|  |  |  |
| --- | --- | --- |
| **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

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 projektowe** | |
| dostępy SSH | Yes - Free ui icons |
| dynamiczny protokoły routingu (OSPF, EIGRP) | Yes - Free ui icons |
| VLANy | Yes - Free ui icons |
| routing między vlanmi | Yes - Free ui icons |
| EtherChannel | Yes - Free ui icons |
| konfiguracja FHRP | Yes - Free ui icons |
| konfiguracja syslogu | Yes - Free ui icons |
| konfiguracja NTP | Yes - Free ui icons |
| konfiguracja AAA | Yes - Free ui icons |
| konfiguracja serwera DHCP | Yes - Free ui icons |
| dwie standardowe listy dostępu ACL | Yes - Free ui icons |
| dwie rozszerzone listy dostępu ACL | Yes - Free ui icons |
| zabezpieczenia przez atakami MAC | Yes - Free ui icons |
| zabezpieczenia przez atakami VLAN | Yes - Free ui icons |
| zabezpieczenia przez atakami DHCP | Yes - Free ui icons |
| zabezpieczenia przez atakami STP | Yes - Free ui icons |
| konfiguracja poziomów dostępowych na urządzeniach sieciowych | Yes - Free ui icons |

# Struktura sieci

Na obrazie poniżej przedstawiono strukturę naszego projektu sieci.

ZDJĘCIE

Struktura sieci z programu Packet Tracer

# Podział na podsieci

Przed implementacją poszczególnych rozwiązań, podzieliliśmy naszą sieć na mniejsze podsieci, z których każda odpowiada za inną funkcjonalność. Dzięki temu udało się uniknąć nadmiernego obciążenia pojedynczych urządzeń oraz poprawić czytelność i organizację konfiguracji. Podsieci zostały oznaczone innymi kolorami, tak jak to można zauważyć na poprzednim zdjęciu, aby podkreślić ich rozłączność. Dodatkowo przy każdej podsieci znajduje się krótka notatka, informująca o zaimplementowanych w niej funkcjach.

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 | 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

Urządzenia sieciowe w naszym projekcie zostały odpowiednio zabezpieczone przed nieautoryzowanym dostępem osób trzecich. Skonfigurowano między innymi zabezpieczenia dostępu do trybu uprzywilejowanego, portów konsolowych oraz wirtualnych terminali (VTY). W przypadku urządzenia router R0 zastosowano autoryzację przy użyciu TACACS+. Poniżej przedstawiono wykorzystane w projekcie dane uwierzytelniania oraz przykładową konfigurację zabezpieczeń na jednym z urządzeń.

Dla celów projektu zastosowano następujące hasła:

* **Domyślny dostęp do urządzenia:** username: cisco / hasło: cisco
* **Dostępy różnych poziomów (dla R0 i S0):** 
  + **Admin (privilege 15):** username: admin/ hasło: admin123
  + **Technik (privilege 10):** username: technik / hasło: technik123
  + **Junior (privilege 5):** username: junior / hasło: junior123
* **Tryb uprzywilejowany (enable):** hasło: class
* **Dane dostępu do routera R0 (TACACS+):** username: ciscoTACACS / hasło: ciscoTACACS

ZDJĘCIE

Przykładowa konfiguracja zabezpieczeń routera w naszej sieci

# 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

Serwer PT w „Podsieci 1” został skonfigurowany do automatycznego przydzielania adresów IP komputerom i innym urządzeniom znajdującym się w tej samej podsieci. Odbywa się to z wykorzystaniem protokołu DHCP (ang. Dynamic Host Configuration Protocol). DHCP pozwala na dynamiczne przypisywanie adresów IP, masek podsieci, bram domyślnych oraz serwerów DNS bez konieczności ręcznego konfigurowania tych parametrów na każdym urządzeniu.

Serwer wykorzystuje zdefiniowaną pulę adresów IP, z której losowo przydziela adresy do urządzeń w podsieci. Dzięki temu proces konfiguracji urządzeń sieciowych staje się szybszy, a zarządzanie adresacją w sieci bardziej efektywne. Poniżej przedstawiono przykładowy adres IP przypisany jednemu z hostów za pomocą tego protokołu.

