



Politechnika Świętokrzyska
Wydział Elektrotechniki, Automatyki i Informatyki

Bezpieczeństwo infrastruktury sieciowej

Przychodnia

Wykonał: Kacper Wojniak, Wiktor
Bednarek

Kierunek:
Cyberbezpieczeństwo

Kielce 2023,

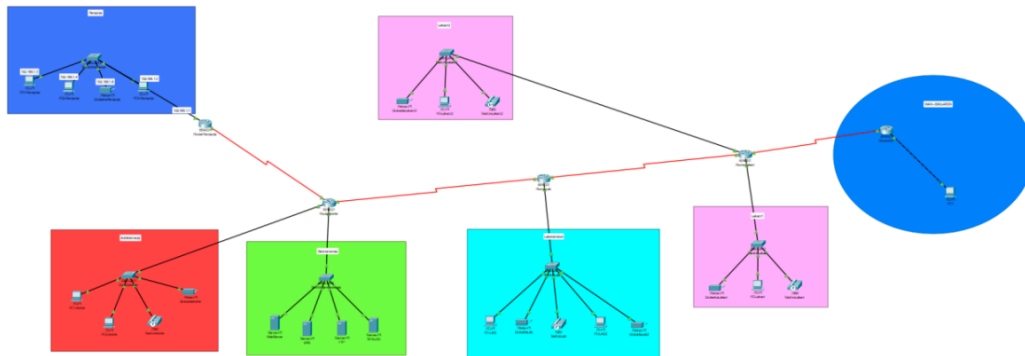
Spis treści

1. Cel projektu.....	3
2. Sieć.....	3
3. Zabezpieczenia.....	12
4. Podsumowanie	14

1. Cel projektu

Celem projektu jest stworzenie i zaprojektowanie sieci przychodni, która będzie posiadała zabezpieczenia przed atakami.

2. Sieć



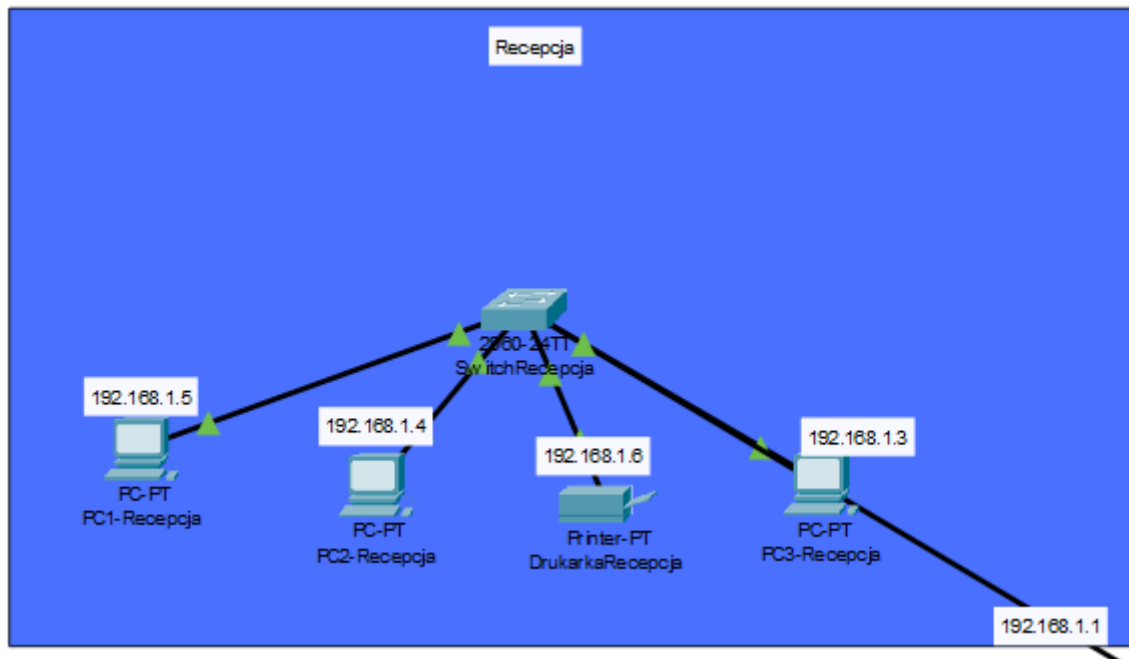
Rys. 2.1 Sieć główna

Powyższe zdjęcie przedstawia sieć główną przychodni. Sieć będzie składała się z 7 obszarów. Sieć będzie posiadała zabezpieczenia.

