|  |  |  |
| --- | --- | --- |
| **Politechnika Świętokrzyska**  Wydział Elektrotechniki, Automatyki i Informatyki | | |
| **Wprowadzenie do cyberbezpieczeństwa** – **Projekt** | | |
| **TEMAT:**  Projekt sieci dla biura rachunkowego | | **SKŁAD ZESPOŁU:**   * Przemysław Kałuziński (91271) * Jakub Kuśmierczyk () * Michał Kaczor (91268) |
| **DATA:**  15.01.2024 | **GRUPA:**  1IZ22B |

Spis treści

[1. Wstęp 3](#_Toc185619850)

[2. Struktura sieci 3](#_Toc185619851)

[3. Adresacja 3](#_Toc185619852)

[4. Podział na podsieci 3](#_Toc185619853)

[5. VLANy 3](#_Toc185619854)

[6. Serwer DHCP 3](#_Toc185619855)

[7. Konfiguracja urządzeń pod kątem dostępu SSH 3](#_Toc185619856)

[8. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS 3](#_Toc185619857)

[8.1. NTP 3](#_Toc185619858)

[8.2. CISCO IOS 3](#_Toc185619859)

[9. Lokalny SPAN 3](#_Toc185619860)

[10. Lista kontroli ACL wewnątrz zabezpieczonej sieci 3](#_Toc185619861)

[11. Zabezpieczenia STP 3](#_Toc185619862)

[12. Uwierzytelnianie AAA na serwerze przy użyciu TACACS+ 3](#_Toc185619863)

[13. Zapora sieciowa typu Private and Public (ZPF) 3](#_Toc185619864)

[14. Demilitarized Zone (DMZ)/Zone-Based Policy 3](#_Toc185619865)

[15. Wnioski 3](#_Toc185619866)

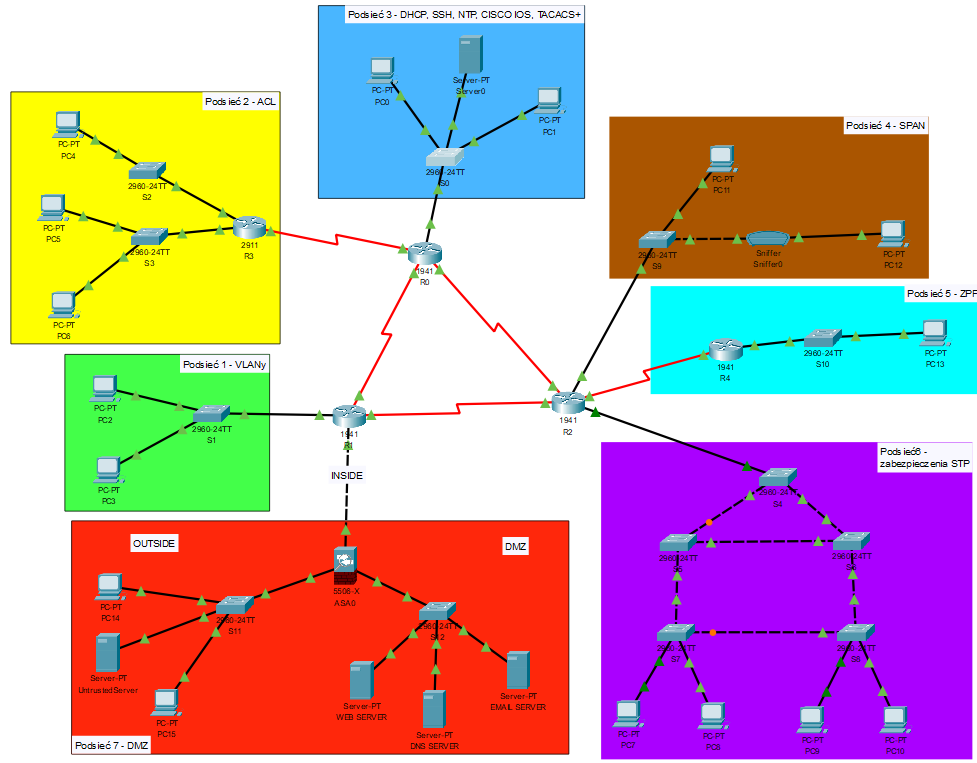
# Wstęp

Tematem naszego projektu było zaprojektowanie struktury sieci dla biura rachunkowego. W ramach realizacji zadania należało opracować schemat sieci oraz odpowiednio skonfigurować urządzenia wchodzące w jej skład. Do prac nad projektem wykorzystano oprogramowanie Cisco PacketTracer. Konfiguracja miała obejmować implementację następujących rozwiązań (w tabeli zaznaczono również, które z nich udało się zrealizować):

