Firma CISCO jest wiodącym producentem urządzeń sieciowych, w tym również przełączników (ang. **switch**). W tym wpisie przedstawię podstawowe polecenie konsoli zarządzania przełącznikiem CISCO oraz pokażę wynik działania poszczególnych poleceń.
Zanim przejdę do omówienia poszczególnych poleceń, zacznę od opisu poziomów dostępu do poleceń konfiguracji przełącznika. W urządzeniach firmy CISCO wyróżniamy dwa takie poziomy:

- 
  - **tryb podstawowy** (***User EXEC***) – w konsoli oznaczony jako ***Switch>***, uniemożliwiający dokonywanie zmian w konfiguracji urządzenia, pozwalający natomiast na np. wyświetlanie informacji o bieżącej konfiguracji, jest on domyślnie uruchamiany przy wejściu do konsoli zarządzania,

- **tryb uprzywilejowany** (***Privileged EXEC)***– w konsoli oznaczony jako ***Switch***#, umożliwiający dokonywanie zmian w konfiguracji, przejście do tego trybu z ***User EXEC*** odbywa się po wpisaniu polecenia ***enable.***

Z trybu uprzywilejowanego (***Privileged EXEC***) mamy możliwość dokonywania zmian w konfiguracji:

- **globalnej** – w konsoli oznaczony jako ***Switch(config)*** #, pozwalający na np. zmianę nazwy systemowej, określanie haseł dostępu czy tworzenie sieci **VLAN**, przejście do tego trybu z ***Privileged EXEC*** odbywa się po wpisaniu polecenia ***configure terminal,***
- **szczególowej** – w konsoli oznaczony jako ***Switch(config-%nazwa%)*** #, pozwalający na dokonywanie wszelkich innych zmian konfiguracyjnych, takich jak: konfiguracja interfejsów sieciowych, określanie trybu pracy poszczególnych portów czy zabezpieczenia ich przed niepowołanym dostępem, przejście do tego trybu z konfiguracji globalnej odbywa się po wpisaniu polecenia odpowiadającego konkretnym ustawieniom, i tak przykładowo, jeśli chcemy dokonać zmian w konfiguracji pierwszego interfejsu Ethernet wpisujemy ***interface fastEthernet 0/1****, wówczas tryb w konsoli oznaczony będzie jako* ***Switch(config-if)#***

Kiedy chcemy opuść dany tryb konfiguracji, np. chcemy wrócić z trybu konfiguracji **szczegółowej** do **globalnej** wystarczy, że wprowadzimy polecenie ***exit,*** natomiast kiedy chcemy przejść bezpośrednio do trybu uprzywilejowanego, bez wzgledu na to, w kótrym trybie się znajdujemy wprowadzamy poleceni ***end.***
Podczas pracy w konsoli zarządzania bardzo przydatne są dwie funkcję:

- dopełnienie – wystarczy wpisać początek polecenia, np: ***en*** i nacisnąć klawisz **TAB** na klawiaturze, a system dopełni nam poleceni do ***enable***,

- podpowiedzi – kiedy nie jesteśmy pewni składni polecenie możemy wpisać znak zapytania (**?**), a system wyświetl nam dostępne dla danego trybu polecenia.

Przedstawię teraz klika podstawowych poleceni konsoli służących do zarządzania przełącznikiem CISCO

- 
  - Wyświetlenie tablicy **ARP:**
    - 
    - **`Switch>show arp`**
  - Wyświetlenie bieżącej konfiguracji interfejsów przełącznika:
    - 
    - **`Switch>show interfaces`**
  - Wyświetlenie tablicy **MAC**:
    - 
    - **`Switch>show mac-address-table`**
  - Wyświetlenie istniejących sieci **VLAN**:
    - 
    - **`Switch>show vlan`**
  - Ustawienie hasła przejścia do trybu konfiguracyjnego:
    - 
    - **`Switch>enable`**
    - **`Switch#configure terminal`**
    - **`Switch#enable secret`**
      **`qwerty`** //zamiast *qwerty* można wpisać dowolne hasło
- Zmiana nazwy systemowej urządzenia:
  - 
    - **`Switch>enable`**
    - **`Switch#configure terminal`**
    - **`Switch#hostname szkolny`** //zamiast *szkolny* można wpisać dowolną nazwę
    - **`szkolny#`** **<-** od teraz nasz przełącznik będzie wyświetlał nową nazwę
- Zapisanie zmian konfiguracji:
  - 
    - **`szkolny#copy running-config startup-config`** i potwierdzamy klawiszem**ENTER**

**Ćwiczenie do wykonania:**

Pobierz plik programu Cisco Packet Tracer (plik został przygotowany w wersji 6.1 oraz spakowany) i wykonaj zadanie w nim zapisane.