Obszary sieci:

- Recepcja
- Administracja
- Serwerownia
- Laboratorium
- Lekarz 1
- Lekarz 2
- WAN - EMULATION

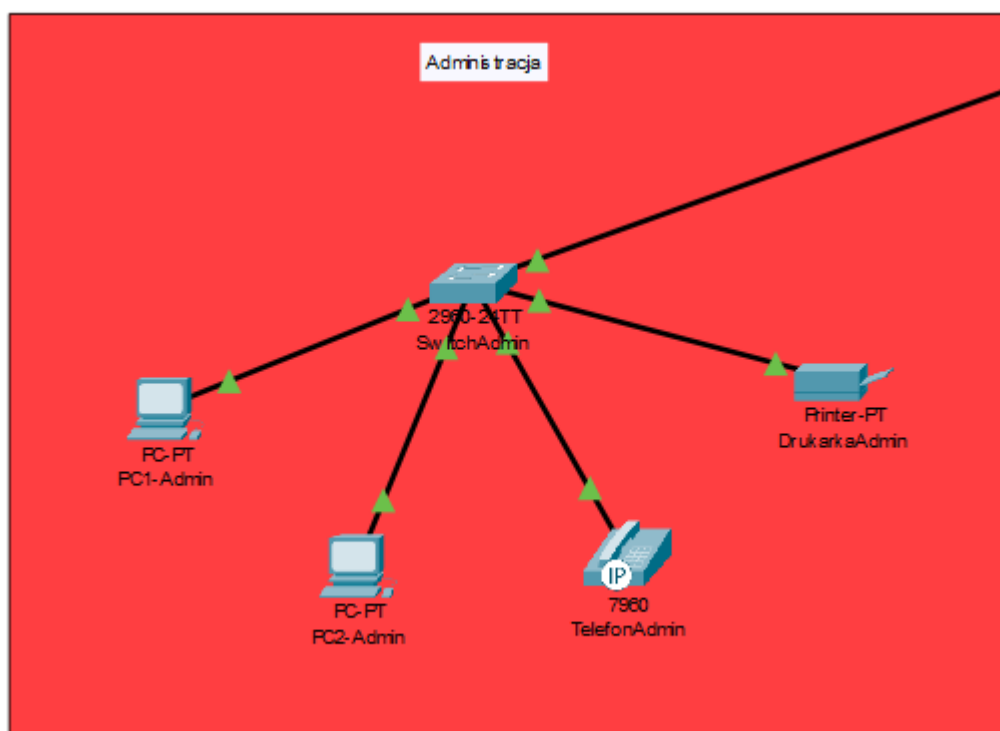
Recepcja:



W obszar recepcji wchodzi trzy komputery oraz drukarka. Wszystkie urządzenia podłączone są do switcha.

Recepcja	
PC1-Recepcja	192.168.1.5
PC2-Recepcja	192.168.1.4
PC3-Recepcja	192.168.1.3
Drukarka Recepcja	192.168.1.6

