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

W projekcie zdecydowaliśmy się na implementację dynamicznego protokołu routingu OSPF (ang. *Open Shortest Path First*), który jest protokołem typu *link-state*. OSPF działa poprzez wymianę informacji o topologii sieci między routerami, co pozwala na dynamiczne obliczanie najkrótszych ścieżek do poszczególnych podsieci. Dzięki temu sieć jest w stanie automatycznie dostosowywać się do zmian, takich jak awarie łączy czy dodawanie nowych urządzeń.

Protokół OSPF został wdrożony na wszystkich routerach w sieci (R0, R1, R2, R3, R4), a każdy z nich został skonfigurowany z unikalnym *router-ID*. Wszystkie sieci zostały przypisane do obszaru 0 (backbone), co zapewnia spójność routingu w całej infrastrukturze. Przykładowa konfiguracja na routerze R0 obejmuje:

* Definicję procesu OSPF z identyfikatorem 1.
* Przypisanie interfejsów do obszaru 0 za pomocą polecenia network.
* Ustawienie statycznego *router-ID* dla lepszej czytelności.

Konfiguracja protokołu OSPF na routerze R0

Głównym powodem wyboru OSPF zamiast EIGRP była jego otwartość (EIGRP to protokół własnościowy Cisco) oraz lepsza skalowalność w większych sieciach. Dodatkowo OSPF zapewnia szybszą zbieżność w przypadku zmian topologii i lepszą kontrolę nad przepływem ruchu dzięki podziałowi na obszary.

**Dlaczego OSPF:**

* W pełni dynamiczny.
* Obsługuje zmienność tras i priorytetowanie.
* Automatycznie aktualizuje routing po zmianach w topologii.
* Można podzielić sieć na obszary (areas), w naszym przypadku jest to jeden duży obszar 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

Aby zapewnić bezpieczeństwo działania protokołu DHCP, wdrożyliśmy mechanizm **DHCP snooping** na przełączniku S0 w „Podsieci 1”. Jego głównym zadaniem jest ochrona przed atakami, takimi jak **fałszywe serwery DHCP (DHCP spoofing)** czy **flooding DHCP**, które mogą prowadzić do nieautoryzowanego przydzielania adresów IP lub przerw w działaniu sieci.

Konfiguracja zabezpieczeń obejmowała następujące kroki:

1. **Włączenie DHCP snooping globalnie** na przełączniku (ip dhcp snooping).
2. **Aktywacja DHCP snooping dla VLAN 1** (ip dhcp snooping vlan 1), który jest używany w naszej podsieci.
3. **Oznaczenie portu FastEthernet0/3 jako zaufanego** (ip dhcp snooping trust), ponieważ jest on bezpośrednio podłączony do legalnego serwera DHCP (Server0).
4. **Ograniczenie liczby pakietów DHCP** na portach niezaufanych (np. FastEthernet0/1, FastEthernet0/2, FastEthernet0/4) do 5 na sekundę (ip dhcp snooping limit rate 5), co zapobiega próbom przeciążenia sieci.

Konfiguracja zabezpieczeń DHCP na switchu S0

W efekcietylko **Server0** może przydzielać adresy IP, a komputery (PC0, PC1) otrzymują wyłącznie jego oferty, a próby uruchomienia fałszywego serwera DHCP (np. na PC2) są automatycznie blokowane, ponieważ przełącznik odrzuca pakiety DHCP OFFER/DISCOVER z niezaufanych portów. Dzięki tym zabezpieczeniom sieć jest odporna na próby manipulacji protokołem DHCP, a użytkownicy mają gwarancję, że korzystają wyłącznie z autoryzowanych zasobów.

# 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

Implementacja poziomów dostępowych zwiększa **bezpieczeństwo zarządzania siecią**, ograniczając ryzyko przypadkowych lub celowych zmian konfiguracji przez nieuprawniony personel.

W projekcie zaimplementowaliśmy **hierarchię poziomów dostępowych** na urządzeniach sieciowych, aby zapewnić kontrolowany dostęp do funkcji konfiguracyjnych w zależności od uprawnień użytkownika. Na routerze **R0** i switchu **S0** zostały zdefiniowane trzy poziomy dostępu:

1. **Poziom 15 (admin)** – pełne uprawnienia konfiguracyjne
2. **Poziom 10 (technik)** – dostęp do podstawowych poleceń diagnostycznych
3. **Poziom 5 (junior)** – ograniczony dostęp tylko do wybranych komend

Na routerze **R0** poziomy dostępowe są skonfigurowane, ale domyślnie nieużywane, ponieważ autoryzacja odbywa się przez **serwer TACACS+ (Server0)** z „Podsieci 1”. W przypadku awarii serwera TACACS+, router automatycznie przejdzie na uwierzytelnianie lokalne.

