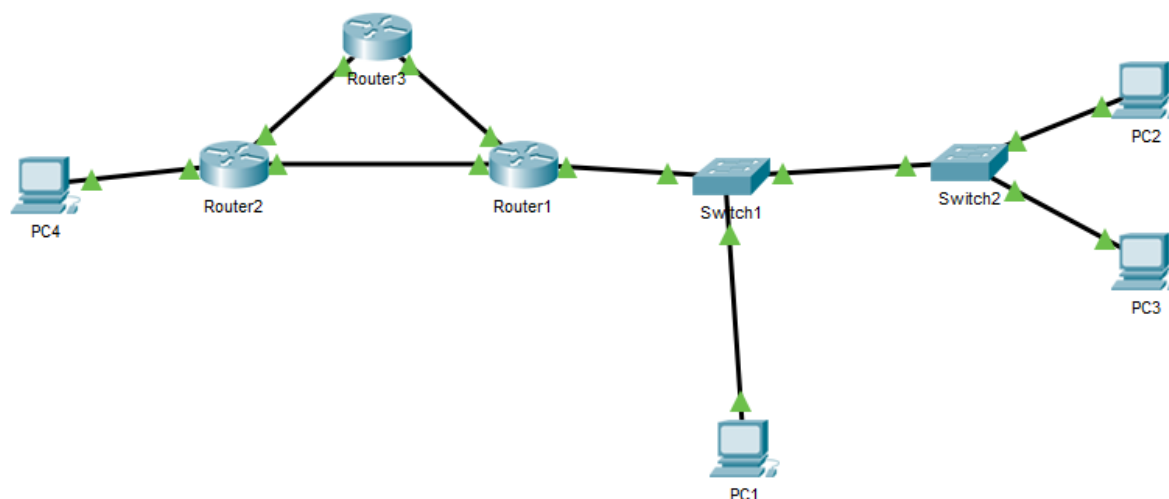


VLSM /routing / switching / ACL / PAT



Zadania:

1. Narysuj w PT sieć wg powyższego schematu.
2. Ustaw nazwy na wszystkich urządzeniach, dodając do hostname swoje inicjały.
3. Skonfiguruj VLANy i ustaw ich nazwy:
 - 10 --> IT
 - 20 --> HR
 - 99 --> MGT
4. Router 1 będzie realizował routing między VLANami 10 i 20.
5. Interfejsy na Switchu 1 od Fa0/11 do Fa0/20 przypisz do VLAN 10
6. Interfejsy na Switchu 2 od Fa0/11 do Fa0/15 przypisz do VLANu 10, a od Fa0/16 do Fa0/20 do VLANu 20.
7. Pozostałe nieużywane interfejsy obu przełączników należy wyłączyć.
8. PC1 i PC3 należą do VLAN 10, PC2 -> vlan 20
9. Na Switchu 2 uruchom mechanizm Port-Security
 - * interfejs do PC2 - bezpieczeństwo statyczne, maksymalna liczba adresów MAC to 2, akcją na naruszenie bezpieczeństwa ma być wyłączenie interfejsu
 - * interfejs do PC3 - przełącznik ma uczyć się i zapamiętywać adresy MAC podłączonych urządzeń i nie dopuszczać, aby na porcie miały pracować inne urządzenia; maksymalna liczba MAC adresów to 1
10. Zaadresuj całą sieć używając dla wszystkich urządzeń adresów z sieci 172.x.4.0 /22, gdzie x - numer z dziennika. Planując adresację należy wziąć pod uwagę, że:
 - * vlan 10 - 20 hostów
 - * vlan 20 - 50 hostów
 - * do Routera 2 docelowo może być podpiętych do 70 hostów
 - * połączenia P2P powinny mieć maskę /30
11. W sieci uruchom protokół routingu RIPv2

Sprawdź czy wszystkie urządzenia na wzajem się komunikują (**zrób screena**)

12. Na Routerze 2 uruchom serwer DHCP, który będzie przydzielał adresy dla urządzeń w VLANach 10 i 20.
13. Na routerze 2 uruchom PAT tak, aby gdy urządzenia w VLANie 20 komunikują się z PC4, to PC4 widzi ruch z adresem źródłowym przypisanym do interfejsu Fa0/0 Routera 2.
14. Hosty w VLANie 10 nie mogą komunikować się z hostem 4.

Oddajemy:

- plik w PT
- tabelę VLSM
- screen zrobiony po punkcie 11.