|  |  |  |
| --- | --- | --- |
| **Politechnika Świętokrzyska**  Wydział Elektrotechniki, Automatyki i Informatyki | | |
| **Bezpieczeństwo Infrastruktury Sieciowej** – **Projekt** | | |
| **TEMAT:**  Projekt sieci dla biura rachunkowego | | **SKŁAD ZESPOŁU:**   * Przemysław Kałuziński (91271) * Jakub Kuśmierczyk (97504) * Michał Kaczor (91268) |
| **DATA:**  01.06.2025 | **GRUPA:**  1IZ22B |

Spis treści

[1. Wstęp 3](#_Toc186532071)

[2. Struktura sieci 4](#_Toc186532072)

[3. Podział na podsieci 5](#_Toc186532073)

[4. Adresacja 5](#_Toc186532074)

[5. Zabezpieczenia 7](#_Toc186532075)

[6. Routing RIP 8](#_Toc186532076)

[7. VLANy 9](#_Toc186532077)

[8. Serwer DHCP 9](#_Toc186532078)

[9. Konfiguracja urządzeń pod kątem dostępu SSH 11](#_Toc186532079)

[10. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS 13](#_Toc186532080)

[10.1. NTP 13](#_Toc186532081)

[10.2. Zarządzanie i raportowanie Cisco IOS 14](#_Toc186532082)

[11. Lokalny SPAN 16](#_Toc186532083)

[12. Lista kontroli ACL wewnątrz zabezpieczonej sieci 17](#_Toc186532084)

[13. Zabezpieczenia STP 18](#_Toc186532085)

[14. Uwierzytelnianie AAA na serwerze przy użyciu TACACS+ 20](#_Toc186532086)

[15. Zapora sieciowa typu Private and Public (ZPF) 21](#_Toc186532087)

[16. Demilitarized Zone (DMZ)/Zone-Based Policy 23](#_Toc186532088)

[17. Wnioski 24](#_Toc186532089)