Na switchu **S0** (również „Podsieć 1”) wykorzystywane jest wyłącznie **uwierzytelnianie lokalne**, dlatego zdefiniowane konta (admin, technik, junior) są aktywnie używane. Poziomy uprawnień są również egzekwowane podczas logowania przez **SSH**.

Użytkownik **junior** (poziom 5) na S0 może wykonać tylko podstawowe polecenia (np. ping, show ip interface brief).

Prezentacja poziomu uprawnień użytkownika „junior”

Użytkownik **technik** (poziom 10) ma dodatkowo dostęp do diagnostyki (np. show interfaces).

Prezentacja poziomu uprawnień użytkownika „technik”

Próba wykonania niedozwolonych komend (np. configure terminal przez użytkownika junior) kończy się błędem.

# 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

W projekcie wdrożyliśmy mechanizm **Port Security** na przełącznikach, aby zabezpieczyć sieć przed najczęstszymi atakami warstwy drugiej, takimi jak **MAC Flooding** (przepełnienie tablicy CAM) czy **MAC Spoofing** (podszywanie się pod adresy MAC). Głównym narzędziem ochrony była funkcja **Port Security**, skonfigurowana na portach dostępowych przełącznika S0 w „Podsieci 1”

**Kluczowe elementy konfiguracji:**

1. **Ograniczenie liczby adresów MAC** – na portach dostępowych (np. FastEthernet0/2, FastEthernet0/4) ustawiono maksymalnie **1 adres MAC** na port (switchport port-security maximum 1).
2. **Tryb reakcji na naruszenie** – wybrano opcję restrict, która **loguje naruszenie**, ale nie wyłącza portu (switchport port-security violation restrict). W środowisku produkcyjnym można rozważyć tryb shutdown dla większej ochrony.
3. **Dynamiczne uczenie adresów MAC** – użyto polecenia switchport port-security mac-address sticky, aby przełącznik automatycznie zapamiętał pierwszy wykryty adres MAC i traktował go jako dozwolony.

W rezultacie próba podłączenia huba lub urządzenia generującego wiele adresów MAC skończy się zablokowaniem nieautoryzowanych adresów. Dodatkowo, gdy atakujący spróbuje zmienić swój adres MAC na inny, port pozostanie aktywny, lecz ruch zostanie zablokowany (zgodnie z zasadą restrict). Tylko host z zapisanym adresem MAC może komunikować się przez port.

Implementacja zabezpieczeń przed atakami MAC na switchu S0

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Weryfikacja działania zabezpieczeń na urządzeniu

# Listy kontroli ACL wewnątrz zabezpieczonej sieci

Listy kontroli dostępu (ACL, ang. Access Control Lists) to mechanizm stosowany w sieciach komputerowych w celu definiowania reguł dostępu do zasobów i filtrowania ruchu sieciowego. ACL pozwalają określać, jakie typy ruchu są dozwolone, a jakie powinny zostać zablokowane, na podstawie takich parametrów jak adresy IP, protokoły czy porty. Domyślnie na końcu każdej listy ACL znajduje się niejawna reguła "deny any", która odrzuca cały niezgodny z wcześniejszymi zapisami ruch. Wyróżniamy zarówno listy standardowe jak i rozszerzone.

## Standardowe ACL

Standardowe listy kontroli dostępu (ACL) to mechanizmy filtrowania ruchu sieciowego działające w warstwie trzeciej modelu OSI, które pozwalają na kontrolę przepływu pakietów na podstawie źródłowych adresów IP. W przeciwieństwie do list rozszerzonych, standardowe ACL nie analizują protokołów, portów ani adresów docelowych - skupiają się wyłącznie na źródle transmisji.

W projekcie zastosowaliśmy dwie standardowe listy kontroli dostępu (ACL), które zostały umieszczone w „Podsieci 2” na urządzeniu router R3.

