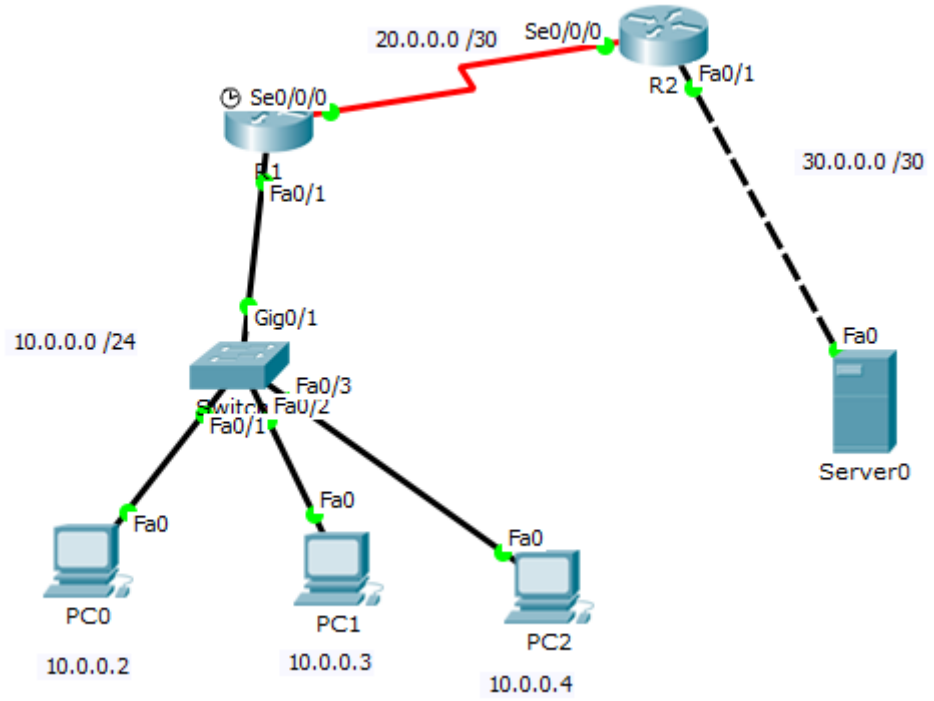
Ćwiczenie - ACL rozszerzona

Utwórz poniższą topologię w programie PT:



Następnie nazwij routery wg rysunku, skonfiguruj interfejsy oraz protokół RIP.
Na serwerze (30.0.0.2) aktywuj konfiguracje usług (sprawdź czy są włączone): http (www.imie.edu) , FTP (login: imię; hasło: nazwisko) – nie stosuj polskich znaków.

Cel ćwiczenia - zapoznanie się z filtrowanie ruchu sieciowego w oparciu o rodzaje aplikacji.

Zadanie 1 - Blokowanie pingów, ale z dostępem do www

Host oferujący strony WWW ma adres 30.0.0.2. Nie chcemy, aby zewnętrzni użytkownicy "pingowali" nasz serwer (DoS = Denial of Services). Utwórz listę ACL 101, która będzie filtrowała wszystkie polecenia ping do serwera.

Przetestuj:
ping z komputera z podsieci 10.0.0.0 do serwera 30.0.0.2
otwieranie strony serwera 30.0.0.2 z komputera z podsieci 10.0.0.0

Jaki otrzymałeś rezultat?

Zadanie 2 - Udostępnianie usługi FTP dla jednego hosta

Usuń poprzednią ACL 101 z routera R2

Udostępniamy usługę FTP tylko dla komputera 10.0.0.2, dla pozostałych komputerów usługa ta jest niedostępna. Utwórz ACL 102 spełniającą powyższe kryteria (FTP to porty tcp 20 i 21). Na jakim routerze i jakim interfejsie należy ją podpiąć?

Sprawdź działanie tej ACL.

Zadanie 3 - Blokujemy usługę TELNET dla hosta

Usuń poprzednią ACL 102 z routera

Telnet jest usługą niebezpieczną, bowiem posługuje się komunikacją za pomocą otwartych tekstów, dlatego Ty jako administrator pracujesz tylko na komputerze 10.0.0.4 i zdecydowałeś, że usługa Telnet będzie całkowicie zablokowana z tego komputera do serwera 30.0.0.2.
Utwórz ACL 103 i podepnij ją do właściwego interfejsu.

Sprawdź efekt.