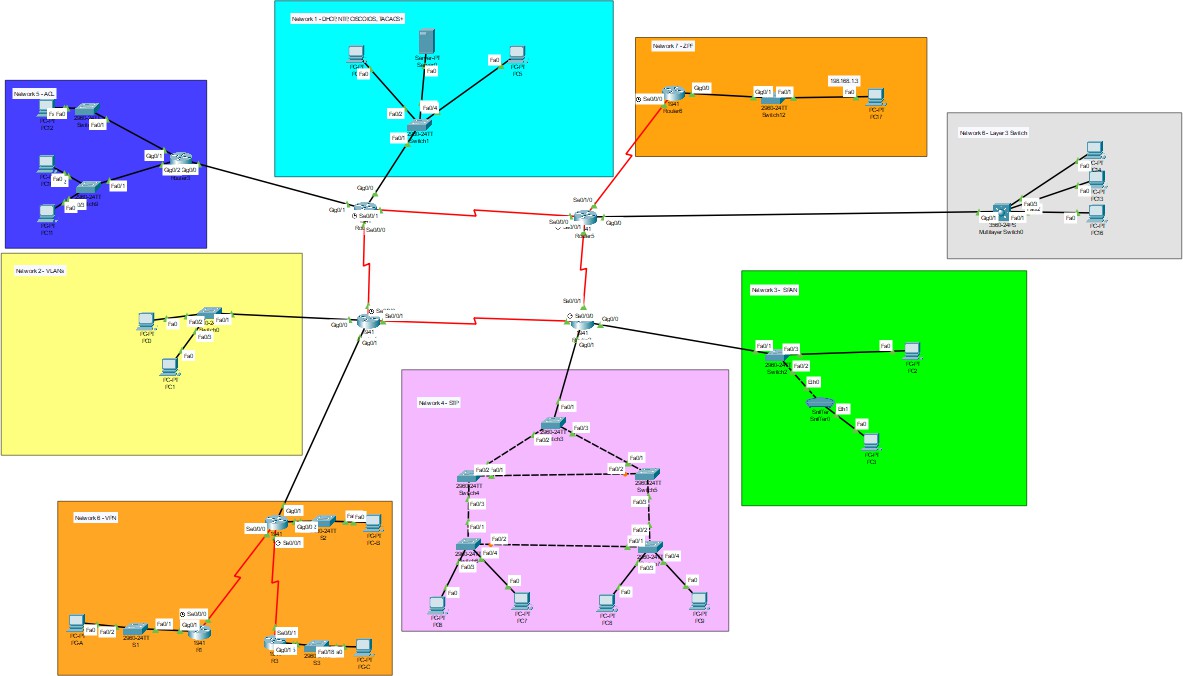
|  |  |  |
| --- | --- | --- |
| **Politechnika Świętokrzyska w Kielcach**  **Wydział Elektrotechniki, Automatyki i Informatyki Katedra Informatyki, Elektroniki i Elektrotechniki** | | |
| Kierunek  **Informatyka** | Projekt  **Wstęp do cyberbezpieczeństwa** | |
| Grupa dziekańska  **1ID25A** | Wykonał:   * **Arkadiusz Wolski** * **Bartosz Kasprzycki** | Temat:  **Osiedle** |

1. **Struktura sieci**

****

1. **Tabele adresacji**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| PC0 | Fa0 | 192.168.1.10 | 255.255.255.0 | 192.168.1.1 |
| PC1 | Fa0 | 192.168.2.10 | 255.255.255.0 | 192.168.2.2 |
| Switch0 | FastEthernet0/1 | -- | -- | -- |
| Switch0 | FastEthernet0/2 | -- | -- | -- |
| Switch0 | FastEthernet0/3 | -- | -- | -- |
| Router1 | Gig0/0.10 | 192.168.1.1 | 255.255.255.0 | -- |
| Router1 | Gig0/0.20 | 192.168.2.2 | 255.255.255.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| PC2 | Fa0 | 194.168.1.3 | 255.255.255.0 | 194.168.1.1 |
| PC3 | Fa0 | 194.168.1.4 | 255.255.255.0 | 194.168.1.1 |
| Switch2 | VLAN 1 | 194.168.1.2 | 255.255.255.0 | 194.168.1.1 |
| Router2 | Gig0/0 | 194.168.1.1 | 255.255.255.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| PC4 | Fa0 | DHCP | 255.255.255.0 | DHCP |
| PC5 | Fa0 | DHCP | 255.255.255.0 | DHCP |
| Server0 | Fa0 | 193.168.1.3 | 255.255.255.0 | 193.168.1.1 |
| Switch1 | VLAN 1 | 193.168.1.2 | 255.255.255.0 | 193.168.1.1 |
| Router0 | Gig0/0 | 193.168.1.1 | 255.255.255.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| Router1 | Serial0/0/0 | 1.0.0.1 | 255.0.0.0 | -- |
| Router0 | Serial0/0/0 | 1.0.0.2 | 255.0.0.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| Router5 | Serial0/0/1 | 3.0.0.2 | 255.0.0.0 | -- |
| Router2 | Serial0/0/1 | 3.0.0.1 | 255.0.0.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| Router2 | Serial0/0/0 | 2.0.0.2 | 255.0.0.0 | -- |
| Router1 | Serial0/0/1 | 2.0.0.1 | 255.0.0.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| Router5 | Serial0/0/1 | 3.0.0.2 | 255.0.0.0 | -- |
| Router0 | Serial0/0/1 | 3.0.0.1 | 255.0.0.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| PC6 | Fa0 | 195.168.1.10 | 255.255.255.0 | 195.168.1.1 |
| PC7 | Fa0 | 195.168.1.11 | 255.255.255.0 | 195.168.1.1 |
| PC8 | Fa0 | 195.168.1.12 | 255.255.255.0 | 195.168.1.1 |
| PC9 | Fa0 | 195.168.1.13 | 255.255.255.0 | 195.168.1.1 |
| Switch3 | -- | -- | -- | -- |
| Switch4 | -- | -- | -- | -- |
| Switch5 | -- | -- | -- | -- |
| Switch6 | -- | -- | -- | -- |
| Switch7 | -- | -- | -- | -- |
| Router2 | Gig0/1 | 195.168.1.1 | 255.255.255.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| PC10 | Fa0 | 196.168.20.3 | 255.255.255.0 | 196.168.20.1 |
| PC11 | Fa0 | 196.168.20.4 | 255.255.255.0 | 196.168.20.1 |
| PC12 | Fa0 | 196.168.10.3 | 255.255.255.0 | 196.168.10.1 |
| Switch8 | -- | -- | -- | -- |
| Switch9 | -- | -- | -- | -- |
| Router3 | Gig0/1 | 196.168.10.1 | 255.255.255.0 | -- |
| Router3 | Gig0/2 | 196.168.20.1 | 255.255.255.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| Router3 | Se0/3/0 | 4.0.0.2 | 255.0.0.0 | -- |
| Router0 | Se0/1/0 | 4.0.0.1 | 255.0.0.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| PC13 | Fa0 | 172.16.31.3 | 255.255.255.0 | 172.16.31.1 |
| PC14 | Fa0 | 172.16.31.4 | 255.255.255.0 | 172.16.31.1 |
| PC16 | Fa0 | 172.16.31.2 | 255.255.255.0 | 172.16.31.1 |
| Multilayer Switch0 | GigabitEthernet0/1 | 197.168.1.2 | 255.255.255.0 | -- |
| Multilayer Switch0 | Vlan1 | 172.16.31.1 | 255.255.255.0 | -- |
| Router5 | Gig0/0 | 197.168.1.1 | 255.255.255.0 | -- |

