Politechnika Świętokrzyska Wydział Elektrotechniki Automatyki i Informatyki Bezpieczeństwo Infrastruktury Sieciowej	
Skład zespołu:	Dominik Grudzień Mikołaj Widanka
Grupa:	1ID24B
Temat:	Sieć dla serwisu rowerowego

1. Wstęp

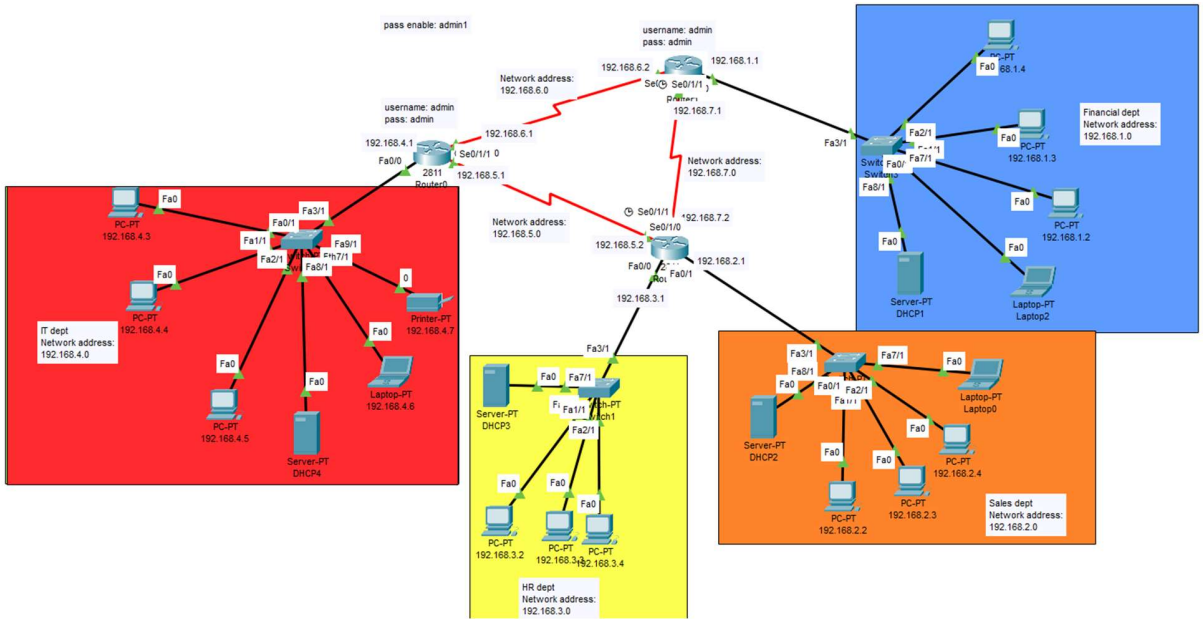
W ramach projektu przy użyciu narzędzia Cisco Packet Tracer, stworzyliśmy sieć obsługującą serwis rowerowy zajmujący się sprzedażą i naprawą rowerów. Przed wykonaniem projektu sporządziliśmy harmonogram prac, według którego przeprowadzaliśmy skalowanie naszej sieci oraz implementację zaplanowanych technologii oraz zabezpieczeń.

Prace nad projektem przebiegały według poniższych wytycznych:

- Dodanie urządzeń w CISCO Packet Tracer
- Połączenie urządzeń i stworzenie wstępnej topologii
- Zabezpieczenie urządzeń (z poziomu konsoli/sprzętu)
- Skonfigurowanie urządzeń w celu zabezpieczenia ich przed atakami (STP, DHCP, VLAN, MAC)
- Skonfigurowanie list dostępu
- Konfiguracja VPN
- Skonfigorwanie AAA, SNMP, NTP, syslog, DHCP
- Konfiguracja sieci VLAN i routingu
- Analiza infrastruktury pod kątem zagrożeń
- Opis wykreowanej infrastruktury

2. Przedstawienie topologii

Stworzona przez nas topologia została zaprezentowana na poniższym schemacie:



Rys. 1 Topologia sieci dla serwisu rowerowego (Widok Packet Tracer)