W dzisiejszych czasach duży nacisk kładziony jest na bezpieczeństwo systemów informatycznych i sieci komputerowych. Istnieje wiele sposobów zabezpieczenia sieci komputerowych przed niepowołanym dostępem, jedne opierają się na zabezpieczeniach systemów operacyjnych, inne zaś na odpowiedniej konfiguracji sprzętu sieciowego. W dzisiejszym artykule przedstawię sposób zabezpieczenia fizycznego dostępu do zasobów naszej sieci komputerowej, poprzez takie ustawienia przełącznika CISCO, aby mógł on obsługiwać tylko jeden adres MAC (przełączniki na podstawie tego parametru przesyłają dane w sieci -przyp.), każdorazowe podłączenie urządzenia z innym adresem fizycznym niż ten zapisane w konfiguracji, spowoduje zablokowanie portu i uniemożliwi korzystanie z sieci. Uzasadnienie takiego sposobu zabezpieczenia jest proste, mianowicie uniemożliwi na korzystanie z naszej sieci urządzeniom spoza niej.

Zadanie zostanie omówione na przykładzie 3 komputerów podłączonych do przełącznika.

Konfigurację przełącznika powinniśmy zacząć od pozyskania adresów MAC urządzeń, które są do niego podłączone. Najłatwiej jest to zrobić wykonując poprzez wyświetlenie tablicy adresów MAC w konsoli:

- **Switch>enable**
- **Switch#show mac-address-table**

W wyniku wykonania polecenia zostanie wyświetlona tabela z adresami MAC przypisanym do danego interfejsu:

```
Vlan      Mac Address         Type      Ports
 1      0001.9666.099c     DYNAMIC    Fa0/1
 1      0060.3ed6.41eb     DYNAMIC    Fa0/2
 1      0060.5c52.b33e     DYNAMIC    Fa0/3
```

Skoro udało nam się pozyskać już adresy MAC naszym komputerów, możemy przejść teraz do etapu przypisywania ich do konkretnego portu przełącznika:

Z trybu uprzywilejowanego (***Switch***#) przejdziemy do trybu konfiguracji globalnej (***Switch(config)***#), a następnie do trybu konfiguracji szczegółowej interfejsu 0/1:

- **Switch#configure terminal**
- **Switch(config)#interface fastEthernet 0/1**

W tym miejscu wykonamy polecenia, które przypiszą adres MAC pierwszego komputera do tego interfejsu:

- **Switch(config-if)#switchport mode access**
- **Switch(config-if)#switchport port-security**
- **Switch(config-if)#switchport port-security maximum 1**
- **Switch(config-if)#switchport port-security mac-address 0001.9666.099c**

- **Switch(config-if)#exit** //opuszczamy tryb konfiguracji szczegółowej dla interfejsu 0/1

Przechodzimy do trybu konfiguracji szczegółowej dla interfejsu fastEthernet 0/2 i przypisujemy adres MAC drugiego komputera:

- **Switch(config)#interface fastEthernet 0/2**
- **Switch(config-if)#switchport mode access**
- **Switch(config-if)#switchport port-security**
- **Switch(config-if)#switchport port-security maximum 1**
- **Switch(config-if)#switchport port-security mac-address 0060.3ed6.41eb**
- **Switch(config-if)#exit**

Następnie przechodzimy do trybu konfiguracji szczegółowej dla interfejsu fastEthernet 0/3 i przypisujemy adres MAC trzeciego komputera:

- **Switch(config)#interface fastEthernet 0/3**
- **Switch(config-if)#switchport mode access**
- **Switch(config-if)#switchport port-security**
- **Switch(config-if)#switchport port-security maximum 1**
- **Switch(config-if)#switchport port-security mac-address 0060.5c52.b33e**
- **Switch(config-if)#exit**