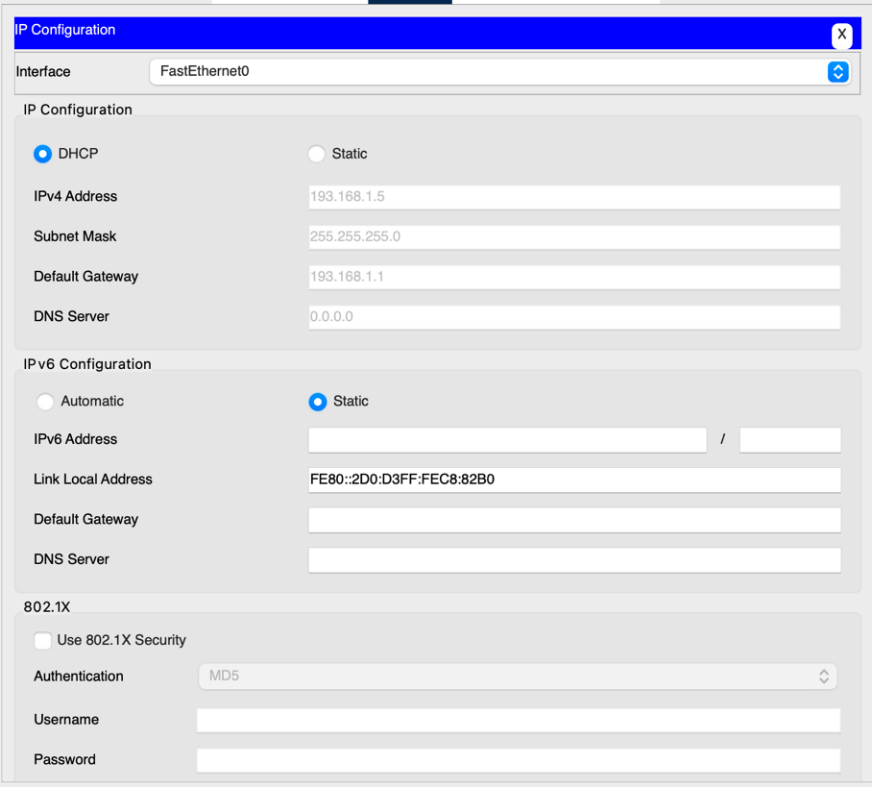
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| PC17 | Fa0 | 198.168.1.3 | 255.255.255.0 | 198.168.1.1 |
| Switch12 | -- | -- | -- | -- |
| Router6 | Gig0/0 | 198.168.1.1 | 255.255.255.0 | -- |
| Router6 | Se0/0/0 | 7.0.0.2 | 255.0.0.0 | -- |
| Router5 | Se0/1/0 | 7.0.0.1 | 255.0.0.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sprzęt | Interfejs | Adres IP | Maska | Brama  wyjściowa |
| PC-A | Fa0 | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-B | Fa0 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 |
| PC-C | Fa0 | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 |
| S1 | -- | -- | -- | -- |
| S2 | -- | -- | -- | -- |
| S3 | -- | -- | -- | -- |
| R1 | Gig0/1 | 192.168.1.1 | 255.255.255.0 | -- |
| R1 | Se0/0/0 | 10.1.1.2 | 255.255.255.252 | -- |
| R2 | Gig0/0 | 192.168.2.1 | 255.255.255.0 | -- |
| R2 | Se0/1/0 | 6.0.0.2 | 255.0.0.0 | -- |
| R2 | Serial0/0/0 | 10.1.1.1 | 255.255.255.252 | -- |
| R2 | Serial0/0/1 | 10.2.2.1 | 255.255.255.252 | -- |
| R3 | Gig0/1 | 192.168.3.1 | 255.255.255.0 | -- |
| R3 | Se0/0/1 | 10.2.2.2 | 255.255.255.252 | -- |
| Router1 | Se0/1/0 | 6.0.0.1 | 255.0.0.0 | -- |