Analizując powyższy schemat można wyróżnić podstawowe elementy charakterystyczne wykreowanej topologii:

- Podział sieci na mniejsze podsieci symulujący poszczególne działy znajdujące się w firmie (HR, Finanse, IT, Sprzedaż)
- Każda podsieć znajdująca się na poszczególnych piętrach posiada swój numer (tj. 192.168.1.0 – 192.168.4.0)
- Sieci połączone są w topologię przypominającą płatek śniegu gdzie do każdego switcha podłączone zostały podstawowe urządzenia znajdujące się w firmie (komputer PC, serwer, drukarka, laptop)
- Sieci stworzone na poszczególnych piętrach łączą się z internetem poprzez podłączenie urządzeń do switcha a następnie do routerów obsługujących te sieci.
- Każda z sieci posiada swój własny serwer DHCP pozwalający na przydział adresów do urządzeń podłączonych w danej sieci
- Urządzenia sieciowe takie jak routery zostały zabezpieczone przed niepowołanym dostępem za pomocą haseł chroniących dostępu do poszczególnych poziomów uprawnień administratora urządzenia

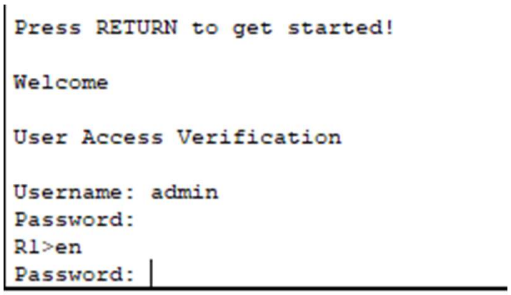
3. Zastosowane technologie

W naszym projekcie wykorzystaliśmy szereg technologii oraz zabezpieczeń dostępnych w programie Packet Tracer:

- Zabezpieczenie urządzeń (z poziomu konsoli/sprzętu)

Rys. 2 Zabezpieczenie routera

Powyższy rysunek przedstawia zastosowane przez nas zabezpieczenia AAA (Authentication, Authorization, Accounting) dotyczące routerów znajdujących się w sieci. Użytkownik witany jest komunikatem, a następnie poproszony o podanie loginu i hasła dostępu do urządzenia.



Rys. 3 Zabezpieczenie trybu enable

Następnie zabezpieczony został również tryb uprawnień *enable* za pomocą drugiego z haseł. Dopiero po wprowadzeniu wszystkich haseł użytkownik otrzymuje dostęp do konfiguracji urządzenia.

W przeciwnym wypadku jeżeli hasła są nieprawidłowe urządzenie zostaje zablokowane po maksymalnej ilości niepoprawnych prób wpisania hasła.

- Zabezpieczenia przed atakami: STP, DHCP, MAC

Atak STP (Spanning Tree Protocol)

W celu obrony przed atakiem wykorzystującym protokół STP będący zagrożeniem w warstwie 2 sieci, wykorzystaliśmy poniższe komendy:

S1(config) # int f0/1 – fx/x

S1(config-if) # spanning-tree portfast

S1(config-if) # spanning-tree bpduguard enable

Komendy *spanning-tree portfast* i *spanning-tree bpduguard enable* pomagają zabezpieczyć sieć przed atakami na protokół Spanning Tree (STP).

- **Spanning-tree PortFast**: Ta funkcja powoduje, że port przełącznika natychmiast przechodzi do stanu przekazywania, pomijając stany nasłuchiwania i nauki. Dzięki temu urządzenia mogą natychmiast połączyć się z siecią. Jednakże, PortFast może być włączony na portach nie-trunkowych łączących dwa przełączniki, co może prowadzić do pętli STP, ponieważ BPDUs nadal są transmitowane i odbierane na tych portach.
- **Spanning-tree BPDU Guard**: Ta funkcja monitoruje, czy na interfejsach, na których jest włączona ta funkcja, nie pojawiają się żadne BPDU. Port zostanie wyłączony (err-disabled), jak tylko zostanie odebrany pierwszy BPDU. Dzięki temu, BPDU Guard zapobiega pętlom, przenosząc port non-trunking do stanu errdisable, gdy na tym porcie odbierany jest BPDU.