**Konfiguracja ACL obejmowała:**

* **ACL 10** - blokuje cały ruch przychodzący z hosta PC2 (192.168.10.2) do routera R3. Została zastosowana na interfejsie GigabitEthernet0/0 w kierunku wejściowym (in).

***Efekt:*** PC2 nie może komunikować się z R3 (np. ping 192.168.10.1), podczas gdy inne hosty w podsieci 192.168.10.0/24 nie mają ograniczeń.

* **ACL 20** - blokuje ruch wychodzący z routera R3 do hosta PC3 (192.168.20.3). Została przypisana do interfejsu GigabitEthernet0/1 w kierunku wyjściowym (out).

***Efekt:*** R3 nie może wysyłać pakietów do PC3, ale inne hosty (np. PC4) w podsieci 192.168.20.0/24 działają normalnie.

Ustawianie standardowych list kontrolnych ACL dla routera R3

Próba **pingowania R3 (192.168.10.1) z PC2** zakończyła się niepowodzeniem (ACL 10 działa).

Test listy ACL 10

**Ping do PC3 z R3** (lub innej podsieci) został zablokowany (ACL 20 działa).

Test listy ACL 20

## Rozszerzone ACL

Rozszerzone listy kontroli dostępu (ACL) stanowią bardziej zaawansowaną formę filtrowania ruchu sieciowego, działającą w warstwach 3 i 4 modelu OSI. W przeciwieństwie do standardowych ACL, rozszerzone listy umożliwiają filtrację na podstawie: adresów źródłowych i docelowych, protokołów warstwy transportowej (np. TCP, UDP), numerów portów, flag TCP (np. established). Pozwalają one na selektywne blokowanie konkretnych usług (np. HTTP, Telnet) z zachowaniem pozostałych funkcji sieci. Dodatkowo należy pamiętać, aby stosować je blisko źródła ruchu (np. na interfejsie wejściowym), aby uniknąć niepotrzebnego obciążenia sieci.

W projekcie wdrożyliśmy dwie rozszerzone listy ACL na routerze R4 w „Podsieci 3”.

**Konfiguracja ACL obejmowała:**

* **ACL 110** – blokuje ruch HTTP (port 80) z hosta PC4 (193.168.10.4) w kierunku „świata” (np. do routera R0). Zastosowano ją na interfejsie GigabitEthernet0/0 w kierunku wejściowym (in).

***Efekt:*** PC4 nie może przeglądać stron WWW (HTTP), ale inne usługi (ping, SSH) działają normalnie.

* **ACL 120** – blokuje połączenia Telnet (port 23) z hosta PC5 (193.168.20.5) do innych urządzeń w tej samej podsieci (193.168.20.0/24). Zastosowano ją na interfejsie GigabitEthernet0/1 w kierunku wejściowym (in).

***Efekt:*** PC5 nie może nawiązać połączenia Telnet z żadnym hostem w swojej podsieci, ale komunikacja z innymi protokołami (np. ping) pozostaje aktywna.

Ustawianie rozszerzonych list kontrolnych ACL dla routera R4

Próba otwarcia strony internetowej (HTTP) na urządzeniu PC4 zakończyła się błędem – ruch został zablokowany (ACL 110).

Test listy ACL 120

Próba połączenia Telnet z urządzenia PC5 z hostem 193.168.20.X (np. S4) nie powiodła się (ACL 120), podczas gdy ping działał poprawnie.

Test listy ACL 120

# Zabezpieczenia przed atakami STP

W celu zapewnienia stabilności i bezpieczeństwa działania protokołu **STP (Spanning Tree Protocol)** w „Podsieci 4”, przeprowadzono konfigurację urządzeń, definiując główne węzły drzewa oraz implementując mechanizmy ochrony przed atakami, które mogłyby prowadzić do przejęcia kontroli nad topologią sieci lub stworzenia pętli komunikacyjnych.

**Główne zabezpieczenia obejmują:**

1. **Ustalenie root bridge** – Przełącznik **Central** został skonfigurowany jako **główny most STP** (spanning-tree vlan 1 root primary), a **S5** jako zapasowy (spanning-tree vlan 1 root secondary), co zapewnia kontrolę nad wyborem ścieżek w sieci. W ten sposób zapewniliśmy celową redundancję, która zapewnia poprawność działania sieci nawet w przypadku awarii głównego urządzenia.