|  |  |
| --- | --- |
| **Wymagania na ocenę 3.0** | |
| Adresacja | Yes - Free ui icons |
| Podział na podsieci | Yes - Free ui icons |
| VLANy | Yes - Free ui icons |
| Serwer DHCP | Yes - Free ui icons |
| Konfiguracja urządzeń pod kątem dostępu SSH. | Yes - Free ui icons |
| Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS. | Yes - Free ui icons |
| Implementacja lokalnego SPAN. | Yes - Free ui icons |
| Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci. | Yes - Free ui icons |
| **Wymagania na ocenę 4.0** | |
| Realizacja wymagań na ocenę 3.0. | Yes - Free ui icons |
| Implementacja zabezpieczeń STP. | Yes - Free ui icons |
| Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+ lub RADIUS. | Yes - Free ui icons |
| Zaprojektowanie zapory sieciowej typu Private and Public. | Yes - Free ui icons |
| **Wymagania na ocenę 5.0** | |
| Realizacja wymagań na ocenę 3.0 oraz 4.0. | Yes - Free ui icons |
| Zaprojektowanie zapory sieciowej typu Demilitarized Zone (DMZ)/Zone-Based Policy. | Yes - Free ui icons |
| Konfiguracja i weryfikacja sieci VPN IPsec. | 8 Grunge Yes No Icon (PNG Transparent) | OnlyGFX.com |

# Struktura sieci

Na obrazie poniżej przedstawiono strukturę naszego projektu sieci.



# Podział na podsieci

Jednym z zadań był podział głównej sieci na podsieci. Wykorzystaliśmy tę możliwość, aby rozdzielić sieć na mniejsze segmenty, z których każdy odpowiada za inną funkcjonalność. Dzięki temu udało się uniknąć nadmiernego obciążenia pojedynczych urządzeń oraz poprawić czytelność i organizację konfiguracji. Każda z podsieci została oznaczona innym kolorem, tak jak to można zauważyć na poprzednim zdjęciu, aby podkreślić ich rozłączność. Dodatkowo przy każdej z podsieci znajduje się krótka notatka, która informuje o zaimplementowanych w niej rozwiązaniach.

Jesteśmy świadomi, że w rzeczywistych zastosowaniach takie podejście nie jest w pełni profesjonalne, ponieważ każda podsieć powinna być w pełni skonfigurowana i w pełni zintegrowana z całą infrastrukturą. Tylko w ten sposób można zagwarantować poprawność działania oraz bezpieczeństwo całej sieci. Jednak w ramach projektu przyjęte rozwiązanie miało na celu przede wszystkim zademonstrowanie naszej umiejętności implementacji wybranych funkcjonalności i osiągnięcia założonych celów.