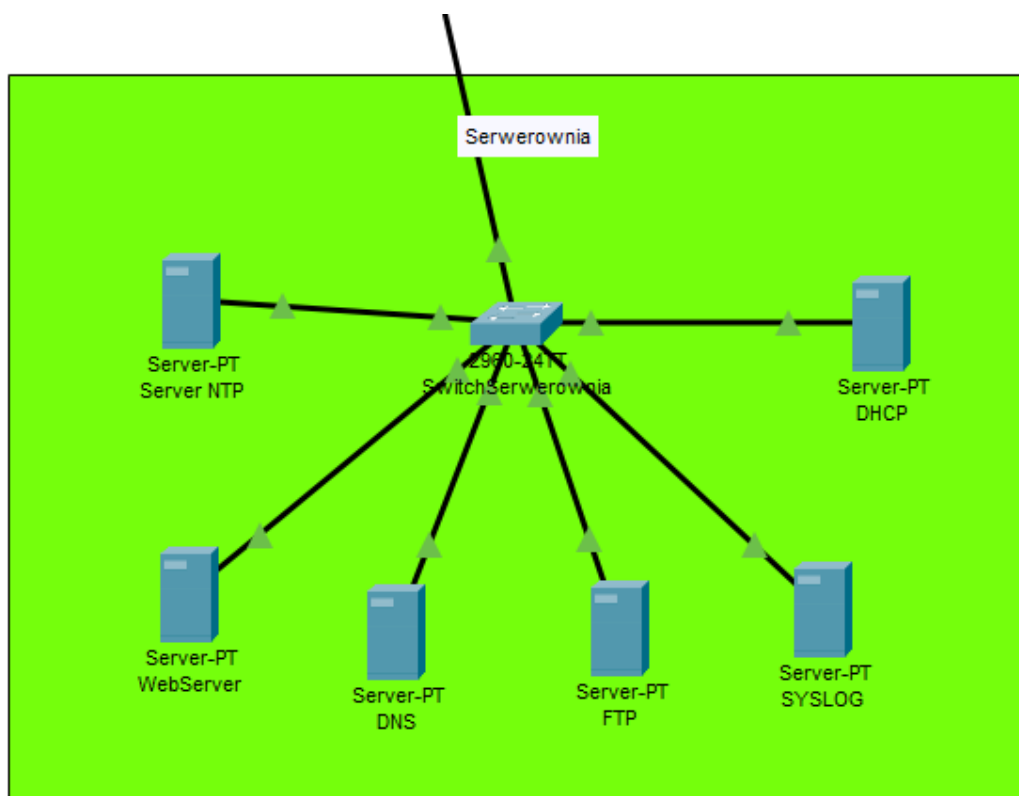
Administracja:



W obszar administracji wchodzi dwa komputery drukarka oraz telefon. Wszystkie urządzenia podłączone są do switcha.

Administracja	
PC1-Admin	192.168.2.3
PC2-Admin	192.168.2.2
TelefonAdmin	-
Drukarka Admin	192.168.2.5

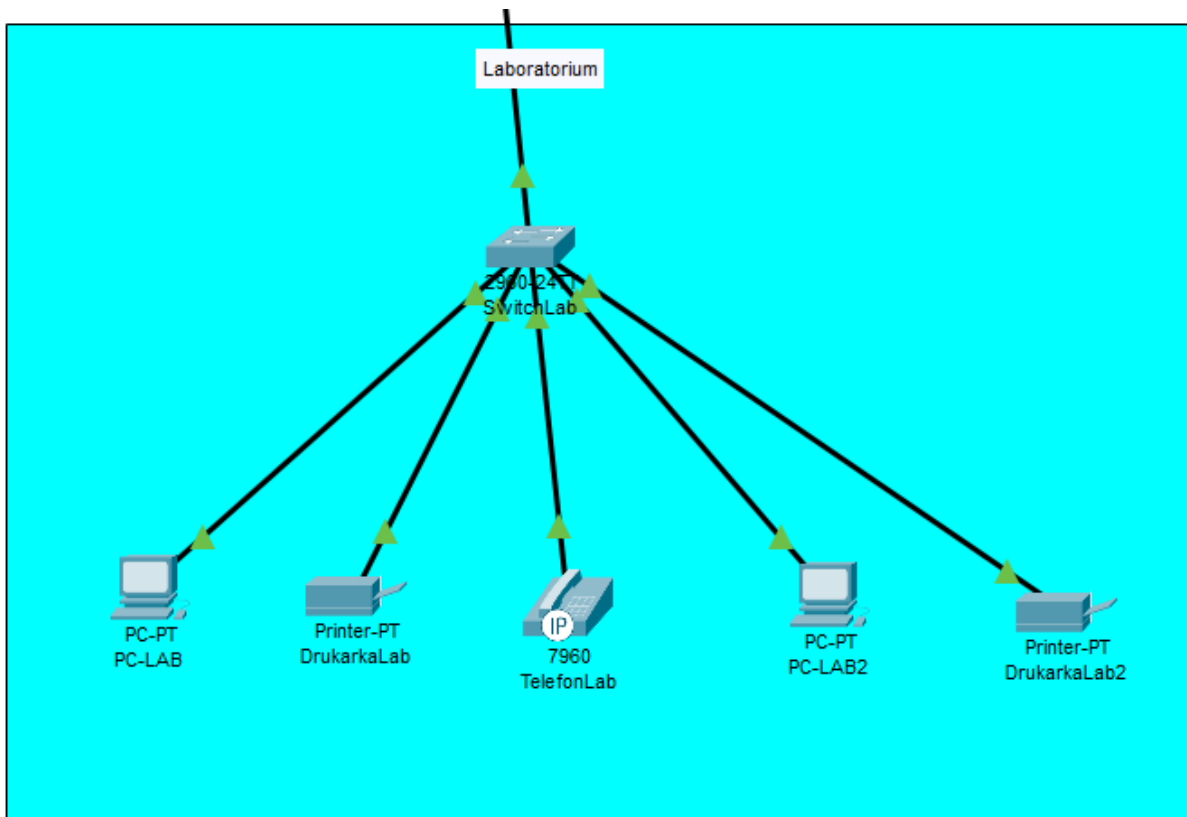
Serwerownia:



W obszar serwerowni wchodzi cztery serwery. Wszystkie urządzenia podłączone są do switcha.

Serwerownia	
WebServer	192.168.6.7
DNS	192.168.6.8
FTP	192.168.6.2
SYSLOG	192.168.6.3
DHCP	192.168.6.6
NTP	192.168.6.10

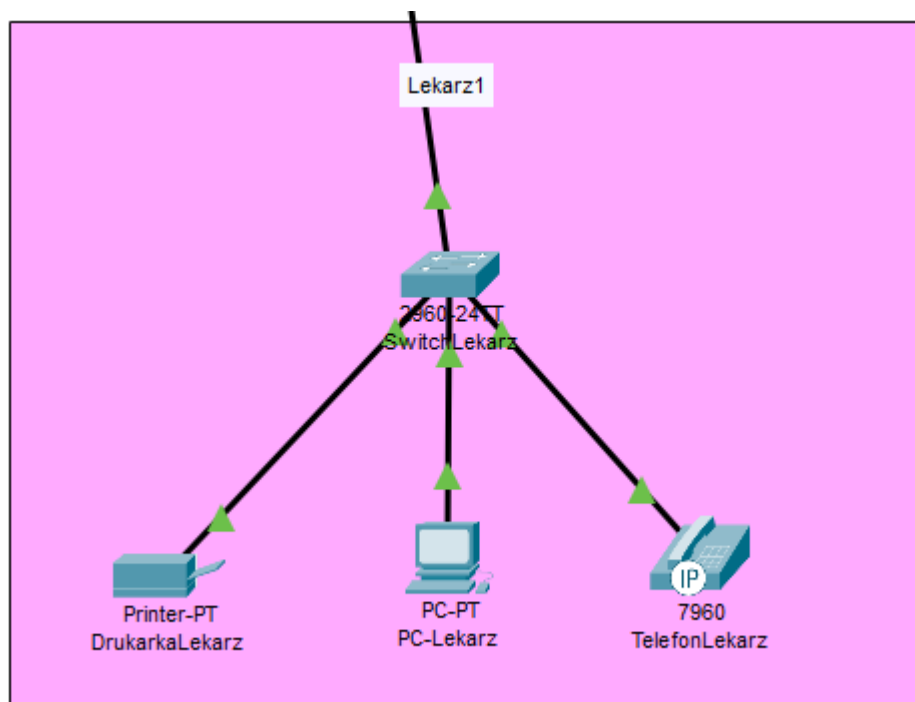
Laboratorium:



W obszar laboratorium wchodzi dwa komputery, dwie drukarki oraz telefon. Wszystkie urządzenia podłączone są do switcha.

Laboratorium	
PC-LAB	192.168.3.2
DrukarkaLab	192.168.3.3
TelefonLab	-
PC-LAB2	192.168.3.1
DrukarkaLab2	192.168.3.4