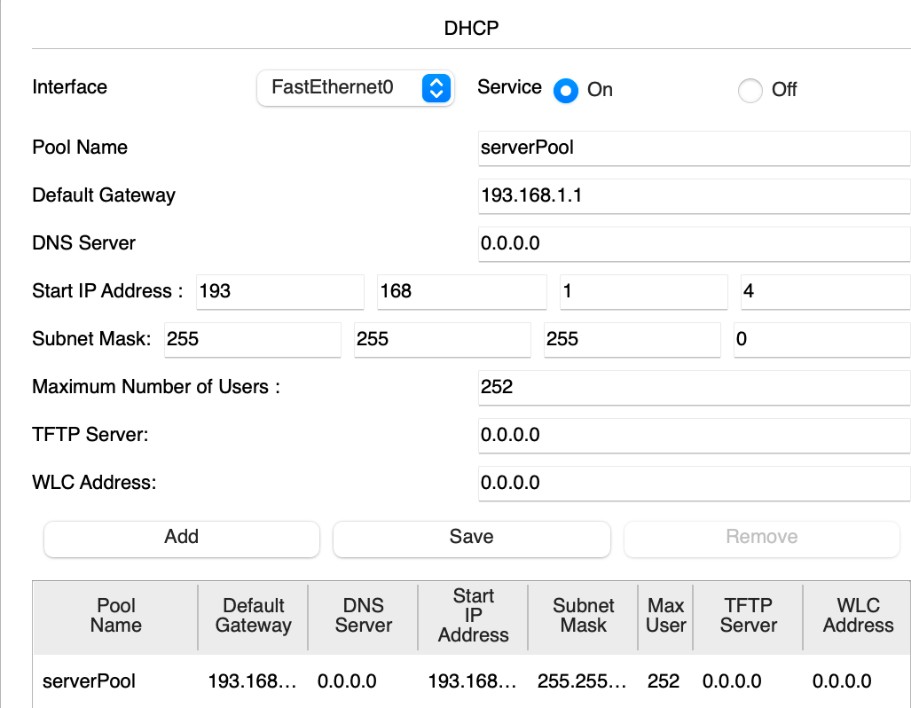
1. **Konfiguracja urządzeń**

# DHCP

Serwer w podsieci *Network 1* został skonfigurowany tak, by przydzielać komputerom adresy z puli adresów przy pomocy protokołu DHCP. Poniżej przedstawiono przykładowy adres IP hosta uzyskany z wykorzystaniem protokołu DHCP.



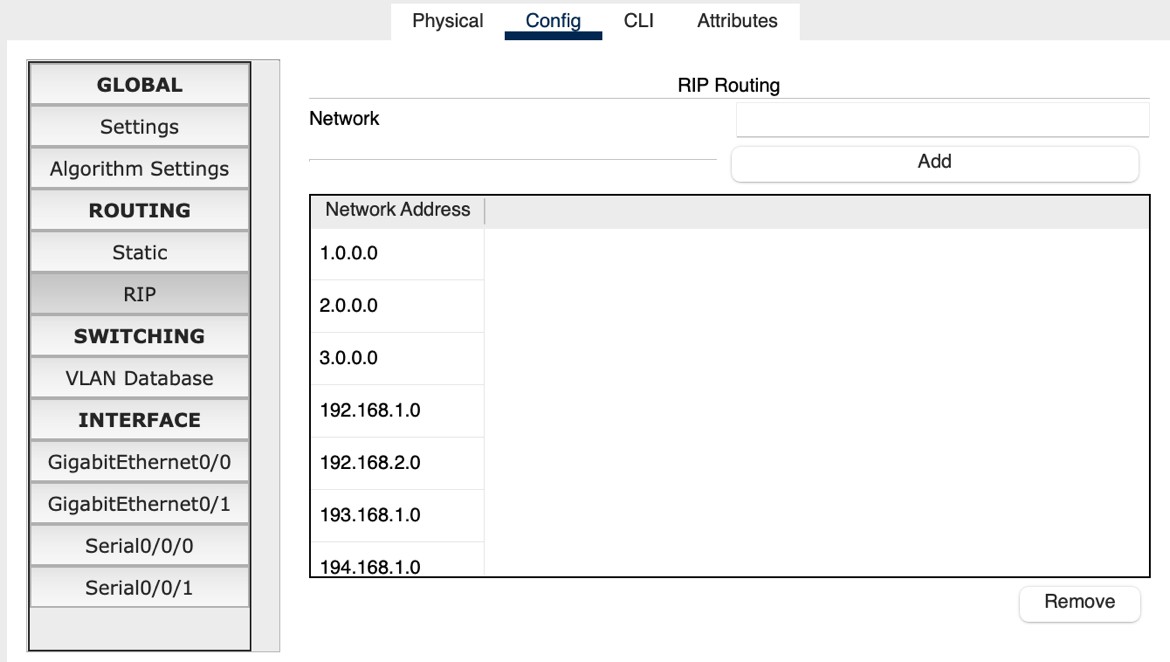
Rys. 3.1. Przykład działania protokołu DHCP dla hosta



Rys. 3.2. Przykładowa konfiguracja protokołu DHCP

# RIP

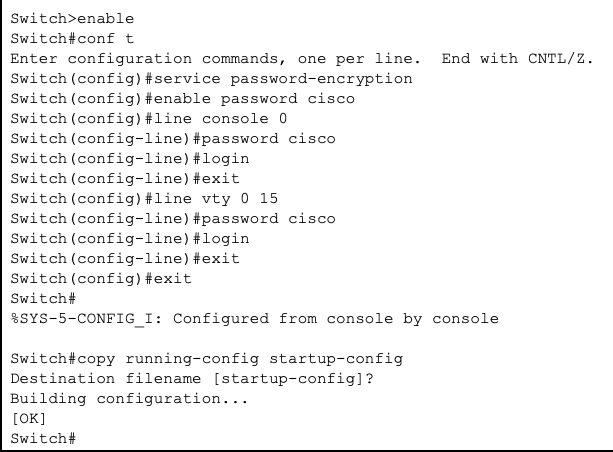
Routery wykorzystują protokół RIP do obliczania najlepszej trasy do celu dla pakietów danych. Przykładowa konfiguracja protokołu RIP została zaprezentowana poniżej.