Na koniec powinniśmy wyłączyć pozostałe interfejsy, tak aby do nich nie mógł się wpiąć żaden inny komputer, a następnie zapisać konfigurację urządzenia:

- **Switch(config)#interface range fastEthernet 0/4-24** //przejście do trybu konfiguracji grupy interfejsów od 4 do 24
- **Switch(config-if-range)#shutdown** //wyłączenie interfejsów
- **Switch(config-if-range)#end**
- **Switch#copy running-config startup-config** //zapisanie konfiguracji

Od teraz każdorazowe podłączenie do jednego z 3 portów urządzenia z innym adresem MAC niż ten przypisane spowoduje zablokowanie interfejsu. Aby go odblokować należy w trybie konfiguracji szczegółowej danego interfejsu wykonać polecenie ***no shutdown***:

- **Switch>enable**
- **Switch#configure terminal**
- **Switch(config)#interface fastEthernet 0/1**
- **Switch(config-if)#no shutdown**

Przedstawiony powyżej sposób zabezpieczenia sieci komputerowej jest tylko jednym z wielu i nie powinien być stosowany jako jedyny. Zawsze należy stosować kilka rodzajów zabezpieczeń, zarówno sprzętowych jak i

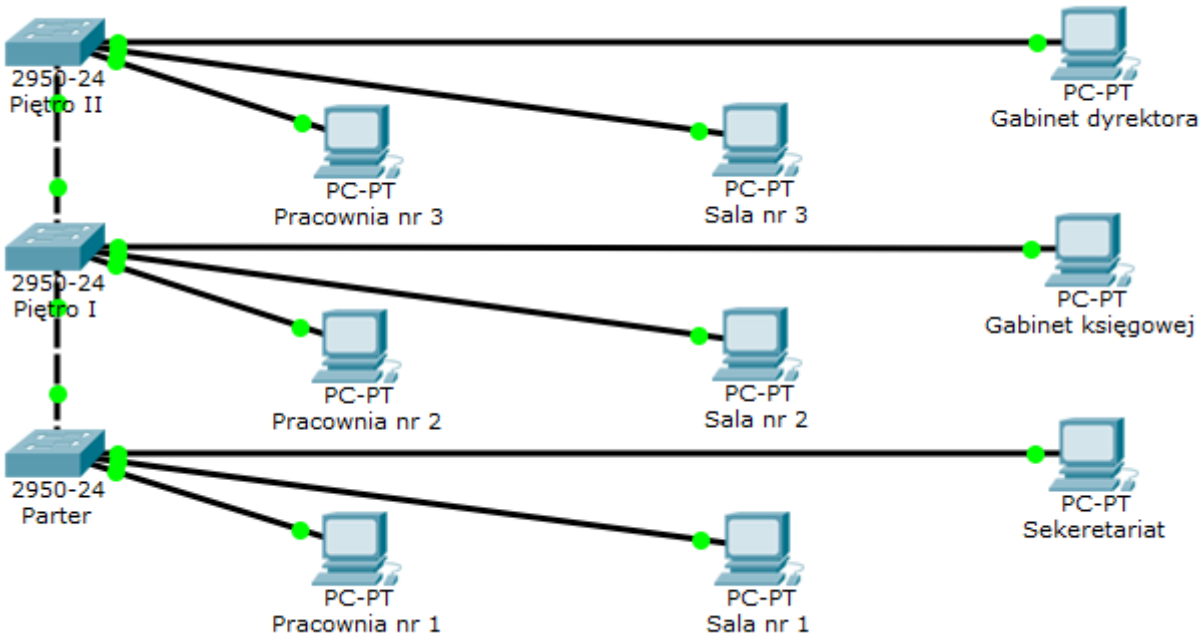
programowych, aby skutecznie zabezpieczyć naszą się przez nieupoważnionym dostępem.

**Ćwiczenie do wykonania:**

Pobierz plik programu Cisco Packet Tracer (plik został przygotowany w wersji 6.1) i wykonaj zadanie w nim zapisane.

