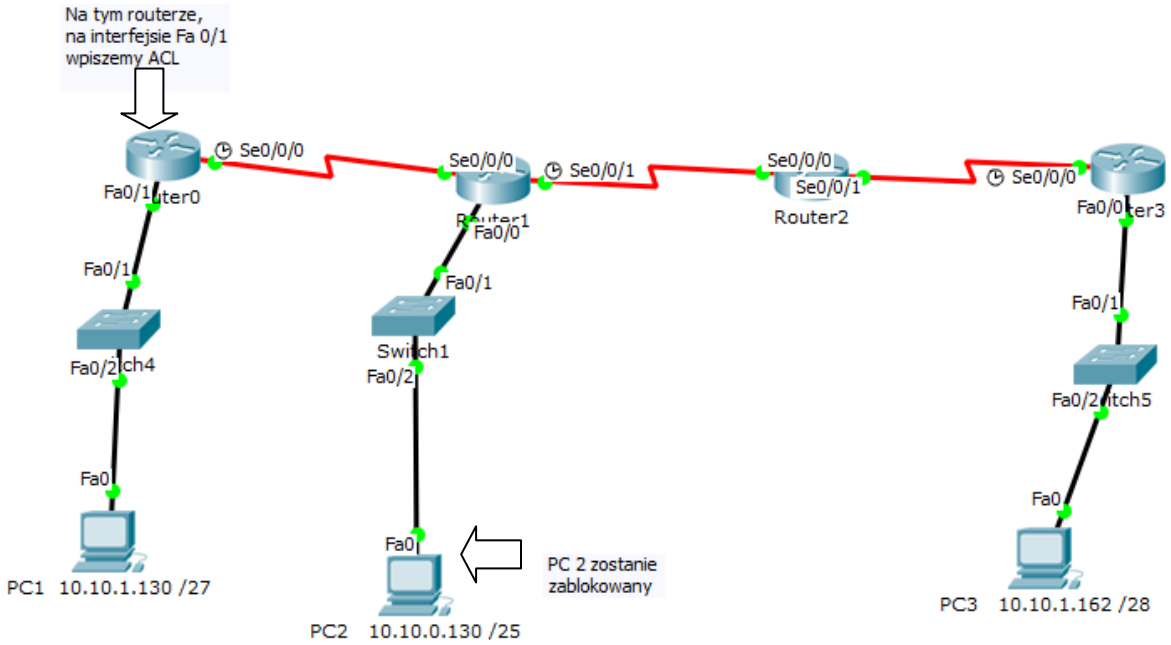
Ćwiczenie 1.1 - Standardowa ACL

Otwórz plik: ćwiczenie 1 - ACL.pkt



1. Sprawdź, czy przechodzi ping z PC2 (10.10.0.130) do PC1 (10.10.1.130)
2. Zablokuj cały ruch z adresu ***10.10.0.130***.
   Listę ACL ustaw na routerze ***Router0*** na interfejsie ***FastEthernet0/1***.

```
Router0>en
Router0#conf t
Router0(config)#access-list 1 deny host 10.10.0.130
Router0(config)#access-list 1 permit any
Router0(config)#int fa0/1
Router0(config-if)#ip access-group 1 out
Router0(config-if)#
```

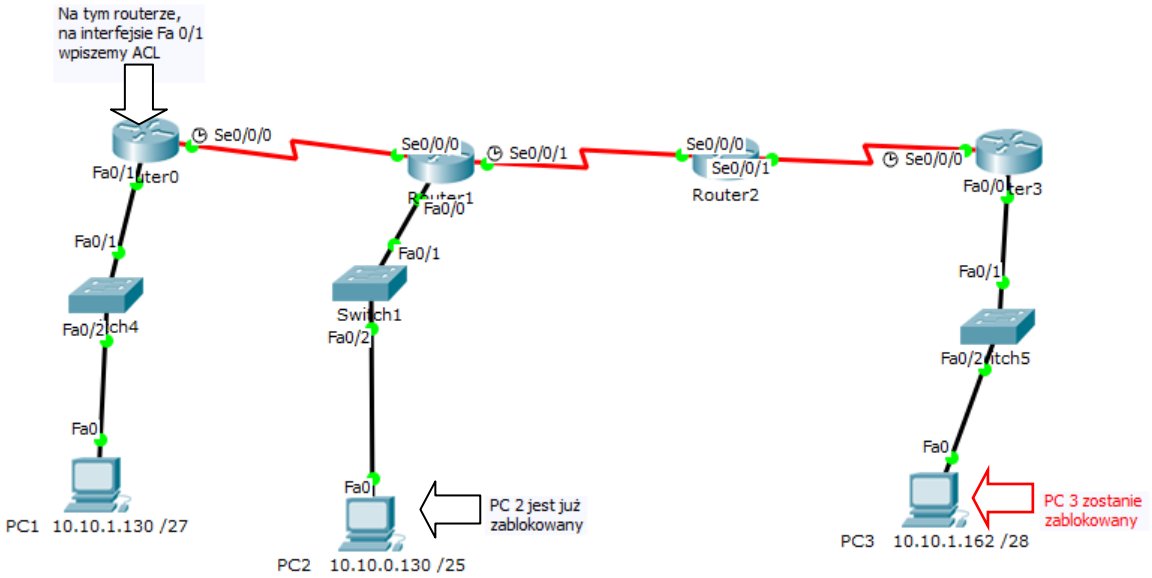
3. Sprawdź, czy przechodzi ping z PC2 (10.10.0.130) do PC1 (10.10.1.130)

Komendy zaznaczone na różowo - na wybranym interfejsie (u nas to Fa0/1) ustawiamy polecenie grupujące listę ACL do interfejsu (***access-group [numer access-listy]***), ***out*** oznacza pakiety wysyłane przez interfejs routera (czyli ruch wychodzący).