# Adresacja

Poniżej znajdują się tabele adresacji dla poszczególnych podsieci w naszym projekcie. W przypadku, gdy jakiś interfejs nie posiada przydzielonych adresów IP lub jest nieaktywny, to nie został on uwzględniony.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Centrum sieci** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Se0/0/0 | 1.0.0.2 | 255.0.0.0 | -- |
| R0 | Se0/0/1 | 5.0.0.1 | 255.0.0.0 | -- |
| R1 | Se0/0/0 | 1.0.0.1 | 255.0.0.0 | -- |
| R1 | Se0/0/1 | 2.0.0.1 | 255.0.0.0 | -- |
| R2 | Se0/0/0 | 2.0.0.2 | 255.0.0.0 | -- |
| R2 | Se0/0/1 | 3.0.0.1 | 255.0.0.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 1 (VLANy)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R1 | Gig0/0.10 | 192.168.1.1 | 255.255.255.0 | -- |
| R1 | Gig0/0.20 | 192.168.2.2 | 255.255.255.0 | -- |
| S1 | Fa0/1 | -- | -- | -- |
| S1 | Fa0/2 | -- | -- | -- |
| S1 | Fa0/3 | -- | -- | -- |
| PC2 | Fa0 | 192.168.1.10 | 255.255.255.0 | 192.168.1.1 |
| PC3 | Fa0 | 192.168.2.10 | 255.255.255.0 | 192.168.2.2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 2 (ACL)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Se0/1/0 | 4.0.0.1 | 255.0.0.0 | -- |
| R3 | Se0/3/0 | 4.0.0.2 | 255.0.0.0 | -- |
| R3 | Gig0/1 | 196.168.10.1 | 255.255.255.0 | -- |
| R3 | Gig0/2 | 196.168.20.1 | 255.255.255.0 | -- |
| S2 | -- | -- | -- | -- |
| S3 | -- | -- | -- | -- |
| PC4 | Fa0 | 196.168.10.3 | 255.255.255.0 | 196.168.10.1 |
| PC5 | Fa0 | 196.168.20.3 | 255.255.255.0 | 196.168.20.1 |
| PC6 | Fa0 | 196.168.20.4 | 255.255.255.0 | 196.168.20.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 3 (DHCP, NTP, CISCO IOS, TACACS+)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Gig0/0 | 193.168.1.1 | 255.255.255.0 | -- |
| S0 | VLAN1 | 193.168.1.2 | 255.255.255.0 | 193.168.1.1 |
| PC0 | Fa0 | DHCP (193.168.1.5) | 255.255.255.0 | DHCP (193.168.1.1) |
| Server0 | Fa0 | 193.168.1.3 | 255.255.255.0 | 193.168.1.1 |
| PC1 | Fa0 | DHCP (193.168.1.4) | 255.255.255.0 | DHCP (193.168.1.1) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 4 (SPAN)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R2 | Gig0/0 | 194.168.1.1 | 255.255.255.0 | -- |
| S9 | VLAN 1 | 194.168.1.2 | 255.255.255.0 | 194.168.1.1 |
| PC11 | Fa0 | 194.168.1.3 | 255.255.255.0 | 194.168.1.1 |
| Sniffer0 | -- | -- | -- | -- |
| PC12 | Fa0 | 194.168.1.4 | 255.255.255.0 | 194.168.1.1 |

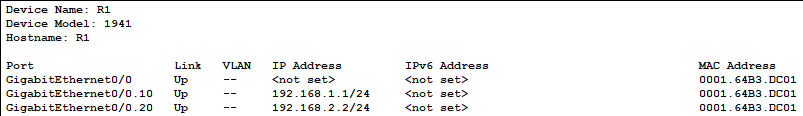
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 5 (ZPF)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R2 | Se0/1/0 | 7.0.0.1 | 255.0.0.0 | -- |
| R4 | Se0/0/0 | 7.0.0.2 | 255.0.0.0 | -- |
| R4 | Gig0/0 | 198.168.1.1 | 255.255.255.0 | -- |
| S10 | -- | -- | -- | -- |
| PC13 | Fa0 | 198.168.1.3 | 255.255.255.0 | 198.168.1.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 6 (STP)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R2 | Gig0/1 | 195.168.1.1 | 255.255.255.0 | -- |
| S4 | -- | -- | -- | -- |
| S5 | -- | -- | -- | -- |
| S6 | -- | -- | -- | -- |
| S7 | -- | -- | -- | -- |
| S8 | -- | -- | -- | -- |
| PC7 | Fa0 | 195.168.1.10 | 255.255.255.0 | 195.168.1.1 |
| PC8 | Fa0 | 195.168.1.11 | 255.255.255.0 | 195.168.1.1 |
| PC9 | Fa0 | 195.168.1.12 | 255.255.255.0 | 195.168.1.1 |
| PC10 | Fa0 | 195.168.1.13 | 255.255.255.0 | 195.168.1.1 |