Obie te funkcje pomagają zabezpieczyć sieć przed manipulacją protokołem STP, co jest częstym celem ataków typu spoofing. Dzięki temu, sieć jest bardziej odporna na potencjalne ataki i nieautoryzowane zmiany w topologii sieci.

```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     00E0.B01C.2386
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00E0.B01C.2386
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa1/1            Desg FWD 19        128.2    P2p
Fa2/1            Desg FWD 19        128.3    P2p
Fa3/1            Desg FWD 19        128.4    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa7/1            Desg FWD 19        128.8    P2p
```

Rys. 4 Sprawdzenie protokołu STP na aktywnych interfejsach

Atak DHCP

Kolejnym z zabezpieczonych przez nas ataków jest DHCP Snooping.

DHCP Snooping to technologia zabezpieczająca działająca na warstwie 2 modelu OSI, która jest wbudowana w system operacyjny zdolnego przełącznika sieciowego. Technologia ta filtruje nieakceptowalny ruch DHCP i zapobiega oferowaniu adresów IP przez nieautoryzowane (rogue) serwery DHCP.

DHCP Snooping działa jako ochrona przed atakami typu man-in-the-middle. Sam DHCP działa na warstwie 3 modelu OSI, natomiast DHCP Snooping działa na urządzeniach warstwy 2, aby filtrować ruch pochodzący od klientów DHCP3.

W celu zabezpieczenia naszej sieci przed tego typu atakiem skorzystaliśmy z następującej konfiguracji:

Switch(config)#interface fastEthernet 0/1 /przejście do trybu konfiguracji szczegółowej 1 interfejsu przełącznika

Switch(config-if)#ip dhcp snooping trust /oznaczenie portu 1 jako zaufanego dla serwera DHCP

Switch(config-if)#exit /wyjście z trybu konfiguracji szczegółowej 1 interfejsu, do trybu konfiguracji globalnej

Switch(config)#ip dhcp snooping vlan 1 /uruchomienie funkcjonalności DHCP Snooping dla vlan'u pierwszego

Switch(config)#ip dhcp snooping /potwierdzenie uruchomienia funkcjonalności DHCP Snooping

```
S1#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet1/1            no         unlimited
FastEthernet2/1            no         unlimited
Ethernet7/1                no         unlimited
FastEthernet8/1            yes        unlimited
FastEthernet9/1            no         unlimited
```

Rys. 5 Sprawdzenie działania DHCP Snooping

Atak MAC Flooding

MAC flooding to technika ataku na sieci komputerowe, która polega na wysyłaniu dużej liczby ramek Ethernet z fałszywymi adresami MAC do tablicy adresów przełącznika, powodując jej przepełnienie. Gdy tablica adresów MAC jest pełna i nie może zapisać nowych adresów MAC, przełącznik przechodzi w stan tzw. “fail-open mode”, w którym nowe pakiety danych, które otrzymuje, są wysyłane do każdego portu (i urządzenia) w sieci. Atak MAC flooding może narazić wszystkie urządzenia sieciowe na ryzyko i ujawnić wrażliwe dane.

Do zabezpieczenia się przed takimi sytuacjami użyliśmy następującej konfiguracji:

S1# conf t // tryb konfiguracji przełącznika

S1 (config)# interface fastethernet0/1 *// przejście do konfiguracji interfejsu*

S1(config-if)# switchport mode access *// Ta komenda konfiguruje port jako port dostępowy. Porty dostępowe są częścią tylko jednej sieci VLAN i nie tagują ruchu VLAN.*

S1(config-if)# switchport port-security *// Ta komenda włącza funkcję zabezpieczeń portu. Zabezpieczenia portu pozwalają ograniczyć ruch przychodzący do portu, ograniczając adresy MAC, które mogą wysyłać ruch do portu*

S1(config-if)# switchport port-security maximum 1 // Ta komenda ustawia maksymalną liczbę bezpiecznych adresów MAC, które mogą być skonfigurowane na porcie, na 1. Oznacza to, że tylko jedno urządzenie (o określonym adresie MAC) może korzystać z tego portu.