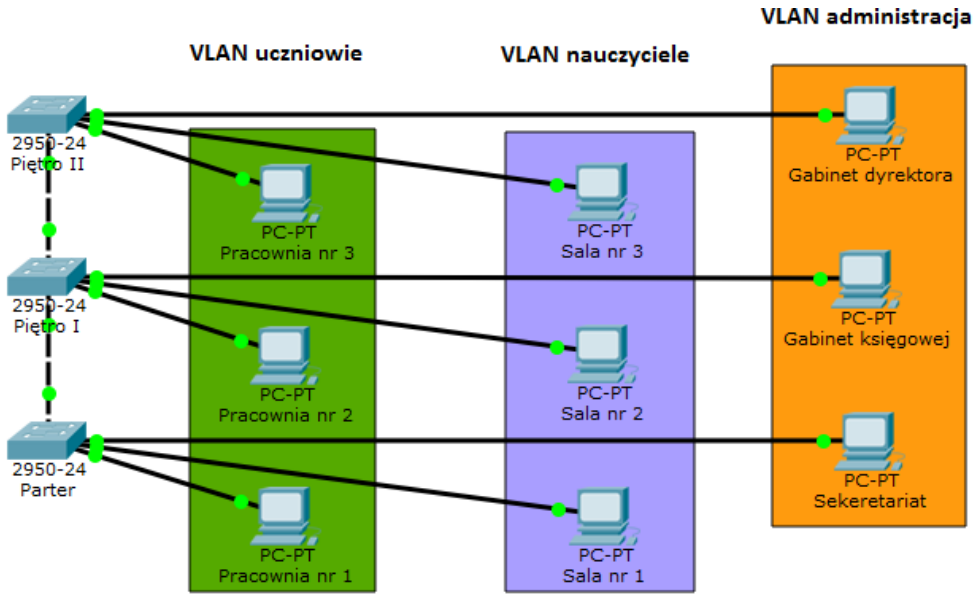
Sieć **VLAN** (ang. **Virtual LAN**) jest to mechanizm pozwalający administratorom dzielić sieć lokalną na mniejsze logiczne sieci, do których należą komputery znajdujące się w fizycznie różnych lokalizacjach (np. na różnych piętrach).
Wyobraźmy sobie szkolną sieć komputerową, do której dostęp maja trzy grupy użytkowników: administracja, nauczyciele oraz uczniowie. Każda z tych grup ma inne uprawnienia oraz dostęp do różnych zasobów sieci. W jaki sposób zorganizować sieć, aby dokonać pogrupowania użytkowników w zależności od tych uprawnień czy dostępu do zasobów? Można podłączyć komputery grupy administracyjnej do jednego przełącznika, nauczycielskiej do drugiego, uczniowskiej do trzeciego. Proste, prawda? Tak, pod warunkiem, że na danym piętrze znajdują się tylko komputery jednej grupy, np. na parterze (gdzie znajduje się pierwszy przełącznik) znajdują się tylko komputery administracji, na I piętrze (gdzie znajduje się drugi przełącznik) są tylko komputery nauczycielskie, a na II piętrze (gdzie znajduje się trzeci przełącznik) znajdują się tylko komputery uczniowskie. Niestety, z taką sytuacją prawie nigdy się nie spotkamy, ponieważ zazwyczaj jest tak, że na danym piętrze występują użytkownicy należący do różnych grup, a ich komputery podłączone są do tego samego przełącznika. Wówczas zastosować możemy podział sieci lokalnej na mniejsze, logiczne obszary (sieci **VLAN**).

Poniższy rysunek obrazuje nam sytuację, o której mówiłem, a mianowicie sieć, w której mamy 3 grupy użytkowników, których komputery podłączone są do różnych przełączników.




Jak widać, na każdym piętrze, do tych samych przełączników podłączone są komputery różnych grup użytkowników (pracownie to komputery uczniowskie, sale to komputery nauczycielskie, a pozostałe to komputery administracji). W takiej sytuacji, aby pogrupować komputery zastosujemy opisany wyżej

sposób, czyli stworzymy wirtualne sieci LAN. Wówczas, logiczny podział takiej sieci wyglądał będzie następująco:




Schemat takiego podziału będzie przedstawiał się nastepująco:

1. Komputery w pracowniach należeć będą do sieci **VLAN** o nazwie **uczniowie**
2. Komputery w salach należeć będą do sieci **VLAN** o nazwie **nauczyciele**
3. Komputery pracowników administracji należeć będą do sieci **VLAN** o nazwie **administracja**.

Tyle teorii… Przejdźmy teraz do konfiguracji urządzeń.