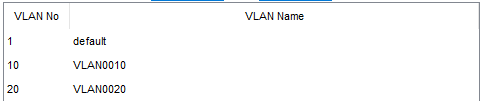
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 7 (DMZ)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R1 | Gig0/1 | 197.168.10.1 | 255.255.255.0 | -- |
| ASA0 | Gig1/1 | 197.168.10.2 | 255.255.255.0 | -- |
| ASA0 | Gig1/2 | 203.0.113.1 | 255.255.255.0 | -- |
| ASA0 | Gig1/3 | 197.168.20.1 | 255.255.255.0 | -- |
| S11 | -- | -- | -- | -- |
| S12 | -- | -- | -- | -- |
| PC14 | Fa0 | 203.0.113.2 | 255.255.255.0 | 203.0.113.1 |
| UntrustedServer | Fa0 | 203.0.113.3 | 255.255.255.0 | 203.0.113.1 |
| PC15 | Fa0 | 203.0.113.4 | 255.255.255.0 | 203.0.113.1 |
| WEB SERVER | Fa0 | 197.168.20.2 | 255.255.255.0 | 197.168.20.1 |
| DNS SERVER | Fa0 | 197.168.20.3 | 255.255.255.0 | 197.168.20.1 |
| EMAIL SERVER | Fa0 | 197.168.20.4 | 255.255.255.0 | 197.168.20.1 |

# VLANy

W podsieci „Podsieć 1” 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.



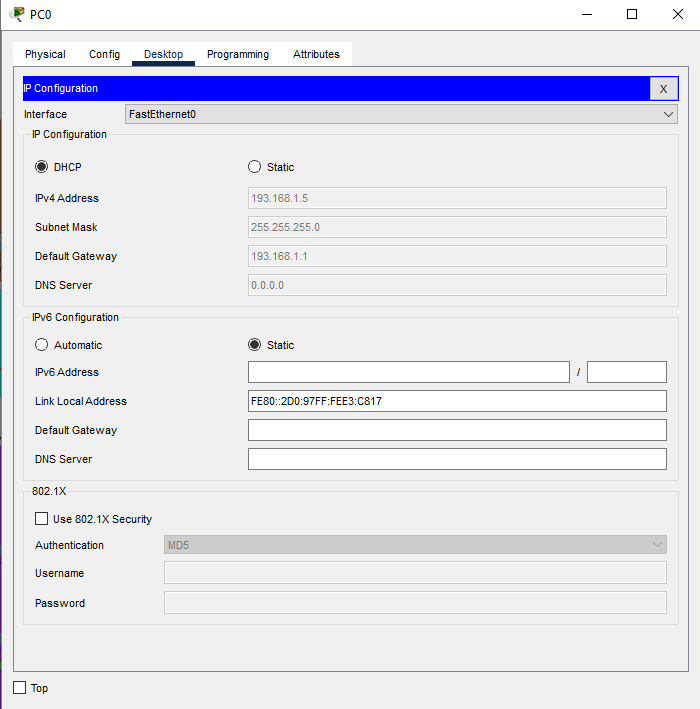
Konfiguracja adresów na routerze



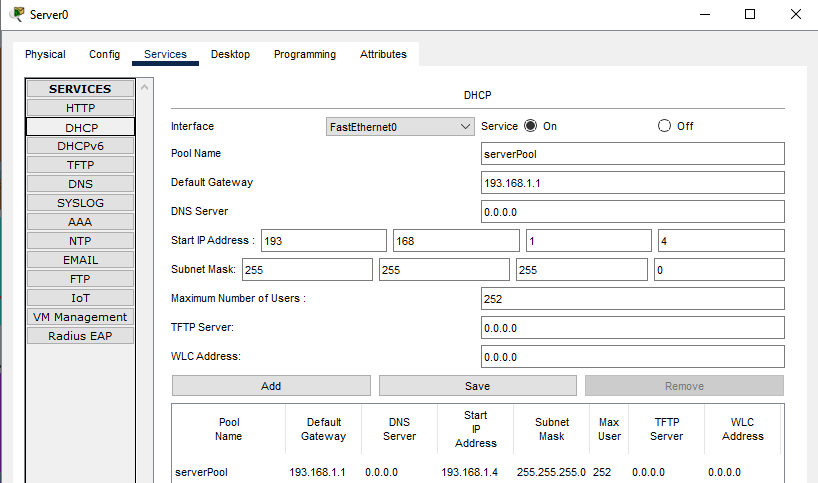
VLANy na switchu

# Serwer DHCP

Serwer w podsieci *„Podsieć 3”* 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.



