDU Guard

Opis działania:

- **BPDU Guard** służy do natychmiastowego wyłączenia portów, które otrzymają **BPDU**, jeśli zostały skonfigurowane jako porty **PortFast**. Port jest wyłączany (stan **err-disable**), ponieważ PortFast zakłada, że port jest podłączony do urządzeń końcowych, które nie uczestniczą w wymianie BPDU.
- **BPDU Guard** działa jako mechanizm ochrony przed błędną konfiguracją lub próbą podłączenia przełącznika do portu, który powinien obsługiwać jedynie urządzenia końcowe.
- **Działanie globalne:** BPDU Guard włącza ochronę na wszystkich portach z PortFast.
- **Działanie na poziomie portu:** Może być także włączony indywidualnie na wybranych portach, niezależnie od tego, czy PortFast jest skonfigurowany globalnie.

Zastosowanie:

- Idealne rozwiązanie, aby chronić porty przeznaczone dla urządzeń końcowych przed niepożądaną wymianą BPDU (np. w przypadku przypadkowego podłączenia innego przełącznika).
- Zapobiega tworzeniu się pętli w sieci poprzez natychmiastowe wyłączenie portu po wykryciu BPDU.

Konfiguracja:

- **Globalnie:**

Switch(config)# spanning-tree portfast bpduguard default

- **Na poziomie portu:**

Switch(config-if)# spanning-tree bpduguard enable