Rys. 3.3. Przykładowa konfiguracja protokołu RIP

# Zabezpieczenia

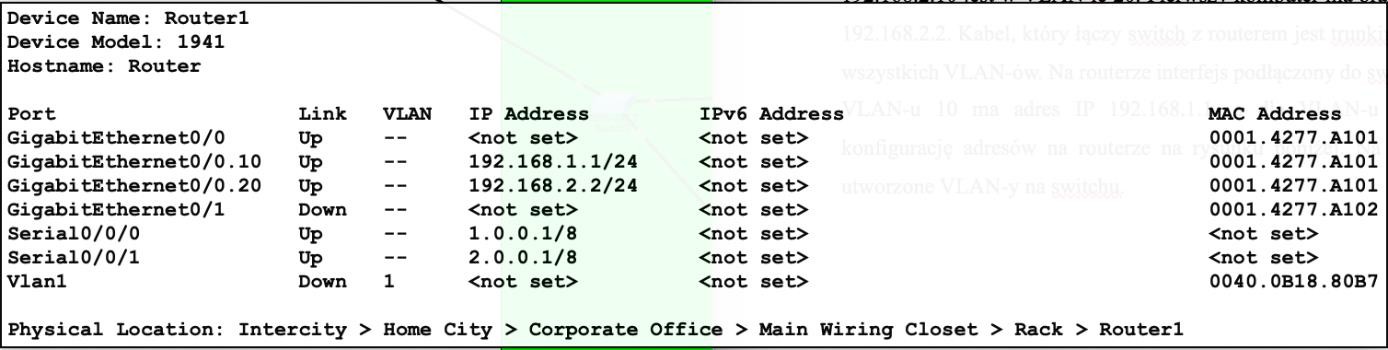
Na Routerach i Switch-ach w podsieciach: *Network 1, Network 2, Network 6* zabezpieczony został dostęp do trybu uprzywilejowanego oraz do portów konsolowych i wirtualnych terminali. Dodatkowo, hasła zostały zaszyfrowane, by uniknąć ich przechowywania w formie jawnej. Dla celów tego projektu, hasła w *Network 1* i *Network 2* to: **cisco**. Poniżej przedstawiono przykładową konfigurację zabezpieczeń. *W Network 6* do *console line* hasło to ciscoconpa55, dla linii vty ciscovtypa55, dla trybu uprzywilejowanego enable ciscoenpa55.



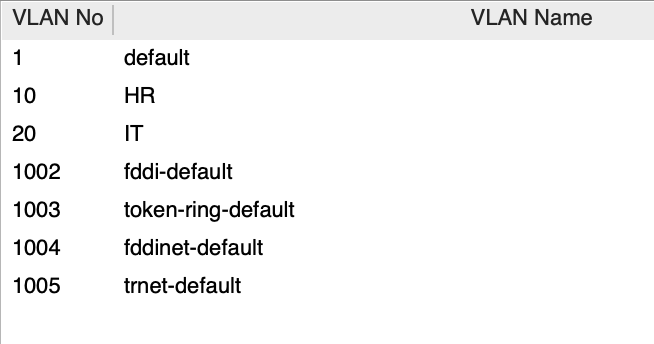
Rys. 3.4. Przykładowa konfiguracja zabezpieczeń

# VLAN-y

W podsieci *Network 2* zostały stworzone dwa VLAN-y: VLAN 10 i VLAN 20. Jeden komputer o adresie IP 192.168.1.10 jest w VLAN-ie 10, natomiast drugi komputer o adresie IP 192.168.2.10 jest w VLAN-ie 20. Pierwszy komputer ma bramę 192.168.1.1, natomiast drugi 192.168.2.2. Kabel, który łączy switch z routerem jest trunkingowy, co oznacza, że należy do wszystkich VLAN-ów. Na routerze interfejs podłączony do switcha skonfigurowano tak, że dla VLAN-u 10 ma adres IP 192.168.1.1, a dla VLAN-u 20 192.168.2.2. Przedstawiono konfigurację adresów na routerze na rysunku poniżej. Na drugim rysunku przedstawiono utworzone VLAN-y na switchu.



Rys. 3.5. Konfiguracja adresów na routerze

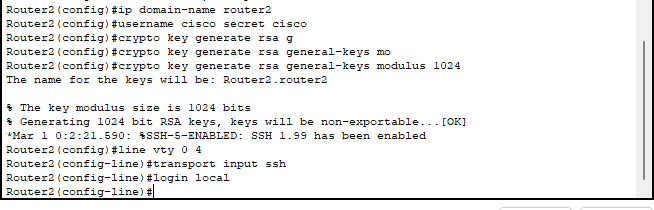


Rys. 3.6. VLAN-y na switchu

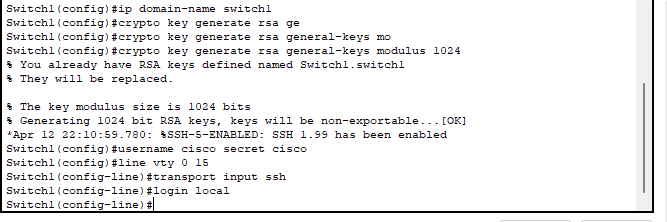
# Konfiguracja urządzeń pod kątem dostępu SSH

Do wykonania konfiguracji urządzeń pod kątem dostępu do SSH wybraliśmy urządzenia: *Router2* oraz *Swtich1*.

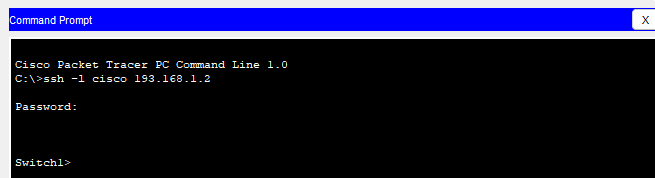
W przypadku routera jak i switcha konfiguracja wyglądała bardzo podobnie. Na początku określona została nazwa domeny, po czym utworzony został użytkownik z loginem ***cisco*** i zaszyfrowanym hasłem ***cisco.*** Następnie utworzony został 1024-bitowy klucz RSA. W kolejnym kroku wykonana została konfiguracja linii VTY w celu umożliwienia dostępu do urządzeń z wykorzystaniem SSH z wykorzystaniem danych utworzonego wcześniej użytkownika. Poniżej przedstawiona została szczegółowa konfiguracja routera oraz switcha.