Przykład działania protokołu DHCP dla hosta

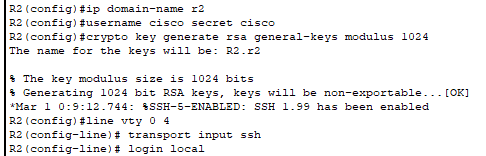


Przykładowa konfiguracja protokołu DHCP

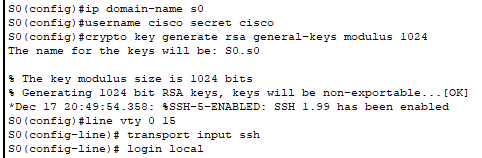
# Konfiguracja urządzeń pod kątem dostępu SSH

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

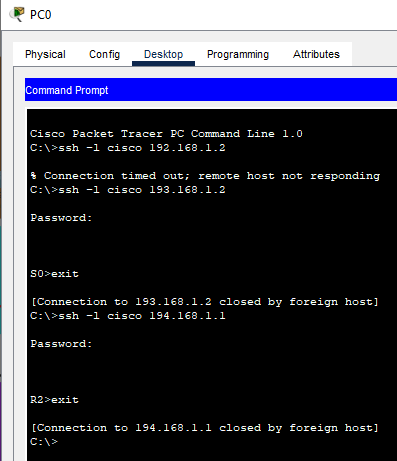
W przypadku routera jak i switcha konfiguracja wyglądała bardzo podobnie. Na początku określona została nazwa domeny, po czym utworzony został użytkownik z loginem cisco i zaszyfrowanym hasłem cisco. Następnie utworzony został 1024-bitowy klucz RSA. W kolejnym kroku wykonana została konfiguracja linii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



Konfiguracja routera pod kątem dostepu SSH



Konfiguracja switcha pod kątem dostępu SSH

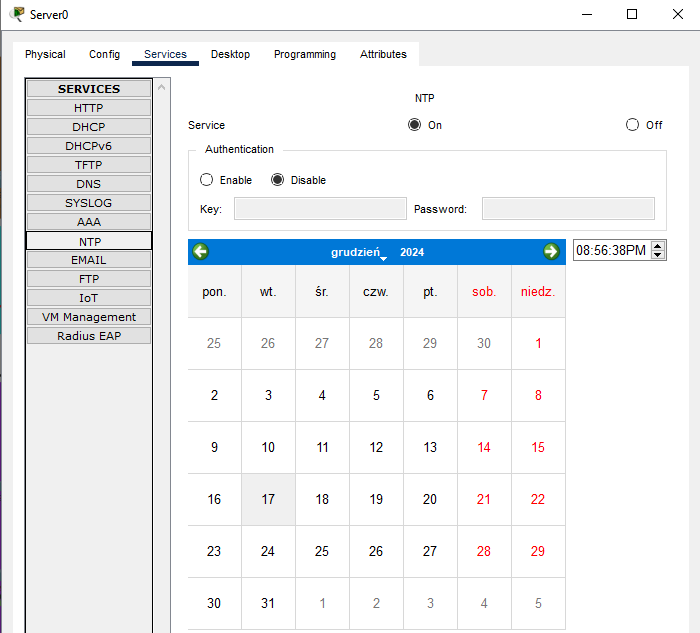


Logowanie poprzez SSH do switcha oraz routera

# Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS

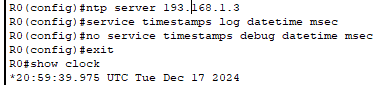
## NTP

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

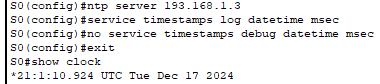


Włączenie usługi NTP

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.