Te komendy pomagają zabezpieczyć sieć przed atakami typu MAC flooding, ograniczając liczbę adresów MAC, które mogą korzystać z danego portu, i umożliwiając wyłączenie portu w przypadku wykrycia naruszenia zasad bezpieczeństwa.

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-----------------------------------------------------------------------
        Fa0/1        1          0                0         Shutdown
        Fa1/1        1          0                0         Shutdown
        Fa2/1        1          0                0         Shutdown
        Fa3/1        1          1                0         Shutdown
        Fa4/1        1          0                0         Shutdown
        Fa5/1        1          0                0         Shutdown
       Eth6/1        1          0                0         Shutdown
        Fa7/1        1          1                0         Shutdown
        Fa8/1        1          0                0         Shutdown
        Fa9/1        1          0                0         Shutdown
-----------------------------------------------------------------------
Switch#show port-security int f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Rys. 6 Sprawdzenie konfiguracji port-security dla przełącznika i wybranego interfejsu

- Skonfigurowanie list dostępu ACL

Listy Kontroli Dostępu (Access Control Lists, ACL) to zestaw reguł służących do kontrolowania ruchu sieciowego i redukcji ataków sieciowych. ACL są używane do filtrowania ruchu na podstawie zdefiniowanych reguł dla ruchu przychodzącego lub wychodzącego z sieci.

ACL mogą określać, które użytkowniki lub procesy systemowe (podmioty) mają dostęp do zasobów (obiektów), a także jakie operacje są dozwolone na danych obiektach. Każda próba dostępu podmiotu do obiektu, która nie ma pasującego wpisu w konfiguracji ACL, zostanie odrzucona.

Główne zastosowania ACL to filtrowanie i klasyfikacja ruchu.

Listy ACL w naszym projekcie konfigurowaliśmy w następujący sposób:

R1(config)# access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255 Ustawienie rozszerzonej listy ACL filtrującej na podstawie zarówno ruchu źródłowego jak i docelowego adresu IP, protokołu (TCP, UDP, ICMP, IGMP itp.) oraz numeru portu.

W tym przypadku filtrowany ruch pomiędzy działem sprzedaży oraz IT jest dozwolony w obu kierunkach.

```
R1#sh access-lists
Extended IP access list 101
    10 permit ip 192.168.4.0 0.0.0.255 192.168.2.0 0.0.0.255
    20 permit ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Rys. 7 Sprawdzenie list ACL dla ruchu pomiędzy departamentami przez router R1

- Konfiguracja VPN

Kolejnym krokiem podczas wykonywania topologii było stworzenie tunelu VPN. W tym celu wykorzystaliśmy dostępne otwarte rozwiązanie Site-to-Site.

Site-to-Site VPN to technologia, która umożliwia połączenie dwóch lub więcej sieci, takich jak sieć korporacyjna i sieć oddziału. Wiele organizacji korzysta z VPN typu Site-to-Site, aby wykorzystać połączenie internetowe do prywatnego ruchu jako alternatywę dla prywatnych obwodów MPLS.

Site-to-Site VPN pomaga w następujących aspektach:

Bezpieczne udostępnianie zasobów:

- Umożliwia bezpieczne udostępnianie zasobów i informacji między pracownikami w różnych lokalizacjach.
- Ochrona danych: Zapewnia bezpieczne połączenie między sieciami, chroniąc dane przed potencjalnymi atakami.
- Zwiększenie wydajności: Umożliwia szybki i niezawodny dostęp do zasobów sieciowych, co zwiększa wydajność i produktywność.
- Oszczędność kosztów: Zamiast korzystać z drogich prywatnych obwodów MPLS, firmy mogą wykorzystać połączenie internetowe do prywatnego ruchu.

Aby skonfigurować taki VPN na jednym z routerów w naszej sieci użyliśmy następującej konfiguracji:

R1(config)# crypto isakmp policy 10: Tworzy politykę ISAKMP (Internet Security Association and Key Management Protocol) o priorytecie 10.

R1(config)# authentication pre-share: Ustala metodę uwierzytelniania na pre-shared key (PSK), co oznacza, że obie strony muszą znać ten sam klucz.

R1(config)# encryption aes 256: Ustala algorytm szyfrowania na AES (Advanced Encryption Standard) z kluczem o długości 256 bitów.

R1(config)# group 2: Określa grupę Diffie-Hellmana do generowania kluczy. Grupa 2 odpowiada 1024-bitowemu kluczowi.

R1(config)# lifetime 86400: Ustala czas życia kluczy na 86400 sekund (24 godziny).

R1(config)# crypto isakmp key cisco address 192.168.5.2: Ustala pre-shared key na “cisco” dla zdalnego hosta o adresie IP 192.168.5.2.

R1(config)# crypto ipsec transform-set TSET esp-aes esp-sha-hmac: Tworzy zestaw transformacji o nazwie “TSET”, który określa, jakie algorytmy są używane do szyfrowania danych (ESP-AES) i uwierzytelniania (ESP-SHA-HMAC).

R1(config)# crypto map CMAP 10 ipsec-isakmp: Tworzy mapę kryptograficzną o nazwie “CMAP” z numerem sekwencyjnym 10, która jest używana do nawiązywania tuneli IPSec.

R1(config)# set peer 192.168.5.2: Określa zdalny host (peer) o adresie IP 192.168.5.2.

R1(config)# match address 101: Określa listę dostępu o numerze 101, która definiuje “interesujący ruch” do szyfrowania.

R1(config)# set transform-set TSET: Przypisuje wcześniej utworzony zestaw transformacji “TSET” do mapy kryptograficznej.

R1(config)# int s0/1/0: Przechodzi do konfiguracji interfejsu Serial 0/1/0.

R1(config)# crypto map CMAP: Przypisuje mapę kryptograficzną “CMAP” do interfejsu.

R1(config)# do write: Zapisuje bieżącą konfigurację do pamięci nieulotnej (NVRAM).