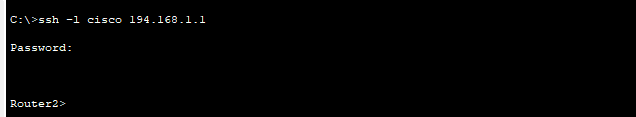
Rys. 3.5. Konfiguracja routera pod kątem dostepu SSH



Rys. 3.6. Konfiguracja switcha pod kątem dostępu SSH



Rys. 3.7. Logowanie poprzez SSH do switcha



Rys. 3.8. Logowanie poprzez SSH do routera

# Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS

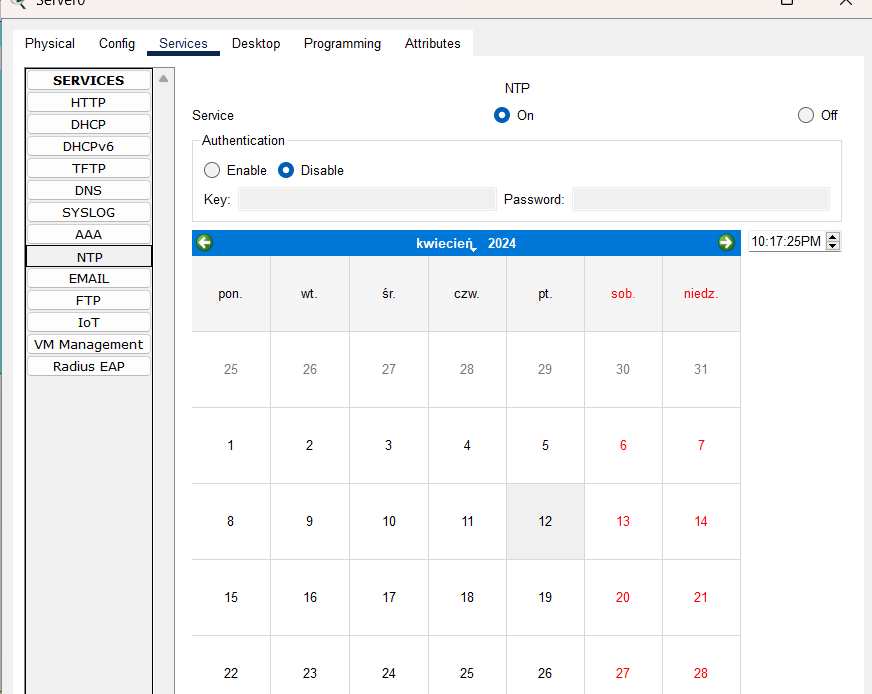
Konfiguracja NTP oraz CISCO IOS również wykonana została na urządzeniach *Router0*

oraz *Switch1* znajdujących się w sieci *Network1*.

czas.

# Konfiguracja NTP

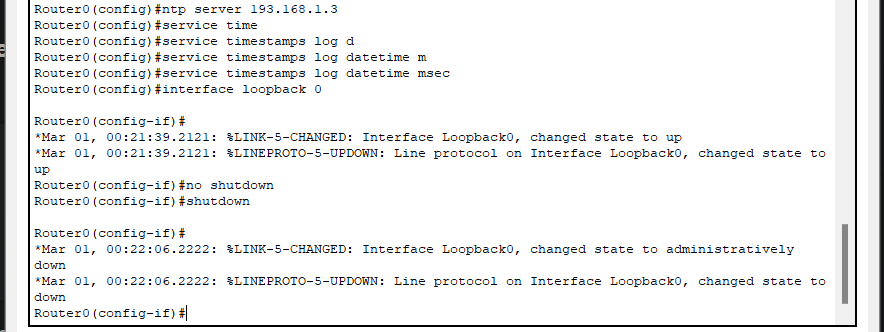
Na początku na serwerze włączona została usługa NTP oraz ustawiony został aktualny



Rys. 3.9. Włączenie usługi NTP

Następnie na routerze jak i na switchu określony został adres ip serwera ntp wraz z konfiguracją logowania pod kątem dołączania znaczników czasu zawierających datę, godzinę

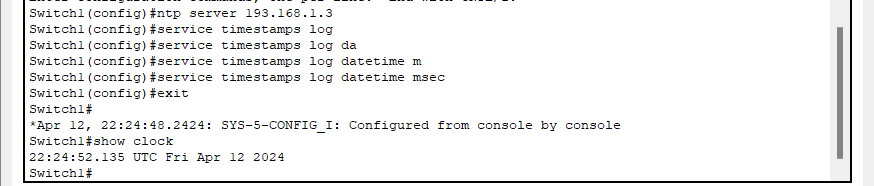
oraz milisekundy.



Rys. 3.10. Konfiguracja NTP na routerze



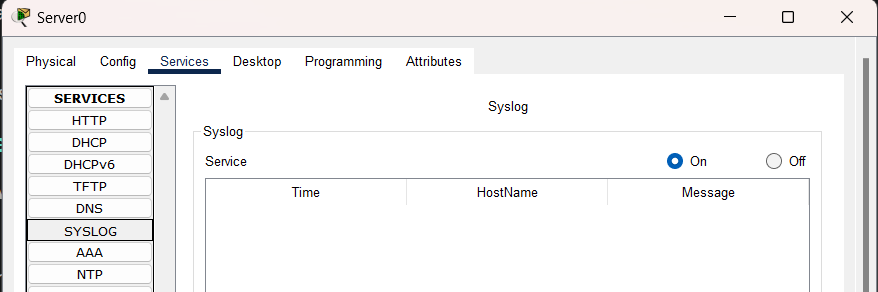
Rys. 3.11. Konfiguracja NTP na routerze (czas)



Rys. 3.12. Konfiguracja NTP na switchu

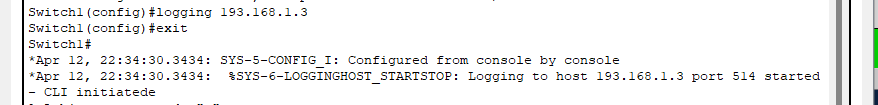
# Konfiguracja CISCO IOS

Podobnie, jak w przypadku konfiguracji NTP, pierwszym krokiem było włączenie usługi CISCO IOS na serwerze.