ZDJĘCIE

Przykład działania protokołu DHCP dla hosta

ZDJĘCIE

Konfiguracja protokołu DHCP na serwerze

## 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

Dostęp SSH (ang. Secure Shell) zapewnia bezpieczny, szyfrowany kanał komunikacji z urządzeniami sieciowymi z poziomu innych urządzeń. W naszym przypadku do konfiguracji urządzeń pod kątem dostępu SSH wybraliśmy dwa urządzenia: router R2 oraz switch S0.

Konfiguracja zarówno routera, jak i switcha przebiegała w podobny sposób. Najpierw należało ustawić nazwę domeny, która jest wymagana do wygenerowania klucza kryptograficznego. Następnie dla routera R2 utworzono użytkownika o nazwie „cisco” z przypisanym zaszyfrowanym hasłem „cisco”. Dla switcha S0 utworzyliśmy trzech osobnych użytkowników, każdy z innym poziomem dostępu, ale więcej na ten temat znajduje się w punkcie 10 sprawozdania. Kolejnym krokiem było wygenerowanie 1024-bitowego klucza RSA, niezbędnego do działania protokołu SSH.

Po wygenerowaniu klucza skonfigurowano linie VTY, umożliwiając dostęp do urządzeń za pomocą SSH. Linie VTY zostały dostosowane tak, aby wykorzystywały dane uwierzytelniające wcześniej utworzonych użytkowników. Szczegółowy przebieg konfiguracji dla urządzeń został przedstawiony w formie screenów z terminala poniżej.

Konfiguracja routera pod kątem dostepu SSH

Konfiguracja switcha pod kątem dostępu SSH

W celu zaprezentowania poprawności działania dostępu SSH, ustanowiono połączenie ze switchem S0 oraz następnie z routerem R2 z poziomu terminala CMD komputera PC0. Dzięki temu istnieje możliwość konfiguracji urządzeń sieciowych pośrednio z poziomu innych urządzeń – tak jak w tym przypadku, można konfigurować S0 lub R2 z terminala komputera PC0.

Logowanie poprzez SSH do switcha oraz routera

# Uwierzytelnianie AAA na serwerze przy użyciu TACACS+

W celu zwiększenia bezpieczeństwa dostępu do urządzeń sieciowych, zaimplementowano uwierzytelnianie AAA (Authentication, Authorization, and Accounting) przy użyciu protokołu TACACS+ (Terminal Access Controller Access-Control System Plus).

Pierwszym krokiem było włączenie usługi uwierzytelniania AAA na serwerze zlokalizowanym w „Podsieci 1” oraz wybranie metody TACACS+. Następnie dodano dane urządzenia (routera R0) korzystającego z usługi uwierzytelniania, w tym adres IP oraz hasło współdzielone dla komunikacji między serwerem a routerem. Dla celów projektu hasło to: ciscoTACACS.

Konfiguracja uwierzytelniania AAA przy użyciu TACACS+ na serwerze

Dalsza konfiguracja dotyczyła już routera R0. Na urządzeniu włączono funkcję AAA, co umożliwiło korzystanie z zewnętrznych serwerów uwierzytelniania, a następnie zdefiniowano serwer TACACS+ poprzez wskazanie jego adresu IP, hasła współdzielonego oraz portu komunikacji. Ostatecznie router został skonfigurowany tak, aby logowanie do urządzenia odbywało się z wykorzystaniem serwera TACACS+, a nie lokalnie na urządzeniu.

Konfiguracja TACACS+ na routerze R0

Po zakończeniu konfiguracji dostęp do routera wymaga podania danych uwierzytelniających skonfigurowanych na serwerze TACACS+. Dzięki temu wszystkie próby logowania są rejestrowane i mogą być monitorowane na serwerze, co zwiększa kontrolę oraz bezpieczeństwo sieci.

