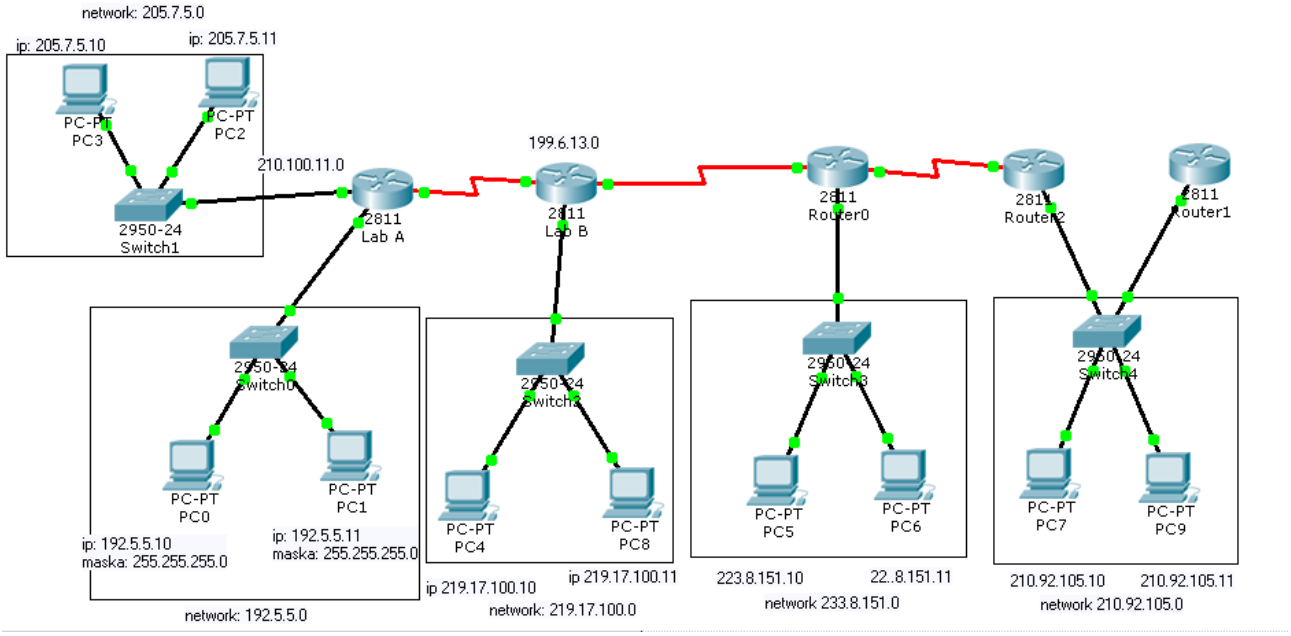
Bezpieczeństwo sieci komputerowych
Temat: Topologia i podstawowa konfiguracja

Data: 27/03/2022
Ewa Namysł
Informatyka stosowana, III rok

1. Opis i cel zadania:

Celem zadania jest przygotowanie topologii zgodnie z załączonym schematem, przypisując ręcznie adresy urządzeniom. Ponadto należy ustawić odpowiednie hasła dostępu oraz hasła trybu uprzywilejowanego.

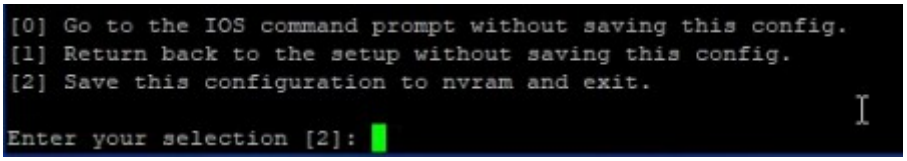


2. Zmiana haseł:

W celu zmiany hasła łączymy komputer z routerem przez port konsolowy. Po aktualizacji oprogramowania i przywróceniu ustawień fabrycznych urządzenia (sprawozdanie 1), przechodzimy do wstępnej konfiguracji.

```
Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: R3

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: llcisco
```

Teraz jesteśmy w stanie wybrać hasła dostępu, nazwę urządzenia etc. Następnie zapisujemy konfigurację lub jeśli chcemy dokonać zmian możemy rozpocząć od początku:



Jeśli ominęliśmy wstępną konfigurację, hasło dla połączenia konsolowego możemy ustawić poprzez komendy:

configure terminal
line console 0
password cisco00
login

Dzięki *line console 0* wchodzimy w konfigurację połączenia konsolowego, następnie ustalamy hasło, a *login* wymusza sprawdzanie hasła przy logowaniu. W podobny sposób możemy ustawić hasło dla połączeń przez SSH lub telnet, zamieniając tylko *line console 0* na *line vty 0 4* (gdzie 0 4 to wybrane wirtualne terminale 0-4).

W przypadku hasła dostępu do trybu uprzywilejowanego postępujemy podobnie, wpisując tym razem:

enable secret cisco11

Secret wymusza szyfrowanie haseł, więc w przeciwieństwie do *enable password* nie są przechowywane jako zwykły tekst w zapisanej konfiguracji.

Po ustawieniu haseł zapisujemy konfigurację *copy running-config startup-config.*

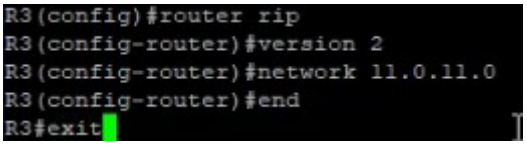
Zapisaną konfigurację można podejrzeć w trybie uprzywilejowanym wpisując *show startup-config.*

2. Przygotowanie topologii:

W naszym przypadku na routerze ustawiamy adres interfejsu G0/0 na 199.6.13.1 z maską 255.255.255.0. Na jednym komputerze ustawiamy adres IP 219.17.100.11 oraz 219.17.100.10 na drugim, maska 255.255.255.0, brama 219.17.100.1.

Przechodzimy do konfiguracji połączenia między switchem a routerem, podłączając go do portu G0/0. Oba komputery z tej sieci podłączamy do switcha i sprawdzamy czy potrafią się ze sobą komunikować. Jeśli udało nam się poprawnie skonfigurować połączenie, to komputery powinny być w stanie pingować się nawzajem.

W konsoli routera konfigurujemy połączenie z drugim routerem, na G0/1 ustawiamy 11.0.11.5/24 i wpisujemy *no shutdown*, aby interfejs został włączony (w stanie up). Aby umożliwić komunikację między dwiema sieciami, musimy aktywować Router Information Protocol (RIP) w configu wpisując *ip routing*, a następnie:



W analogiczny sposób dodajemy kolejną sieć na G0/2.

Po zakończeniu konfiguracji, wpisując *show ip route* zobaczymy tablicę routingu.

Jeśli nie popełniliśmy błędu i wszystkie routery zostały ze sobą połączone, powinniśmy móc spingować adresy z własnej sieci, adresy z sieci połączonych z nami sąsiednich routerów, ale też z sieci, która nie jest bezpośrednio połączona z nami.