Konfiguracja urządzenia switch Central jako głównego węzła drzewa (root-primary)

Konfiguracja urządzenia switch S5 jako drugorzędnego węzła drzewa (root-secondary)

1. **Ochrona przed nieautoryzowanymi root bridge** – Na przełącznikach **S7** i **S8** włączono funkcję **BPDU Guard** na portach dostępowych (spanning-tree bpduguard enable), co blokuje próby podłączenia nieautoryzowanych urządzeń mogących przejąć rolę root bridge.

Konfiguracja BPDU Guard na urządzeniu switch S7

Konfiguracja BPDU Guard na urządzeniu switch S8

1. **Ochrona przed fałszywymi BPDU** – Porty trunkowe między przełącznikami dystrybucyjnymi (**S5** i **S6**) zostały zabezpieczone funkcją **Root Guard** (spanning-tree guard root), która uniemożliwia zmianę root bridge przez atakującego.

Konfiguracja Root Guard na urządzeniu switch S5

Konfiguracja Root Guard na urządzeniu switch S6

1. **Przyspieszenie konwergencji** – Porty podłączone do hostów (**S7** i **S8**) skonfigurowano w trybie **PortFast** (spanning-tree portfast), aby uniknąć niepotrzebnych opóźnień, przy jednoczesnym włączeniu **BPDU Guard** dla ochrony. . PortFast pozwala na szybkie przełączanie portów do stanu przekazywania (forwarding), co jest szczególnie przydatne na portach końcowych.

Konfiguracja PortFast na urządzeniu switch S7

Konfiguracja PortFast na urządzeniu switch S8

W rezultacie próba **podłączenia nieautoryzowanego przełącznika** do portu z włączonym BPDU Guard spowoduje natychmiastowe wyłączenie portu, a atak **fałszywymi ramkami BPDU** nie może zmienić root bridge dzięki Root Guard na portach między **S5** a **S6**.

Dzięki tym zabezpieczeniom sieć jest odporna na ataki typu **STP Hijacking** lub **STP Reconnaissance**, a stabilność topologii jest zachowana.

# Konfiguracja FHRP

**FHRP (First Hop Redundancy Protocol)** to grupa protokołów (takich jak HSRP, VRRP czy GLBP) zapewniających nadmiarowość bramy domyślnej w sieci LAN. Ich głównym zadaniem jest utrzymanie ciągłości połączenia nawet w przypadku awarii głównego routera, poprzez automatyczne przejęcie jego funkcji przez urządzenie zapasowe. W naszym projekcie wykorzystaliśmy **HSRP (Hot Standby Router Protocol)** - rozwiązanie Cisco, które tworzy wirtualną bramę dostępną dla wszystkich hostów w podsieci.

Wdrożyliśmy protokół **HSRP w wersji 2** na routerach **R1** i **R2**, aby zapewnić redundantność bramy domyślnej dla hostów w „Podsieci 5”. Dzięki temu w przypadku awarii jednego z routerów ruch jest automatycznie przekierowywany przez drugie urządzenie, co zapewnia ciągłość działania sieci.

**Kluczowe elementy konfiguracji:**

1. **Router R1** został skonfigurowany jako **aktywny (active)** dla grupy HSRP 1 z priorytetem **150** (domyślnie 100), co gwarantuje, że to właśnie on będzie domyślną bramą dla hostów (PC10, PC11). Dodatkowo włączono opcję **preempt**, aby R1 automatycznie przejmował rolę aktywnego routera po powrocie do sprawności:

Konfiguracja HSRP na routerze R1

1. **Router R2** pełni rolę **zapasowego (standby)** dla tej samej grupy HSRP. Jego priorytet pozostawiono domyślny (100):

Konfiguracja HSRP na routerze 21

1. **Hosty (PC10, PC11)** oraz **switche (S9, S10)** zostały skonfigurowane z wirtualnym adresem bramy (**195.168.1.254**), który jest wspólny dla obu routerów.

Konfiguracja wirtualnej bramy domyślnej na switchu S10

Konfiguracja wirtualnej bramy domyślnej na urządzeniu PC11

Podczas normalnej pracy ruch z hostów przechodzi przez **R1**, ale w razie awarii R1 (np. wyłączenie interfejsu Gig0/1) ruch zostanie automatycznie przejęty przez **R2**. Po ponownym włączeniu interfejsu, R1 odzyska rolę aktywnego rutera dzięki **preempt**.