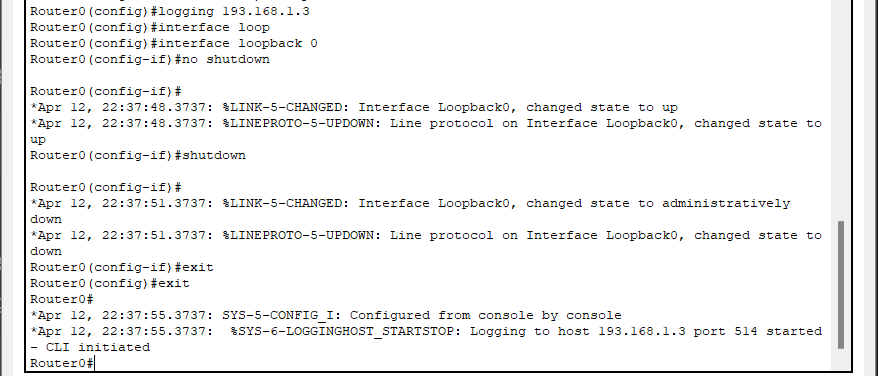


Rys. 3.13. Włączenie usługi CISCO IOS

Następnie, z wykorzystaniem komendy *logging* na routerze oraz switchu określony został adres serwera z włączoną usługą logowania.

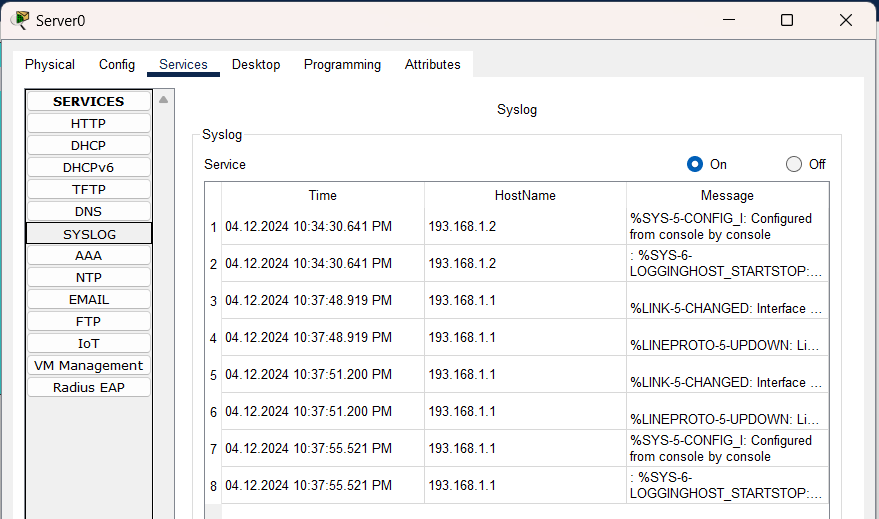


Rys. 3.14. Konfiguracja CISCO IOS na switchu



Rys. 3.15. Konfiguracja CISCO IOS na routerze

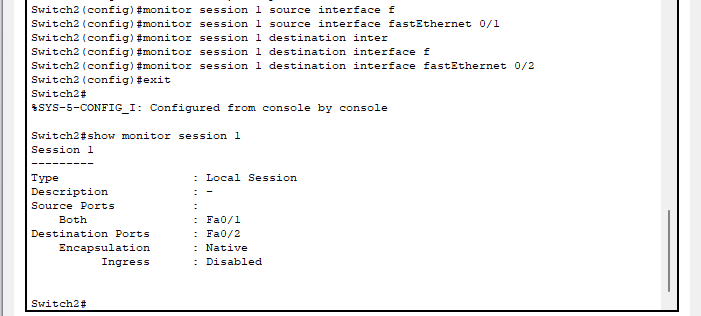
Poniżej przedstawione zostały logi pochodzące z routera oraz switcha.



Rys. 3.16. Logi z routera oraz switcha

# Implementacja lokalnego SPAN

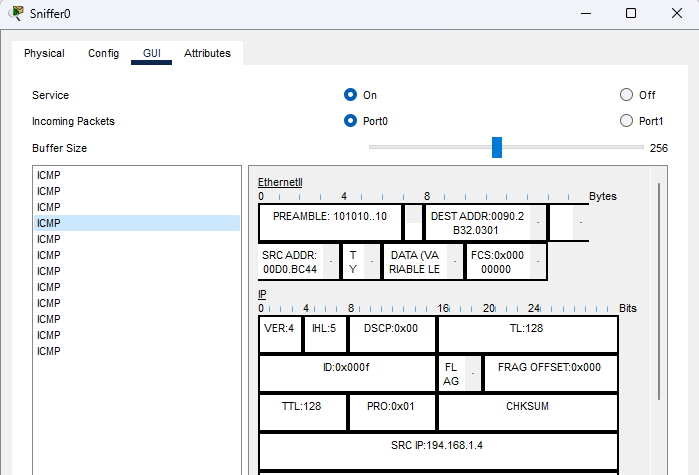
Konfiguracja lokalnego SPAN wykonana została w sieci *Network 3*. Switch2 został skonfigurowany tak, by ruch z portu FastEthernet 0/1 był kopiowany i przesyłany na port FastEthernet 0/2.



Rys. 3.17. Konfiguracja lokalnego SPAN

Poniżej zaprezentowano pakiety przechwycone przez Sniffera prezentujące działanie

STP.

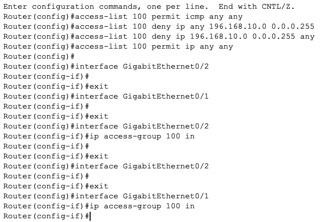


Rys. 3.18. Pakiety przechwycone przez Sniffera

# Implementacja listy kontroli ACL wewnątrz zabezpieczonej sieci

Najpierw tworzona jest lista kontroli ACL. „Permit icmp any any”, która zezwala na cały ruch ICMP w sieci. „Deny ip any 196.168.10.0 0.0.0.255” blokuje cały ruch IP do tej sieci.

„Deny ip 196.168.10.0 0.0.0.255 any” blokuje cały ruch z tej sieci do dowolnego celu. „Permit ip any any” zezwala na cały pozostały ruch. Następnie do interfejsów są przypisywane listy ACL, aby kontrolować na nich ruch.



Rys. 3.7 Ustawianie list kontrolnych

# Implementacja zabezpieczeń STP

Na początku konfiguracji zabezpieczenia STP jako główny węzeł drzewa(*root*) wybrano urządzenie *Switch3*, natomiast jako root-primary wybrano *Switch4*.