Zanim jednak to zrobimy powinniśmy nadać sieciom wirtualnym identyfikator i zaprojektować dla nich**adresację IP**. Aby zadania dodatkowo nie komplikować, proponuje przyjąć następujące zasady:

1. VLAN **uczniowie** będzie miał przypisany identyfikator **10** (może być inny z zakresu 2-1001, nie ma większego znaczenie jaki Wy wybierzecie), a adres

   IP dla tej sieci VLAN będzie miał postać: **192.168.10.0/24**.

2. VLAN **nauczyciele** będzie miał przypisany identyfikator **20**, zatem adres IP dla tej sieci VLAN będzie miał postać: **192.168.20.0/24**.
3. VLAN **administracja** będzie miał przypisany identyfikator **30**, zatem adres IP dla tej sieci VLAN będzie miał postać: **192.168.30.0/24**.

Zwrócicie uwagę na to że identyfikator każdej z sieci VLAN jest taki sam jak 3 oktet adresu IP. Jest to z mojej strony zabieg celowy ponieważ łatwiej jest wówczas identyfikować urządzenia należące do danej sieci. Pamiętajcie jednak o tym, że nie jest to warunek konieczny, i że podczas wykonywania późniejszych ćwiczeń możecie zastosować inne oznaczenia i adresację.

Skoro mamy już zaprojektowaną adresację IP, przejdźmy teraz do konfiguracji pierwszego przełącznika. Uruchamiamy konsolę CLI przełącznika **Parter** i tworzymy VLAN'y:

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10                    //stworzenie vlan o identyfikatorze 10
Switch(config-vlan)#name uczniowie        //nadanie nazwy sieci VLAN
Switch(config-vlan)#exit
Switch(config)#vlan 20                    //stworzenie vlan o identyfikatorze 20
Switch(config-vlan)#name nauczyciele
Switch(config-vlan)#exit
Switch(config)#vlan 30                    //stworzenie vlan o identyfikatorze 30
Switch(config-vlan)#name administracja
Switch(config-vlan)#end
```

Poleceniem ***show vlan*** (wpisanym w trybie *Privileged EXEC* )sprawdzamy poprawność wykonanych czynności. Jak widać poniżej, VLAN'y zostały stworzone poprawnie.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   uczniowie                         active
20   nauczyciele                       active
30   administracja                     active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Kolejną czynnością, którą musimy wykonać jest przypisanie poszczególnych portów przełącznika do określonej sieci VLAN. Przyjmijmy, że dla:

1. VLAN **uczniowie** dostępne porty to od **1** do **10**.
2. VLAN **nauczyciele** dostępne porty to od **11** do **20**.
3. VLAN **administracja** dostępne porty to od **21** do **22**.

Porty **23** i **24** do połączeń pomiędzy przełącznikami oraz ruterem więc nie przypisujemy ich do sieci VLAN.

Przejdźmy zatem do konfiguracji portów, uruchamiamy konsolę CLI przełącznika **Parter** i wpisujemy polecenia:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface range fastEthernet 0/1-10      //przejście do trybu konfiguracji portów od 1 do 10
Switch(config-if-range)#switchport access vlan 10       //dodanie portów do VLAN 10
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/11-20     //przejście do trybu konfiguracji portów od 11 do 20
Switch(config-if-range)#switchport access vlan 20       //dodanie portów do VLAN 20
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/21-22     //przejście do trybu konfiguracji portów 21 i 20
Switch(config-if-range)#switchport access vlan 30       //dodanie portów do VLAN 30
Switch(config-if-range)#end
```

Sprawdzamy jeszcze raz poleceniem ***show vlan*** poprawność konfiguracji. Jak widać na rysunku poniżej ustawienia zostały skonfigurowane poprawnie.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/23, Fa0/24
10   uczniowie                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
20   nauczyciele                       active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20
30   administracja                     active    Fa0/21, Fa0/22
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Powyższe działania konfiguracyjne należy powtórzyć dla pozostałych przełączników w sieci. Jest to proces niezbędny, aby sieci VLAN działały poprawnie.