```
R1#sh crypto isakm sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.5.2     192.168.5.1     QM_IDLE           1089    0 ACTIVE
```

Rys. 8 Sprawdzenie statusu jednej ze stron tunelu

```
R1#sh crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: CMAP, local addr 192.168.5.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 192.168.5.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0
```

Rys. 9 Sprawdzenie pakietów przesyłanych przez tunel VPN

- Skonfigurowanie AAA, SNMP, NTP, syslog, DHCP

Metoda AAA

Metoda AAA (Authentication, Authorization, Accounting) to zaawansowany mechanizm zabezpieczający, który umożliwia kontrolę dostępu do urządzeń sieciowych. Nazwa tej metody wywodzi się od trzech słów:

- Authentication (Uwierzytelnienie): sprawdza, czy dany użytkownik jest faktycznie tym, za kogo się podaje.
- Authorization (Autoryzacja): weryfikuje, do jakich zasobów konkretny użytkownik ma dostęp.
- Accounting (Raportowanie): zbiera informacje – logi o czynnościach, jakie wykonał użytkownik.

Metoda AAA może wykorzystywać lokalną bazę użytkowników, którą utworzoną mamy na urządzeniu, ale także bazy użytkowników zapisane na serwerach logowania, które stosują protokoły uwierzytelniania takie jak RADIUS lub też TACACS.

Dzięki metodzie AAA, można skutecznie zarządzać dostępem do sieci i zasobów sieciowych, co pomaga w zwiększeniu bezpieczeństwa sieci.

Do konfiguracji lokalnego uwierzytelniania wykorzystaliśmy następujące komendy:

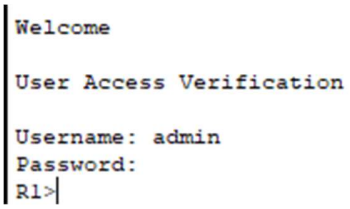
R1(config)# username admin secret admin // Ta komenda tworzy konto użytkownika o nazwie “admin” z hasłem “admin”. Hasło jest szyfrowane za pomocą silnego algorytmu szyfrowania

R1(config)# aaa new-model // Ta komenda włącza usługę AAA (Authentication, Authorization, and Accounting), która umożliwia bardziej zaawansowaną kontrolę dostępu do urządzenia.

R1(config)# aaa authentication login default local // Ta komenda konfiguruje domyślną listę metod uwierzytelniania AAA do logowania. Słowo “default” oznacza, że będzie używana domyślna lista metod, a “local” oznacza, że będzie używana lokalna baza danych do uwierzytelniania

R1(config)# line console 0 // Ta komenda przechodzi do konfiguracji konsoli.

R1(config-line)# login authentication default // Ta komenda stosuje domyślną listę metod uwierzytelniania do logowania na konsolę.



Rys. 10 Sprawdzenie lokalnej metody uwierzytelniania AAA na routerze nr 1

Protokół SNMP

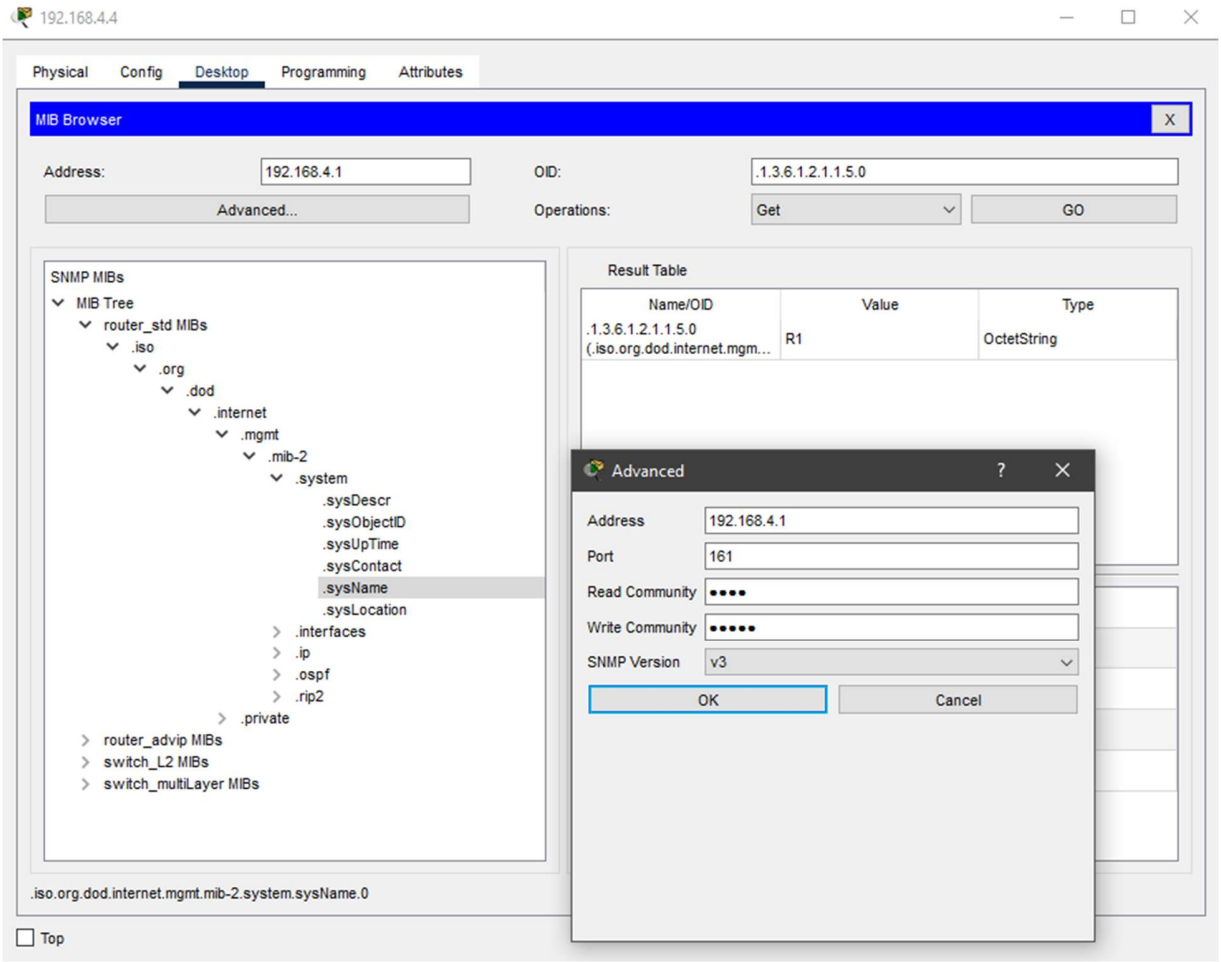
SNMP (Simple Network Management Protocol) to protokół działający w warstwie aplikacji modelu ISO/OSI, który jest używany do zarządzania i monitorowania urządzeń sieciowych w sieciach IP, takich jak routery, przełączniki, firewalle, serwery portów szeregowych, sterowniki PLC, urządzenia bezprzewodowe itp.