Komenda show standby na routerze R1

Weryfikacja działania HSRP na routerze R1

Komenda show standby na routerze R2

Weryfikacja działania HSRP na routerze R2

Komenda show standby na routerze R2

Weryfikacja działania HSRP na routerze R2 po wyłączeniu interfejsu Gig0/1

# EtherChannel

show etherchannel summary

# VLANy

W ramach „Podsieci 7” zaimplementowaliśmy trzy **VLAN-y (Virtual Local Area Networks)**: **VLAN 10**, **VLAN 20** oraz **VLAN 30**. Pozwoliło nam to na logiczne podzielenie fizycznej sieci na odseparowane segmenty. Każdy z VLAN-ów został przypisany do określonych portów przełącznika **S14**, a następnie do odpowiednich komputerów (np. PC6 i PC7 dla VLAN 10, PC8 i PC9 dla VLAN 20). Dzięki takiemu rozwiązaniu urządzenia należące do różnych VLAN-ów mogą współdzielić tę samą infrastrukturę fizyczną, zachowując przy tym pełną izolację ruchu sieciowego. VLAN-y zwiększają również bezpieczeństwo sieci, ograniczając możliwość niekontrolowanego rozprzestrzeniania się ruchu (np. w przypadku ataków typu **broadcast storm**). W naszym projekcie sieci do każdego z VLANów przypisano po dwa komputery PC.

Przypisanie portów switcha S14 do odpowiednich VLAN-ów

VLANy skonfigurowane na switchu S1

## Routing między VLANami

Aby umożliwić komunikację między VLAN-ami, skonfigurowaliśmy **interfejsy podrzędne (subinterfaces)** na routerze **R0**, które działają jako wirtualne bramy dla każdego VLAN-u. Każdy interfejs podrzędny (np. GigabitEthernet0/1.10 dla VLAN 10) został oznaczony tagiem odpowiedniego VLAN-u (encapsulation dot1Q) i otrzymał unikalny adres IP (np. 197.168.1.1/24 dla VLAN 10). Na przełączniku **S14** port podłączony do routera (np. FastEthernet0/1) został skonfigurowany jako **trunk**, co pozwala na przesyłanie ruchu wszystkich VLAN-ów przez jedno fizyczne łącze. Dzięki temu komputery z różnych VLAN-ów mogą się komunikować, zachowując przy tym zasadę separacji ruchu.

Konfiguracja interfejsów podrzędnych na routerze R0

Konfiguracja portu trunk na switchu S14

## Zabezpieczenia przed atakami VLANami

W projekcie wdrożyliśmy kilka mechanizmów chroniących przed atakami na VLAN-y:

1. **Ochrona przed VLAN Hopping**:
   * Wyłączyliśmy **autonegocjację trunków** na portach dostępowych (switchport nonegotiate), aby uniknąć przypadkowego przełączenia portu w tryb trunk przez atakującego.
   * Wszystkie porty dostępowe zostały jawnie ustawione w trybie access (switchport mode access).

Konfiguracja ochrony przed VLAN Hooping na Switchu S14

1. **Zabezpieczenie nieużywanych portów**:
   * Nieużywane porty (np. Fa0/8-24 na S14) zostały przypisane do **VLAN-u 999** (izolowanego) i **wyłączone** (shutdown), aby uniemożliwić ich wykorzystanie do ataków.

Zabezpieczenie nieużywanych portów na Switchu S14

1. **Ochrona przed nieautoryzowanym dostępem**:
   * Włączono **Port Security** na portach dostępowych, aby ograniczyć liczbę dozwolonych adresów MAC.
   * Użyto polecenia switchport port-security mac-address sticky, aby przełącznik dynamicznie uczył się adresów MAC i blokował nieznane urządzenia.

Konfiguracja ochrony przed nieautoryzowanym dostępem na Switchu S14

W rezultacie próba podłączenia nieautoryzowanego urządzenia do portu dostępowego zakończy się zablokowaniem ruchu (Port Security), a atak VLAN Hopping (np. przez wysyłanie fałszywych ramek 802.1Q) stanie się niemożliwy dzięki wyłączeniu negocjacji trunków.

# Potencjalne zagrożenia mogące wystąpić w stworzonej sieci

# Wnioski