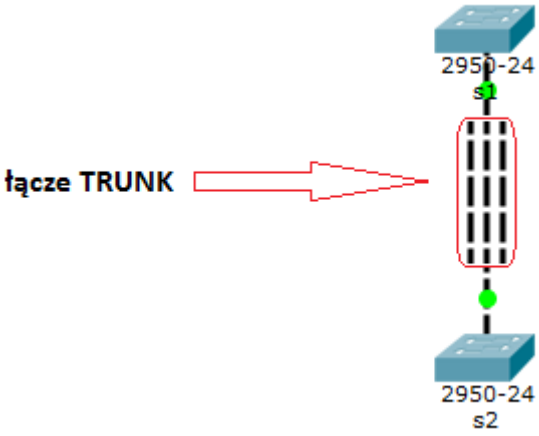
Pozostała nam jeszcze jedna czynność konfiguracyjna, którą musimy wykonać na przełącznikach. Będzie nią odpowiednie skonfigurowanie portów służących

do połączeń pomiędzy samymi przełącznikami. Aby dane mogły być przesyłane między komputerami w danej sieci VLAN, porty łączące przełączniki muszą pracować w trybie **TRUNK**. Czy jest trunk? Trunk to taki „tunel” zawierający w sobie dane przesyłane do różnych sieci VLAN. W naszym zadaniu mamy 3 sieci VLAN, a więc aby urządzenia mogły wymieniać dane między sobą potrzebne były by 3 fizyczne połączenia przełączników, 1 dla każdej sieci VLAN, tak jak zostało to pokazane na rysunku:

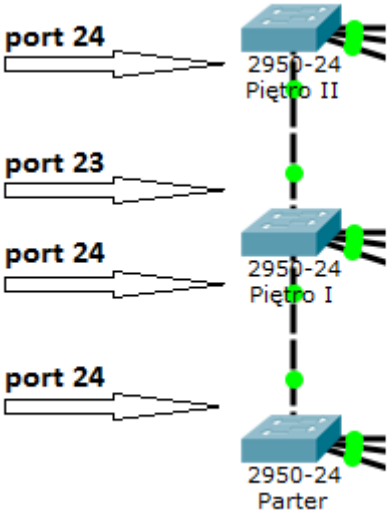
Powyższe działania konfiguracyjne należy powtórzyć dla pozostałych przełączników w sieci. Jest to proces niezbędny, aby sieci VLAN działały poprawnie.

Pozostała nam jeszcze jedna czynność konfiguracyjna, którą musimy wykonać na przełącznikach. Będzie nią odpowiednie skonfigurowanie portów służących do połączeń pomiędzy samymi przełącznikami. Aby dane mogły być przesyłane między komputerami w danej sieci VLAN, porty łączące przełączniki muszą pracować w trybie **TRUNK**. Czy jest trunk? Trunk to taki „tunel” zawierający w sobie dane przesyłane do różnych sieci VLAN. W naszym zadaniu mamy 3 sieci VLAN, a więc aby urządzenia mogły wymieniać dane między sobą potrzebne były by 3 fizyczne połączenia przełączników, 1 dla każdej sieci VLAN, tak jak zostało to pokazane na rysunku:


W przypadku naszej sieci jest to jeszcze sytuacja do przyjęcia ponieważ zajęte są tylko 3 porty, ale zdarzają się duże sieci, w których jest duża liczba logicznych sieci VLAN i wówczas takie rozwiązanie nie może być zastosowane ze względu na zbyt liczne wykorzystanie portów. W takiej sytuacji stosuje się właśnie „tunelowanie”, które powoduje, że w ramach jednego portu przełącznika wysyłane są dane do różnych sieci VLAN. Mówiąc wprost, w jednym kablu mamy 3 logiczne tory przesyła danych, tak jak przedstawia to rysunek poniżej:




Przełączniki w naszym przykładzie połączone są między sobą portami:




Tak więc właśnie te porty muszą skonfigurowane być do pracy w trybie **TRUNK**. Na dalszych etapach konfiguracji do przełącznika **Parter**podłączony zostanie jeszcze ruter, który pozwoli się komunikować między sobą komputerom w całej sieci, także port, do którego podłączymy router (w naszym przypadku 23) też musi pracować w trybie **TRUNK**.