Dzięki SNMP możliwe jest zbieranie informacji z wielu różnych urządzeń w jednym miejscu sieci, na przykład na stacji roboczej administratora. Możemy monitorować praktycznie każde parametry urządzenia sieciowego – aktualne obciążenie procesora, ilość wolnego miejsca na dysku twardym, fizyczny stan portów na przełączniku itp. Dodatkowo, wykorzystując protokół SNMP, możemy zdalnie zmieniać konfigurację urządzeń.

Do włączenia protokołu SNMP wykorzystaliśmy następującą konfigurację:

R1(config)#snmp-server community read ro // Ta komenda konfiguruje SNMP (Simple Network Management Protocol) na routerze R1, tworząc społeczność o nazwie “read” z prawami tylko do odczytu (read-only, ro). Oznacza to, że urządzenia, które są członkami tej społeczności, mogą tylko pobierać informacje z urządzenia, ale nie mogą zmieniać konfiguracji

R1(config)#snmp-server community write rw // Ta komenda tworzy społeczność SNMP o nazwie “write” z prawami do odczytu i zapisu (read-write, rw). Oznacza to, że urządzenia, które są członkami tej społeczności, mogą zarówno pobierać informacje, jak i zmieniać konfigurację urządzenia



Rys. 11 Sprawdzenie działania protokołu SNMP na przykładzie zarządzania routerem R1

Serwer NTP

Serwer NTP (Network Time Protocol) to system używany do synchronizacji czasu w sieciach komputerowych. Działa na zasadzie dostarczania dokładnego czasu do wszystkich podłączonych urządzeń w sieci. Czas dostarczany przez serwer NTP jest starannie zsynchronizowany z tzw. wzorcowym czasem NTP, którego źródłem są sygnały pochodzące od systemu GPS, gwarantując niezwykłą dokładność i spójność czasu w całej infrastrukturze informatycznej.