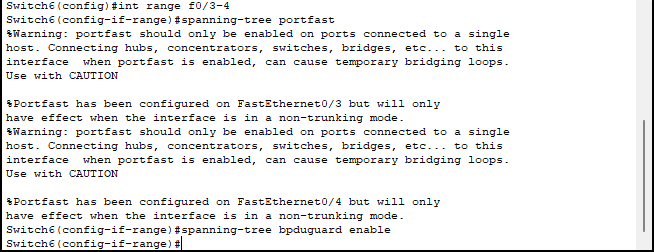


Rys. 3.19. Konfiguracja urządzenia Switch3 jako głównego węzła drzewa

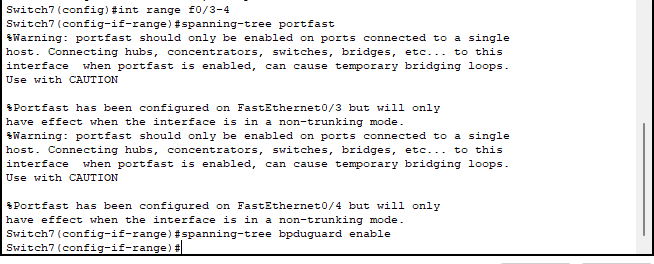


Rys. 3.20. Konfiguracja urządzenia Switch4 jako root-secondary

Następnie wykonano konfiguracje zabezpieczającą przed atakami manipulacyjnymi STP, polegające na ustawieniu funkcji *PortFast* oraz *BPDU Guard* na urządzeniach *Switch6* oraz *Switch7*. Dodatkowo, na głównych węzłach drzewa ustawiony został *Root Guard*.



Rys. 3.21. Konfiguracja PortFast oraz BPDU Guard na urządzeniu Switch6



Rys. 3.22. Konfiguracja PortFast oraz BPDU Guard na urządzeni Switch7



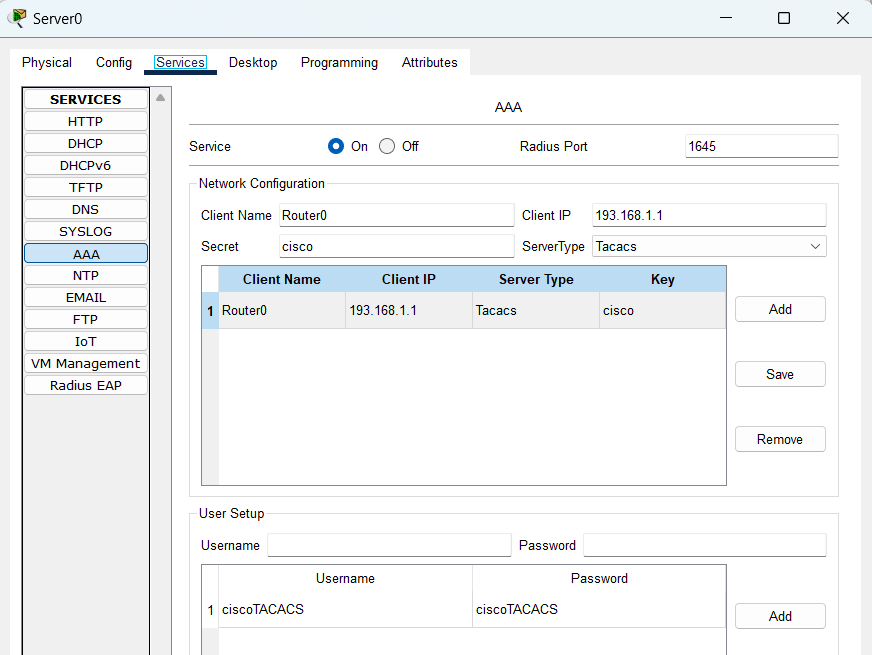
Rys. 3.23. Konfiguracja Root Guard na urządzeniu Switch4



Rys. 3.24. Konfiguracja Root Guard na urządzeniu Switch5

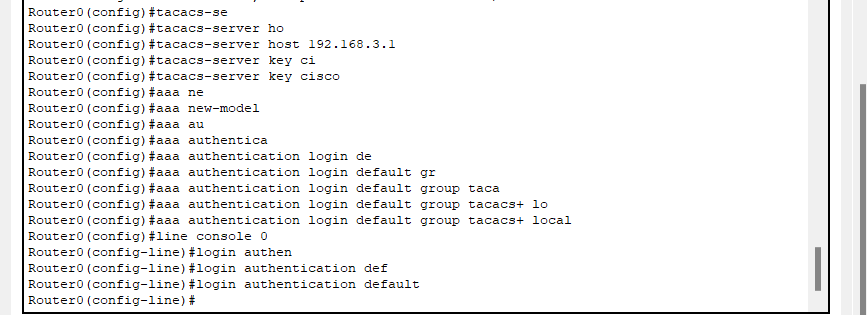
# Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+

Pierwszym krokiem podczas konfigurowania uwierzytelniania AAA przy użyciu TACACS+ było włączenie tej usługi na serwerze w podcięci *Network 1* oraz utworzenie wpisu dotyczącego routera, który ma być zabezpieczony, oraz danych do logowania: **ciscoTacacs**.



Rys. 3.25. Konfiguracja uwierzytelniania AAA przy użyciu TACACS+ na serwerze.

Następne kroki konfiguracyjne dotyczyły *Routera0*, i polegały na włączeniu uwierzytelniania AAA, określeniu serwera TACACS+ oraz włączenia logowania z wykorzystaniem TACACS+.



Rys. 3.26. Konfiguracja TACACS+ na routerze

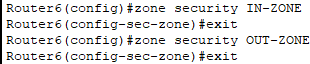
Po wykonaniu tych kroków dostęp do routera wymaga podania danych uwierzytelniających określonych podczas konfiguracji.



Rys. 3.27. Zabezpieczony dostęp wykorzystujący TACACS+

# Zaprojektowanie zapory sieciowej typu ZPF

Pierwszym krokiem podczas tworzenia zapory sieciowej typu ZPF było utworzenie dwóch stref: wewnętrznej i zewnętrznej.



Rys. 3.28. Tworzenie stref

Następnie utworzona została lista kontroli pozwalająca na ruch wychodzący z sieci wewnętrznej do sieci zewnętrznych.