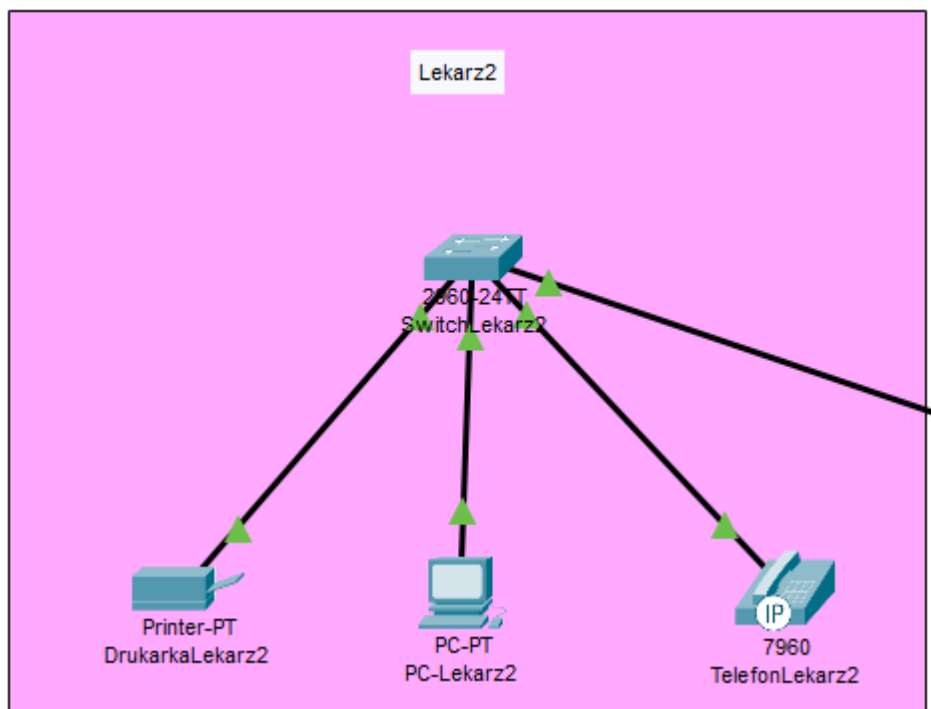
Lekarz1:



W obszar lekarz1 wchodzi drukarka, telefon oraz komputer. Wszystkie urządzenia podłączone są do switcha.

Lekarz1	
PC-Lekarz	192.168.4.3
DrukarkaLekarz	192.168.4.2
TelefonLekarz	-

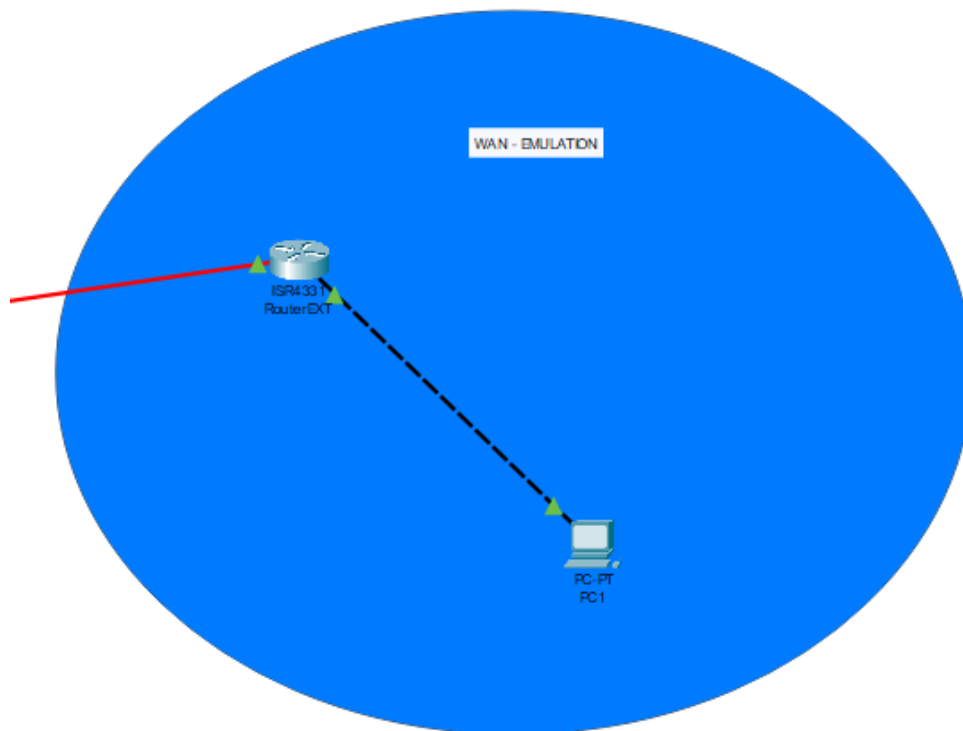
Lekarz2:



W obszar lekarz2 wchodzi drukarka, telefon oraz komputer. Wszystkie urządzenia podłączone są do switcha.