Zabezpieczony dostęp wykorzystujący uwierzytelnianie TACACS+

# Konfiguracja poziomów dostępowych na urządzeniach sieciowych

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

## NTP

Network Time Protocol (NTP) to protokół służący do synchronizacji zegarów systemowych w urządzeniach sieciowych. Zapewnia dokładne i spójne ustawienia czasu w całej infrastrukturze, co ma kluczowe znaczenie dla działania usług sieciowych, takich jak logowanie zdarzeń, uwierzytelnianie czy analiza ruchu sieciowego. NTP działa w modelu hierarchicznym, gdzie serwery wyższego poziomu synchronizują się z zegarami atomowymi lub GPS, a urządzenia w sieci lokalnej pobierają czas od lokalnych serwerów NTP, minimalizując opóźnienia.

W celu konfiguracji protokołu NTP w naszej sieci należało zacząć od włączenia usługi NTP na serwerze znajdującym się w „Podsieci 1” oraz ustawienia bieżącego czasu, wobec którego będą synchronizowane pozostałe urządzenia.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Włączenie usługi NTP na serwerze

Następnie na routerze R0 i switchu S0 ustawiono adres IP serwera NTP oraz włączono funkcję logowania ze znacznikami czasu, które zawierają dokładne informacje o dacie oraz godzinie.

Konfiguracja NTP na routerze oraz weryfikacja działania (sprawdzenie czasu)

Konfiguracja NTP na switchu oraz weryfikacja działania (sprawdzenie czasu)

## Zarządzanie i raportowanie CISCO IOS (syslog)

Cisco IOS wspiera efektywne zarządzanie siecią dzięki funkcji rejestrowania zdarzeń (syslog) i konfiguracji serwerów logów. Funkcja pozwala na przesyłanie zdarzeń z urządzeń sieciowych do zdalnego serwera, co ułatwia późniejsze zarządzanie logami i ich analizę.

W celu implementacji tego rozwiązania w naszej sieci, podobnie jak w przypadku konfiguracji NTP, pierwszym krokiem było włączenie usługi SYSLOG na serwerze w „Podsieci 1”

Obraz zawierający tekst, oprogramowanie, numer, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Włączenie usługi SYSLOG na serwerze

Następnie, z wykorzystaniem komendy logging na routerze R0 oraz switchu S0, został określony adres serwera z włączoną usługą logowania, co umożliwiło przesyłanie logów systemowych z tych urządzeń do centralnego serwera syslog.

Konfiguracja SYSLOG na switchu S0

Konfiguracja SYSLOG na routerze R0

Aby zweryfikować poprawność działania opcji rejestrowania zdarzeń systemowych, wystarczyło przejść do zakładki SYSLOG na serwerze w „Podsieci 1”. Jak można zaobserwować na poniższym zrzucie ekranu, na serwer spłynęły wszystkie logi dotyczące zmian w konfiguracji wybranych urządzeń sieciowych.

Logi z routera R0 oraz switcha S0, które spłynęły na główny serwer

# 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

# 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 przed atakami STP

# Konfiguracja FHRP

# EtherChannel

show etherchannel summary

# VLANy

W ramach „Podsieci 7” zostały utworzone trzy VLAN-y: VLAN 10, VLAN 20 oraz VLAN 30. Pozwoliło nam to na logiczne podzielenie fizycznej sieci na odseparowane segmenty. Dzięki temu urządzenia należące do różnych VLAN-ów mogą działać w tej samej fizycznej infrastrukturze, ale ich ruch sieciowy pozostaje oddzielony. W naszym projekcie sieci do każdego z VLANów przypisano po dwa komputery PC.

Konfiguracja adresów na routerze R1 połączonym ze switchem S1 w „Podsieci 1”

VLANy skonfigurowane na switchu S1

## Routing między VLANami

Aby umożliwić komunikację między VLAN-ami, zastosowano trunking na kablu łączącym switch S1 z routerem R1. Jest to mechanizm, który pozwala na przesyłanie ruchu należącego do różnych VLAN-ów przez jeden wspólny interfejs, przy jednoczesnym oznaczaniu pakietów odpowiednimi tagami VLAN (przy użyciu standardu IEEE 802.1Q).

**🔁 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).

# Potencjalne zagrożenia mogące wystąpić w stworzonej sieci

# Wnioski