Przechodzimy zatem do konfiguracji naszych przełączników, wykorzystując poniższe polecenia zmieniamy tryby pracy portów dla przełącznika**Parter**:

- `Switch>enable`
- `Switch#configure terminal`
- `Switch(config)#interface range fastEthernet 0/23-24`
- `Switch(config-if-range)#switchport mode trunk` //przełączenie trybu pracy portów na TRUNK
- `Switch(config-if-range)#switchport trunk allowed vlan add 10` //dodanie vlan 10 do łącza TRUNK
- `Switch(config-if-range)#switchport trunk allowed vlan add 20` //dodanie vlan 20 do łącza TRUNK
- `Switch(config-if-range)#switchport trunk allowed vlan add 30` //dodanie vlan 30 do łącza TRUNK
- `Switch(config-if-range)#end`

Sprawdzamy poprawność konfiguracji wpisując polecenie ***show interface trunk*** (w trybie *Privileged EXEC* ). Jak widać na rysunku poniżej wszystko zostało właściwie skonfigurowane.

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/23      on           802.1q         trunking      1
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/23      10,20,30
Fa0/24      1-1005

Port        Vlans allowed and active in management domain
Fa0/23      10,20,30
Fa0/24      1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/23      10,20,30
Fa0/24      1,10,20,30
```

Powyższą konfigurację należy powtórzyć również dla pozostałych przełączników, pamiętając o tym, że dla przełącznika **Piętro II** konfigurujemy tylko port **24** (do **23** nie jest aktualnie nic podłączone).
Teraz przejdziemy do podłączenia i skonfigurowania rutera do naszej sieci. W związku z tym, iż stworzyliśmy nowe podsieci, które mają różną adresację, komputery znajdujące się w danej sieci VLAN nie mogą komunikować się z komputerami z innej. Aby taką komunikację umożliwić, należy w odpowiedni sposób skonfigurować ruter. Podłączamy zatem urządzenie do **23** portu przełącznika i wykonujemy następujące polecenia:

```
Router>enable
Router#configure terminal
Router(config)#interface fastEthernet 0/0.10      //stworzenie wirtualnego interfejsu do obsługi VLAN uczniowie
Router(config-subif)#encapsulation dot1Q 10       //określenie enkapsulacji dla wirtualnego interfejsu (10 jest identyfikatorem VLAN)
Router(config-subif)#ip address 192.168.10.1 255.255.255.0 //ustawienie adresu IP i maski
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.20      //stworzenie wirtualnego interfejsu do obsługi VLAN nauczyciele
Router(config-subif)#encapsulation dot1Q 20       //określenie enkapsulacji dla wirtualnego interfejsu
Router(config-subif)#ip address 192.168.20.1 255.255.255.0 //ustawienie adresu IP i maski
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.30      //stworzenie wirtualnego interfejsu do obsługi VLAN administracja
Router(config-subif)#encapsulation dot1Q 30       //określenie enkapsulacji dla wirtualnego interfejsu
Router(config-subif)#ip address 192.168.30.1 255.255.255.0 //ustawienie adresu IP i maski
Router(config)#end
```

Aby sprawdzić poprawność konfiguracji należy najechać strzałką na symbol rutera i poczekać na wyświetlanie podsumowania, jak widać na poniższym rysunku konfiguracja przebiegła właściwie.

```
Port              Link   VLAN   IP Address         IPv6 Address                          MAC Address
FastEthernet0/0   Up     --     <not set>          <not set>                             0060.3E20.DC01
FastEthernet0/0.10 Up    --     192.168.10.1/24    <not set>                             0060.3E20.DC01
FastEthernet0/0.20 Up    --     192.168.20.1/24    <not set>                             0060.3E20.DC01
FastEthernet0/0.30 Up    --     192.168.30.1/24    <not set>                             0060.3E20.DC01
FastEthernet0/1   Down   --     <not set>          <not set>                             0060.3E20.DC02
Vlan1             Down   1      <not set>          <not set>                             0060.70B9.2EB3
Hostname: Router

Physical Location: Intercity, Home City, Corporate Office, Wiring Closet
```

Na koniec pozostaje tylko przypisać adresy IP dla poszczególnych komputerów w sieci i wykonać testy. Dla mojej sieci przebiegły one pomyślnie, wszystkie urządzenia mogą się wzajemnie komunikować.

Pamiętajcie również o tym, aby co jakiś czas zapisywać konfigurację urządzeń. Polecenie do zapisu: ***copy running-config startup-config***

**Ćwiczenie do wykonania:**

Pobierz plik programu Cisco Packet Tracer (plik został przygotowany w wersji 6.1) i wykonaj zadanie w nim zapisane.