Lekarz2	
PC-Lekarz2	192.168.5.1
DrukarkaLekarz2	192.168.5.3
TelefonLekarz2	-

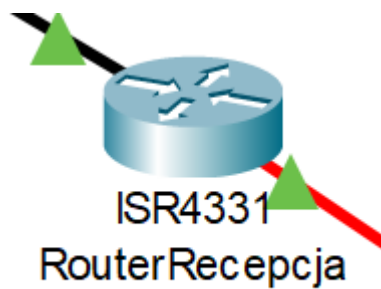
WAN – EMULATION:



W obszar wan-emulation wchodzi komputer oraz ruter.

WAN – EMULATION	
PC1	192.168.7.1
RouterEXT	192.168.7.2

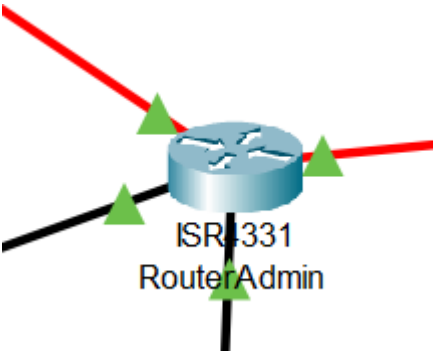
RouterRecepcja:



RouterRecepcja

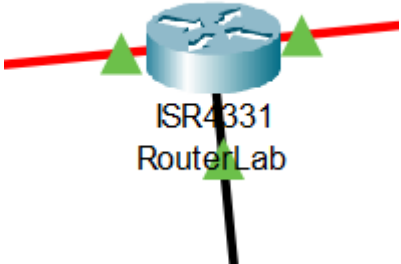
RouterRecepcja	192.168.1.1
----------------	-------------

RouterAdmin:



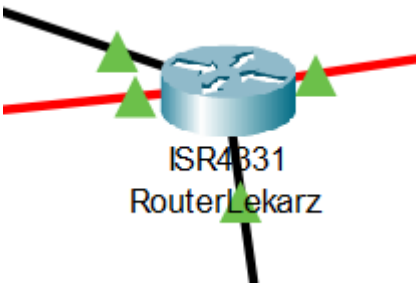
RouterAdmin	
RouterAdmin	192.168.2.1

RouterLab:



RouterLab	
RouterLab	192.168.3.1

RouterLekarz:



RouterLekarz	
RouterLekarz	192.168.4.1

3. Zabezpieczenia

IPS, czyli System Zapobiegania Włamaniom, to rodzaj rozwiązania bezpieczeństwa sieciowego, które ma na celu wykrywanie i blokowanie nieautoryzowanego dostępu, ataków sieciowych oraz innych form naruszeń bezpieczeństwa w sieci.

Działanie IPS polega na analizie ruchu sieciowego w czasie rzeczywistym w celu identyfikacji potencjalnych zagrożeń i podejrzanych aktywności. Istnieje kilka różnych metod wykrywania i prewencji stosowanych przez różne systemy IPS, ale ogólnie działają one na podobnych zasadach.

IPS w naszym przypadku został umieszczony na ruterze EXT, przez którego przechodzi zewnętrzne połączenie.

ACL (Access Control List) to lista kontroli dostępu, która jest wykorzystywana w sieciach komputerowych i systemach operacyjnych do zarządzania uprawnieniami użytkowników oraz kontrolowania dostępu do zasobów sieciowych.

Działanie listy ACL polega na definiowaniu reguł, które określają, które połączenia sieciowe lub operacje są dozwolone, a które są blokowane. Lista ACL może być stosowana na różnych warstwach sieci, takich jak warstwa 2 (MAC), warstwa 3 (IP) i warstwa 4 (porty).

Każda reguła w liście ACL składa się z dwóch podstawowych elementów:

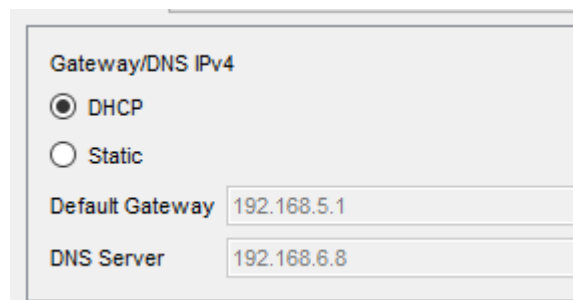
- Adres źródłowy lub identyfikator użytkownika: Określa, skąd pochodzi dane połączenie lub które konto użytkownika jest uwzględnione w regule. Może to być adres IP, adres MAC, numer portu lub inna informacja identyfikująca źródło.
- Adres docelowy lub typ operacji: Określa, jaki jest docelowy adres IP, adres MAC, numer portu lub rodzaj operacji, na której reguła jest stosowana. Może to być adres IP, adres MAC, numer portu lub inna informacja identyfikująca cel.