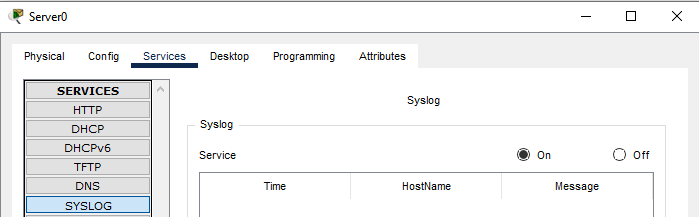
Konfiguracja NTP na routerze oraz weryfikacja działania (sprawdzenie czasu)



Konfiguracja NTP na switchu

## CISCO IOS

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



Włączenie usługi CISCO IOS na serwerze

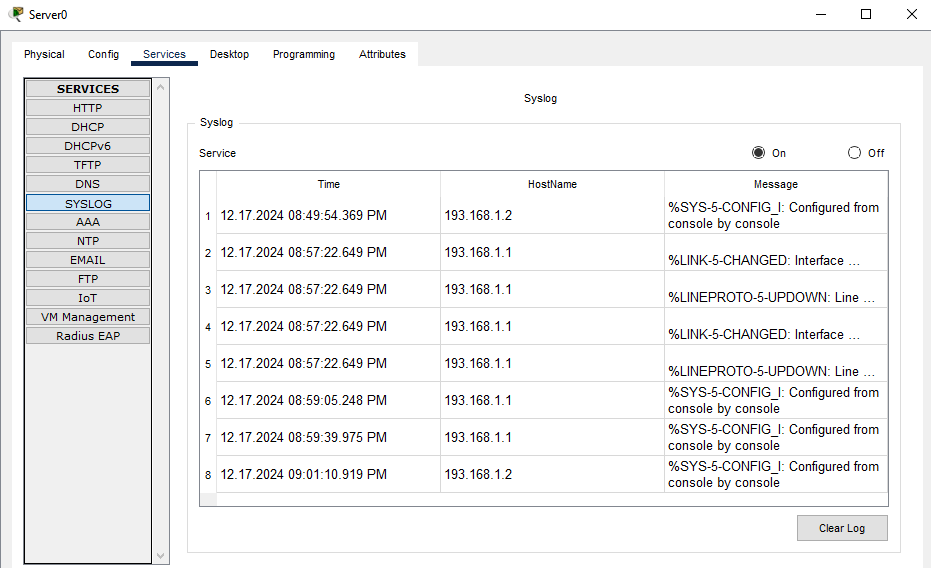
Następnie, z wykorzystaniem komendy *logging* na routerze oraz switchu określony został adres serwera z włączoną usługą logowania.



Konfiguracja CISCO IOS na switchu



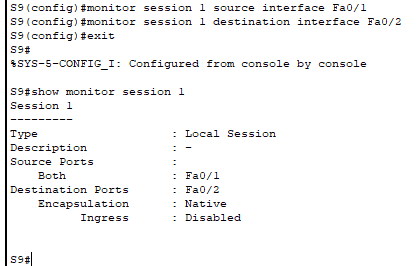
Konfiguracja CISCO IOS na routerze



Logi z routera oraz switcha

# Lokalny SPAN

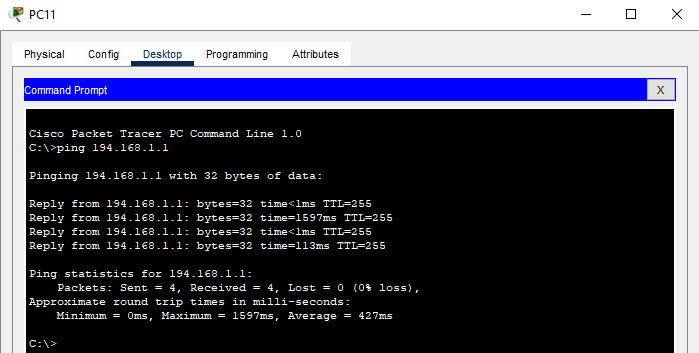
Konfiguracja lokalnego SPAN wykonana została w sieci *Network 3*. Switch2 został skonfigurowany tak, by ruch z portu FastEthernet 0/1 był kopiowany i przesyłany na port FastEthernet 0/2.