Może być jeszcze słowo kluczowe ***in***, które będzie oznaczać pakiety odbierane przez interfejs routera (czyli ruch przychodzący).

Ćwiczenie 1.2 - Standardowa ACL

Kontynuujemy poprzednie zadania.



1. Sprawdź komunikację PC3 i PC1 (powinna być)

2. Sprawdź jak wygląda obecna ACL na Routerze0:

```
Router0#sh access-list

Standard IP access list 1
10 deny host 10.10.0.130
20 permit any

Router0#
```

3. Teraz zablokuj host *10.10.1.162.*

Na routerze Router0 musimy dopisać kolejny wiersz ACL.
Pamiętamy, że ważna jest kolejność zapisu, gdyż ACL jest czytane od góry do dołu.

Dopisując deny host 10.10.1.162 na końcu nic nie osiągnęlibyśmy, gdyż wcześniej jest instrukcja zezwalająca na przepuszczanie całego ruchu.
Wykonaj następujące kroki:

```
Router0#conf t
Router0(config)#no access-list 1
Router0(config)#access-list 1 deny host 10.10.0.130
Router0(config)#access-list 1 deny host 10.10.1.162
Router0(config)#access-list 1 permit any
```

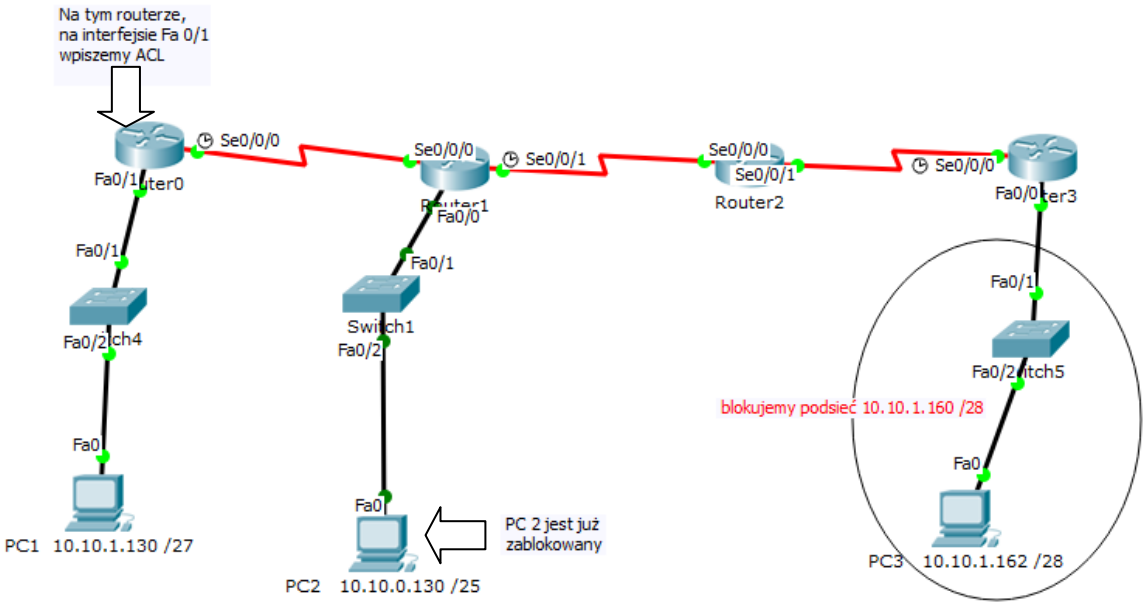
```
Router0(config)#
```

Polecenie ***no access-list 1*** usuwa naszą ACL z konfiguracji. Następnie musimy ja od początku wpisać.

4. Sprawdź komunikację PC3 i PC1 (nie powinna działać)

Ćwiczenie 1.3 - Standardowa ACL

Teraz zamiast blokowania komputera z ćwiczenia 2 chcemy zablokować ruch z całej podsieci 10.10.1.160 /28.



Wykonujemy następujące kroki:

```
Router0#conf t
Router0(config)#no access-list 1
Router0(config)#access-list 1 deny host 10.10.0.130
Router0(config)#access-list 1 deny 10.10.1.160 0.0.0.15
Router0(config)#access-list 1 permit any
Router0(config)#
```

Czyli znowu usuwamy access-listę 1 (kolor różowy). Następnie wprowadzamy kolejne instrukcje.
W drugiej instrukcji (kolor niebieski) mamy zastosowanie wildcard mask (czyli odwrotność maski podsieci).

Dodaj teraz kolejny komputer do podsieci 10.10.1.160 /28 i sprawdź czy działa z niego komunikacja do komputera 10.10.1.130.