# Wstęp

# Struktura sieci

# Podział na podsieci

# 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 | 3.0.0.2 | 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 (DHCP, SSH, NTP, CISCO IOS, TACACS+)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Gig0/0 | 191.168.1.1 | 255.255.255.0 | -- |
| S0 | VLAN1 | 191.168.1.2 | 255.255.255.0 | 191.168.1.1 |
| PC0 | Fa0 | DHCP (191.168.1.10) | 255.255.255.0 | DHCP (191.168.1.1) |
| Server0 | Fa0 | 191.168.1.3 | 255.255.255.0 | 191.168.1.1 |
| PC1 | Fa0 | DHCP (191.168.1.11) | 255.255.255.0 | DHCP (191.168.1.1) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 2 (dwie standardowe 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 | Gig0/0 | 192.168.10.1 | 255.255.255.0 | -- |
| R3 | Gig0/1 | 192.168.20.1 | 255.255.255.0 | -- |
| S1 | -- | -- | -- | -- |
| S2 | -- | -- | -- | -- |
| PC2 | Fa0 | 192.168.10.2 | 255.255.255.0 | 192.168.10.1 |
| PC3 | Fa0 | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 3 (dwie rozszerzone ACL)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Se0/1/1 | 5.0.0.1 | 255.0.0.0 | -- |
| R4 | Se0/3/0 | 5.0.0.2 | 255.0.0.0 | -- |
| R4 | Gig0/0 | 193.168.10.1 | 255.255.255.0 | -- |
| R4 | Gig0/1 | 193.168.20.1 | 255.255.255.0 | -- |
| S3 | -- | -- | -- | -- |
| S4 | -- | -- | -- | -- |
| PC4 | Fa0 | 193.168.10.4 | 255.255.255.0 | 193.168.10.1 |
| PC5 | Fa0 | 193.168.20.5 | 255.255.255.0 | 193.168.20.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 4 (zabezpieczenia STP)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R1 | Gig0/0 | 194.168.1.1 | 255.255.255.0 | -- |
| SCentral | -- | -- | -- | -- |
| S5 | -- | -- | -- | -- |
| S6 | -- | -- | -- | -- |
| S7 | -- | -- | -- | -- |
| S8 | -- | -- | -- | -- |
| PC6 | Fa0 | 194.168.1.6 | 255.255.255.0 | 194.168.1.1 |
| PC7 | Fa0 | 194.168.1.7 | 255.255.255.0 | 194.168.1.1 |
| PC8 | Fa0 | 194.168.1.8 | 255.255.255.0 | 194.168.1.1 |
| PC9 | Fa0 | 194.168.1.9 | 255.255.255.0 | 194.168.1.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 5 (FHRP - HSRP)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| HSRP (adres wirtualny) | -- | 195.168.1.254 | -- | -- |
| R1 (adres fizyczny) | Gig0/1 | 195.168.1.1 | 255.255.255.0 | -- |
| R2 (adres fizyczny) | Gig0/0 | 195.168.1.2 | 255.255.255.0 | -- |
| S9 | -- | -- | -- | -- |
| S10 | -- | -- | -- | -- |
| PC10 | Fa0 | 195.168.1.10 | 255.255.255.0 | 195.168.1.254 |
| PC11 | Fa0 | 195.168.1.11 | 255.255.255.0 | 195.168.1.254 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 6 (EtherChannel)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R2 | Gig0/1 | 196.168.1.1 | 255.255.255.0 | -- |
| S11 | -- | -- | -- | -- |
| S12 | -- | -- | -- | -- |
| S13 | -- | -- | -- | -- |
| PC12 | Fa0 | 196.168.1.12 | 255.255.255.0 | 196.168.1.1 |
| PC13 | Fa0 | 196.168.1.13 | 255.255.255.0 | 196.168.1.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 7 (VLANy)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Gig0/0.10 | 197.168.1.1 | 255.255.255.0 | -- |
| R0 | Gig0/0.20 | 197.168.2.1 | 255.255.255.0 | -- |
| R0 | Gig0/0.30 | 197.168.3.1 | 255.255.255.0 | -- |
| S1 | VLAN1 | 197.168.1.10 | 255.255.255.0 | 197.168.1.1 |
| PC14 | Fa0 | 197.168.1.14 | 255.255.255.0 | 197.168.1.1 |
| PC15 | Fa0 | 197.168.1.15 | 255.255.255.0 | 197.168.1.1 |
| PC16 | Fa0 | 197.168.2.16 | 255.255.255.0 | 197.168.2.1 |
| PC17 | Fa0 | 197.168.2.17 | 255.255.255.0 | 197.168.2.1 |
| PC18 | Fa0 | 197.168.3.18 | 255.255.255.0 | 197.168.3.1 |
| PC19 | Fa0 | 197.168.3.19 | 255.255.255.0 | 197.168.3.1 |

# Zabezpieczenia

# Dynamiczny protokół routingu OSPF

**Dlaczego OSPF:**

* W pełni dynamiczny.
* Obsługuje zmienność tras i priorytetowanie.
* Automatycznie aktualizuje routing po zmianach w topologii.
* Możesz podzielić sieć na **obszary (areas)**, np. jeden duży Area 0 (backbone).

# Serwer DHCP

## Zabezpieczenia przed atakami DHCP

**Co musimy zrobić:**

1. ✅ Włączyć **DHCP snooping** globalnie na przełączniku.
2. ✅ Włączyć DHCP snooping dla odpowiedniego **VLANu** (np. VLAN 1, jeśli nie zmieniałeś).
3. ✅ Oznaczyć **port połączony z legalnym serwerem DHCP** jako **zaufany (trusted)**.
4. ✅ Pozostałe porty powinny być **niezaufane (domyślnie)** – na nich ruch DHCP będzie filtrowany.
5. ✅ Upewnić się, że serwer DHCP działa prawidłowo.

**Efekt końcowy:**

* **Serwer DHCP** (Server0) może bez problemu przydzielać adresy IP.
* **Komputery PC0 i PC1** otrzymują poprawne adresy IP tylko od **zaufanego serwera**.
* **Fałszywe serwery DHCP (np. podłączone przez innego hosta)** zostaną **zablokowane** – przełącznik nie dopuści ich ofert.