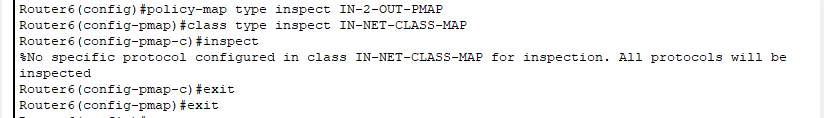


Rys. 3.29. Lista kontroli określająca zasady ruchu sieci wewnętrznej

W kolejnym kroku tworzony jest klasyfikator ruchu typu class-map definiujący cały ruch związany z ruchem bazującym na wcześniej zdefiniowanej liście kontroli ACL. Na tej podstawie tworzona jest mapa zasad policy-map, określającą kontrolę dostępu opartą na kontekście dla określonego ruchu sieciowego.



Rys. 3.30. Utworzenie klasyfikatora ruchu typu class-map

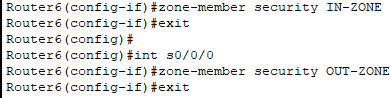


Rys. 3.31. Tworzenie mapy zasad policy-map

Ostatnim krokiem jest zastosowanie zapory poprzez określenie pary stref, przypisanie mapy zasad zajmującej się ruchem pomiędzy strefami oraz przypisanie interfejsów do poszczególnych stref.



Rys. 3.32. Utworzenie pary stref i przypisanie zasad obsługi ruchu



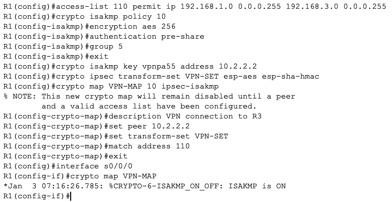
Rys. 3.33. Przypisanie interfejsów do poszczególnych stref

# Konfiguracja i weryfikacja sieci VPN IPsec

Na routerze R1 najpierw utworzono listę ACL 110, która zezwala na ruch z sieci 192.168.1.0 do 192.168.3.0. Utworzono politykę ISAKMP z numerem 10 i ustawiono szyfrowanie AES 256-bitowe. Następnie ustawiono uwierzytelnianie przy użyciu pre-shared key i ustawiono grupę Diffie-Hellman 5 dla wymiany kluczy. Ustawiono pre-shared key

„vpnpa55” dla peer o adresie 10.2.2.2. Utworzono zestaw transformacji IPsec nazwany „VPN- SET”, który używa szyfrowanie AES i uwierzytelnianie HMAC-SHA. Utworzono mapę kryptograficzną „VPN-MAP” z numerem sekwencji 10 używającą IPsec z ISAKMP. Ustawiono adres drugiej strony połączenia na 10.2.2.2. Przypisano zestaw transformacji „VPN- SET: do mapy kryptograficznej. Ustawiono dopasowanie ruchu IP zgodnie z ACL 110. Przypisano mapę kryptogradiczną do interfejsu S0/0/0.

Na routerze R3 podjęto podobne kroki, jednak z pewnymi różnicami takimi jak: ACL zezwala na ruch z sieci 192.168.3.0 do sieci 192.168.1.0, użyto adresu peer 10.1.1.2 zamiast 10.2.2.2 i przypisano mapę kryptograficzną do interfejsu S0/0/1 zamiast S0/0/0.



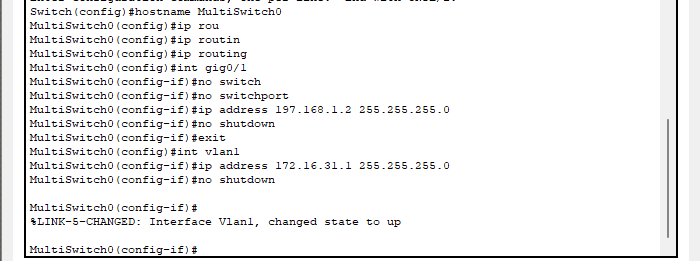
Rys. 3.34. Konfiguracja routera R1



Rys. 3.35. Konfiguracja routera R3

# Przełącznik warstwy trzeciej

Pierwszym krokiem podczas konfigurowania przełącznika warstwy trzeciej było włączenie routingu. Następnie zmieniono tryb interfejsu *GigabitEthernet 0/1* na tryb warstwy trzeciej, po czym skonfigurowano adresy poszczególnych interfejsów.

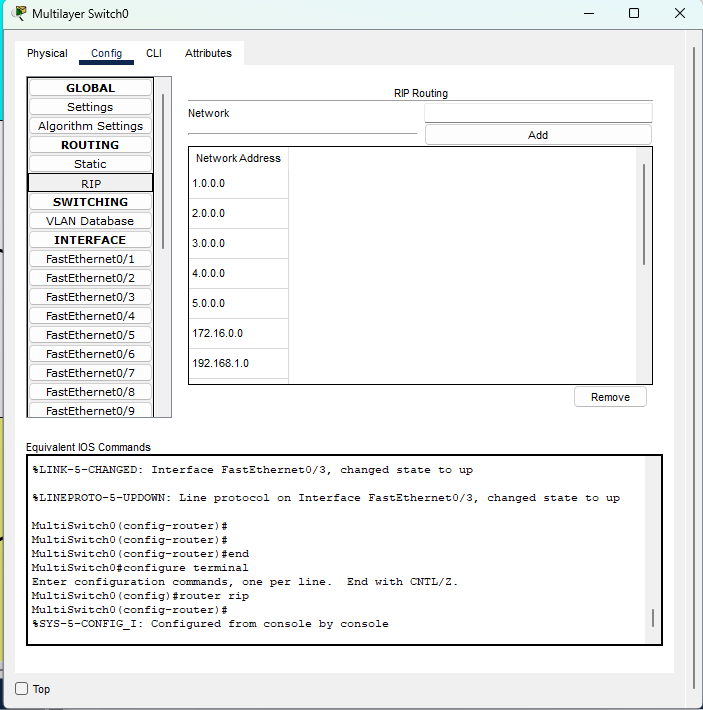


Rys. 3.36. Konfiguracja przełącznika warstwy trzeciej

Ostatnim krokiem konfiguracji było określenie trasy domyślnej oraz konfiguracja protokołu RIP na switchu.



Rys. 3.37. Określenie trasy domyślnej



Rys. 3.38. Konfiguracja protokołu RIP