ACL w naszym przypadku został użyty na wszystkich ruterach, gdzie przykładowo administracja może wysłać wiadomość do wszystkich urządzeń a pozostałe obszary nie mogą tylko widzieć własne urządzenia.

```
R2#
R2#show access-lists
Standard IP access list 1
  10 permit any (4 match(es))
```

Dodatkowo zastosowaliśmy **Serwer DNS**, odpowiedzialna za przekształcanie nazw domenowych, takich jak WebServer, na adresy IP, które są potrzebne do nawiązania połączenia z danym serwerem. Działanie serwera DNS opiera się na hierarchicznej strukturze domen i procesie rozwiązywania nazw.

Serwer DHCP jest odpowiedzialny za przydzielanie dynamicznych adresów IP i konfigurację sieci dla urządzeń w sieci komputerowej.



Gateway/DNS IPv4

☒ DHCP

☐ Static

Default Gateway 192.168.5.1

DNS Server 192.168.6.8

SPAN monitoruje ruch sieciowy. Pozwala na przechwytywanie pakietów danych przesyłanych między dwoma urządzeniami w sieci i przekierowywanie ich do specjalnie skonfigurowanego portu na przełączniku. Dzięki temu administrator sieci może analizować i monitorować ruch sieciowy w celu diagnostyki, rozwiązywania problemów, monitorowania wydajności oraz analizowania zachowań w sieci.

Serwer NTP (Network Time Protocol) to specjalizowany serwer komputerowy, który zapewnia synchronizację czasu na sieci komputerowej lub w systemach rozproszonych. Jego głównym zadaniem jest dostarczanie dokładnego czasu referencyjnego dla innych urządzeń w sieci.

Dodatkowo serwery NTP korzystają z algorytmów i protokołów komunikacyjnych, aby zapewnić dokładną synchronizację czasu na wszystkich podłączonych urządzeniach. Działają one na zasadzie klient-serwer, gdzie serwer NTP dostarcza informacje o aktualnym czasie, a klient NTP synchronizuje swój czas z serwerem.

```

R2#show clock
17:25:59.688 UTC Wed Jul 5 2023
R2#show clock
17:26:33.648 UTC Wed Jul 5 2023
R2#show clock
17:26:35.330 UTC Wed Jul 5 2023
R2#show clock de
R2#show clock detail
17:26:39.550 UTC Wed Jul 5 2023
Time source is NTP
R2#show clock detail
17:27:50.949 UTC Wed Jul 5 2023
Time source is NTP

```

VLAN (Virtual Local Area Network) to technologia stosowana w sieciach komputerowych, która umożliwia podział jednej fizycznej sieci lokalnej (LAN) na logiczne, odrębne grupy. Dzięki VLANom można segregować ruch między różnymi segmentami sieci, nawet jeśli fizycznie są one połączone tym samym sprzętem sieciowym.

```
SR#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10 Recepcja	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

SSH (Secure Shell) to protokół komunikacyjny, który umożliwia bezpieczne zdalne połączenia z innym urządzeniem przez niezaufane sieci. SSH zapewnia szyfrowane połączenie, co oznacza, że dane przesyłane między klientem a serwerem są chronione przed przechwytywaniem lub manipulacją przez potencjalnych atakujących.

SNMP (Simple Network Management Protocol) to protokół używany do monitorowania i zarządzania urządzeniami sieciowymi. SNMP umożliwia administratorom systemów zdalny dostęp do informacji o stanie i wydajności urządzeń sieciowych, takich jak routery, przełączniki, serwery i inne urządzenia sieciowe.

4. Podsumowanie

Sieć ta, spełnia wymagania dotyczące i bezpieczeństwa sieci prywatnej oraz zapewnia również optymalną wydajność podczas korzystania z usług telekomunikacyjnych.

Zainstalowany sprzęt pozwolił na zorganizowanie szybkiego przewodowego i bezprzewodowego dostępu do Internetu na terenie całego obiektu przychodni, jak również zapewniając transfer wszelkiego rodzaju danych.