**Jak przetestować?**

1. Ustaw PC0 i PC1 na **DHCP**.
2. Upewnij się, że Server0 ma włączoną usługę DHCP i skonfigurowaną pulę adresów.
3. (Opcjonalnie) Dodaj inny komputer np. PC2 i uruchom na nim **DHCP service** (fałszywy serwer), podłączając go do Fa0/3 — DHCP snooping zablokuje jego pakiety DHCP OFFER/DISCOVER.

# Konfiguracja urządzeń pod kątem dostępu SSH

# Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS (syslog)

## NTP

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Włączenie usługi NTP na serwerze

## Zarządzanie i raportowanie Cisco IOS

# Uwierzytelnianie AAA na serwerze przy użyciu TACACS+

# Zabezpieczenia przed atakami MAC

✅ **Główna technologia: Port Security**

To narzędzie dostępne na switchach Cisco, które pozwala ograniczyć liczbę adresów MAC dozwolonych na danym porcie i/lub zdefiniować konkretne adresy MAC, które mogą się połączyć.

Polecenie Opis

switchport port-security Włącza Port Security

switchport port-security maximum 1 Tylko 1 MAC na porcie

switchport port-security violation restrict Blokuje i loguje naruszenie (bez wyłączania portu)

switchport port-security mac-address sticky Uczy się MAC-a i zapisuje go jako "dozwolony"

Atak Zabezpieczenie

MAC Flooding – zalewanie tablicy CAM wieloma MAC-ami maximum 1 ogranicza

MAC Spoofing – podszywanie się pod inny MAC sticky + violation restrict/shutdown

Nieautoryzowane urządzenia tylko określony MAC może działać

**Sprawdzenie statusu:**

show port-security interface FastEthernet0/3

# VLANy

## Routing między VLANami

**🔁 Routing między VLANami – podsumowanie (już gotowe)**

Zgodnie z konfiguracją:

* Router R0 posiada podinterfejsy z tagowaniem dot1Q, więc ruch między VLANami może być kierowany (routing działa).
* Switch S1 ma port trunkowy (Fa0/1) do routera.

Ten routing już działa – urządzenia z różnych VLANów mogą się komunikować **za pośrednictwem routera**.

## Zabezpieczenia przed atakami VLANami

W sieciach VLAN należy się zabezpieczyć głównie przed:

* **VLAN Hopping** (atak przez fałszywe trunkowanie),
* **Nieautoryzowany dostęp do trunków**,
* **Nieprawidłowa konfiguracja VTP** (jeśli używany),
* **Unused ports attack** (atak przez porty nieużywane).

# EtherChannel

show etherchannel summary

# Konfiguracja FHRP

# Dwie standardowe listy kontroli ACL wewnątrz zabezpieczonej sieci

Na przykład:

1. **ACL 10** – zablokować PC2 (192.168.10.2) dostęp do routera R3, czyli zablokuj ruch przychodzący z tego hosta na interfejsie Gig0/0.
2. **ACL 20** – zablokować cały ruch wychodzący z routera R3 **do** PC3 (192.168.20.3), czyli zablokować na interfejsie Gig0/1 ruch wychodzący.

**✅ TESTY**

Po wdrożeniu ACL sprawdź:

* Z PC2 nie da się pingować R3 (192.168.10.1).
* Z routera (lub innej podsieci) nie da się pingować PC3.
* Inni użytkownicy w tej podsieci nie mają ograniczeń.

# Dwie rozszerzone listy kontroli ACL wewnątrz zabezpieczonej sieci

Załóżmy następujące wymagania:

1. **ACL 110** – zablokować PC4 (193.168.10.4) **wszelki ruch HTTP (port 80)** wychodzący w świat (np. do routera R0 i dalej).
2. **ACL 120** – zablokować PC5 (193.168.20.5) możliwość **telnetowania (port 23)** **do jakichkolwiek urządzeń**, ale tylko w obrębie własnej podsieci (np. telnet do S4, R4 itd.).

**✅ TESTY**

* Na PC4: spróbuj otworzyć stronę przez przeglądarkę (symulacja HTTP) — będzie zablokowane.
* Na PC5: spróbuj połączyć się przez Telnet do innego hosta w tej samej podsieci (telnet 193.168.20.X) — powinno być zablokowane.
* Inne typy ruchu jak ping, SSH, FTP – będą działać.

# Zabezpieczenia STP

# Wnioski