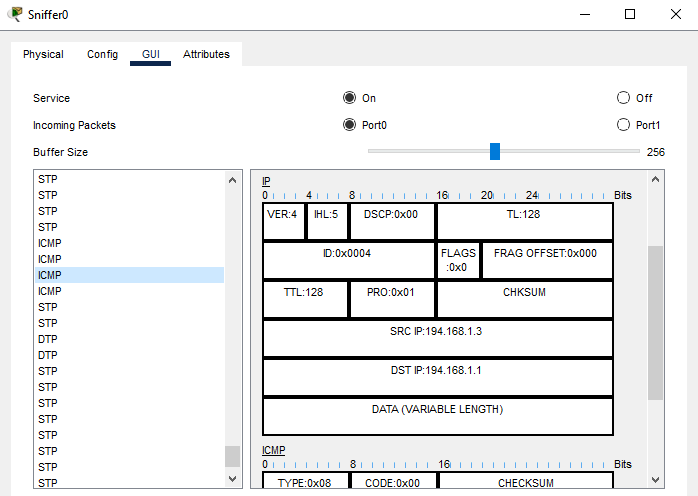
Konfiguracja lokalnego SPAN

Poniżej zaprezentowano pakiety przechwycone przez Sniffera prezentujące działanie

STP.



Wysyłanie poleceń „ping” z PC11 do routera R2

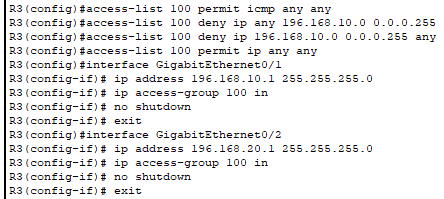


Pakiety przechwycone przez Sniffera

# Lista 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.



Ustawianie list kontrolnych

# Zabezpieczenia STP

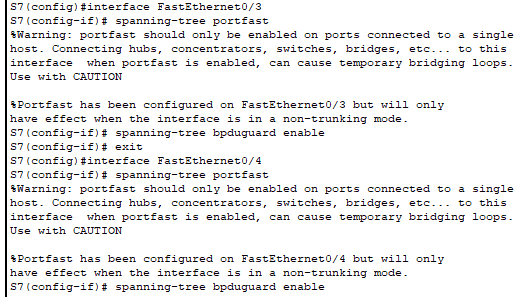
Na początku konfiguracji zabezpieczenia STP jako główny węzeł drzewa(root) wybrano urządzenie Switch3, natomiast jako root-primary wybrano Switch4.



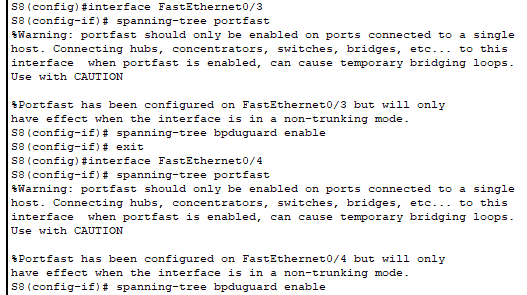
Konfiguracja urządzenia Switch3 jako głównego węzła drzewa



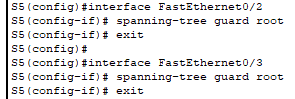
Konfiguracja urządzenia Switch4 jako root-secondary



Konfiguracja PortFast oraz BPDU Guard na urządzeniu Switch6



Konfiguracja PortFast oraz BPDU Guard na urządzeni Switch7



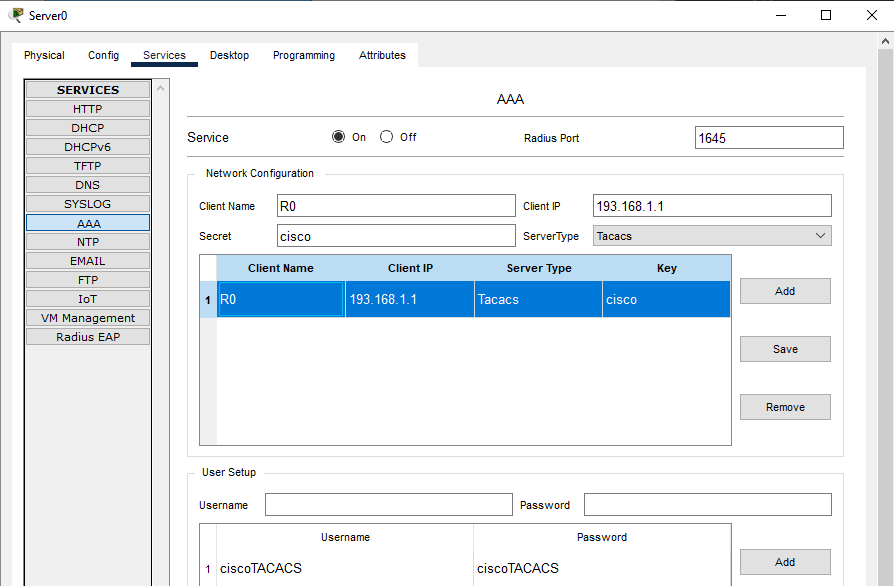
Konfiguracja Root Guard na urządzeniu Switch4



Konfiguracja Root Guard na urządzeniu Switch5

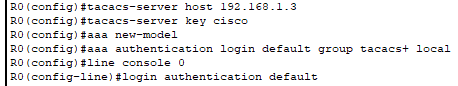
# Uwierzytelnianie AAA na serwerze przy użyciu TACACS+

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**.



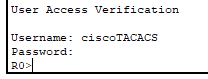
Konfiguracja uwierzytelniania AAA przy użyciu TACACS+ na serwerze.

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



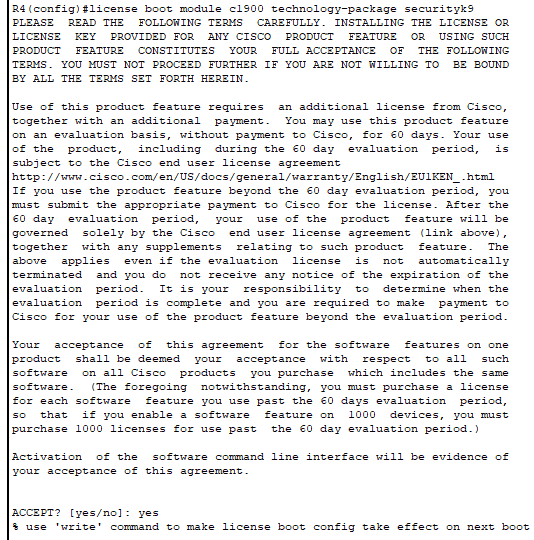
Konfiguracja TACACS+ na routerze

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



Zabezpieczony dostęp wykorzystujący TACACS+

# Zapora sieciowa typu Private and Public (ZPF)



Aktywacja pakietu funkcjonalności dla zapory sieciowej ZPF

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



Tworzenie stref

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

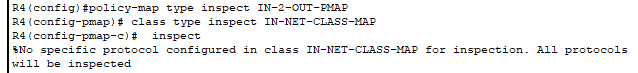


Lista kontroli określająca zasady ruchu sieci wewnętrznej

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.



Utworzenie klasyfikatora ruchu typu class-map

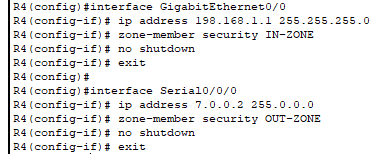


Tworzenie mapy zasad policy-map

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

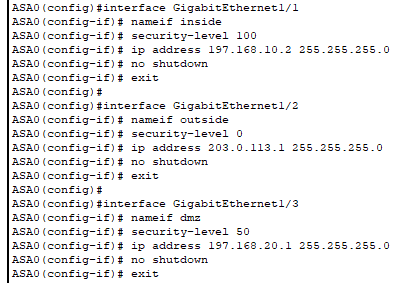


Utworzenie pary stref i przypisanie zasad obsługi ruchu



Przypisanie interfejsów do poszczególnych stref

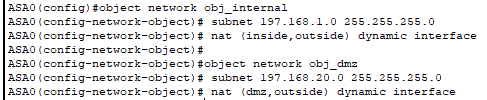
# Demilitarized Zone (DMZ)/Zone-Based Policy



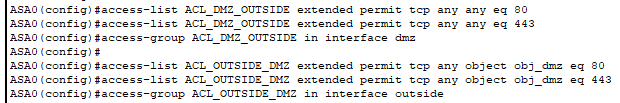
Konfiguracja interfejsów dla poszczególnych stref



Konfiguracja tras statycznych



Konfiguracja NAT



Dostęp dla ruchu z DMZ do zewnętrznej sieci oraz z zewnętrznej sieci do DMZ (ograniczony do serwisów)



Tworzenie VLAN 10 (dla sieci zewnętrznej)



Tworzenie VLAN 20 (dla DMZ)

# Wnioski