Komendy wykorzystane do uruchomienia serwera NTP:

R1(config)# ntp server 192.168.4.2 // Ta komenda konfiguruje serwer NTP (Network Time Protocol) o adresie IP 192.168.4.2, do którego router będzie się synchronizować

R1(config)# ntp authenticate // Ta komenda włącza uwierzytelnianie NTP na routerze. Oznacza to, że router będzie wymagał uwierzytelnienia od swojego serwera NTP

R1(config)# ntp trusted-key 1 // Ta komenda mówi routerowi, który z skonfigurowanych kluczy ma użyć do uwierzytelniania serwera NTP. W tym przypadku, klucz o numerze 1 jest uznany za zaufany

R1(config)# ntp authentication-key 1 md5 admin // Ta komenda definiuje klucz uwierzytelniania NTP o numerze 1, używając algorytmu MD5 i hasła “admin” jako klucza

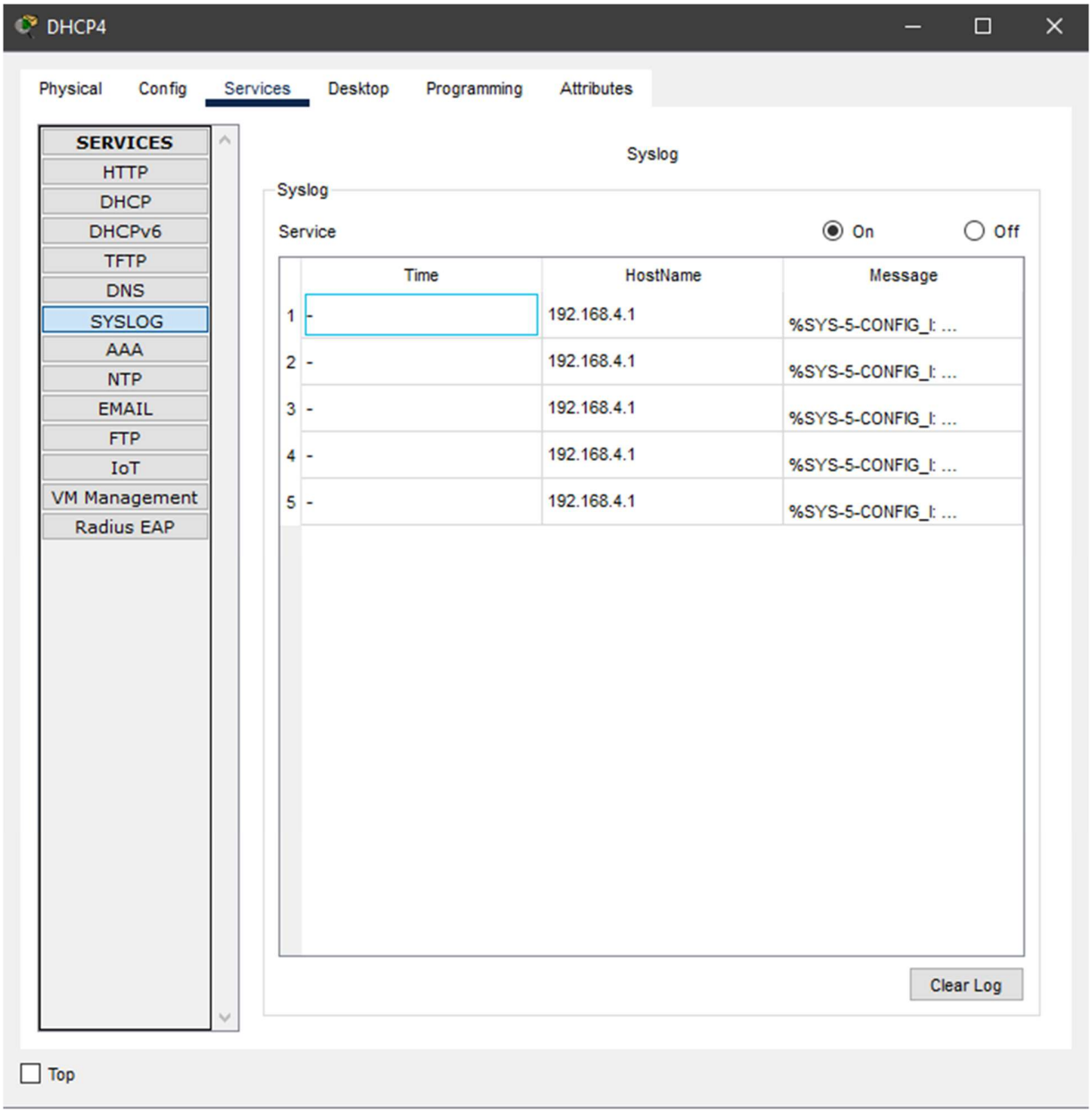
```
R2#show clock detail
2:50:40.476 UTC Mon Dec 18 2023
Time source is NTP
```

Rys. 12 Sprawdzenie działania serwera NTP

Syslog

Syslog to protokół logowania, który jest jednym z najważniejszych narzędzi systemowych w systemach operacyjnych uniksowych i uniksopodobnych1. Umożliwia rejestrowanie zdarzeń zachodzących w systemie przy pomocy scentralizowanego mechanizmu1. Pozwala na rejestrowanie informacji pochodzących ze źródeł: zgłoszeń przekazywanych przez bibliotekę systemową oraz informacji pochodzących od jądra systemu.

Serwer Syslog skonfigurowaliśmy z poziomu interfejsu GUI w następujący sposób:

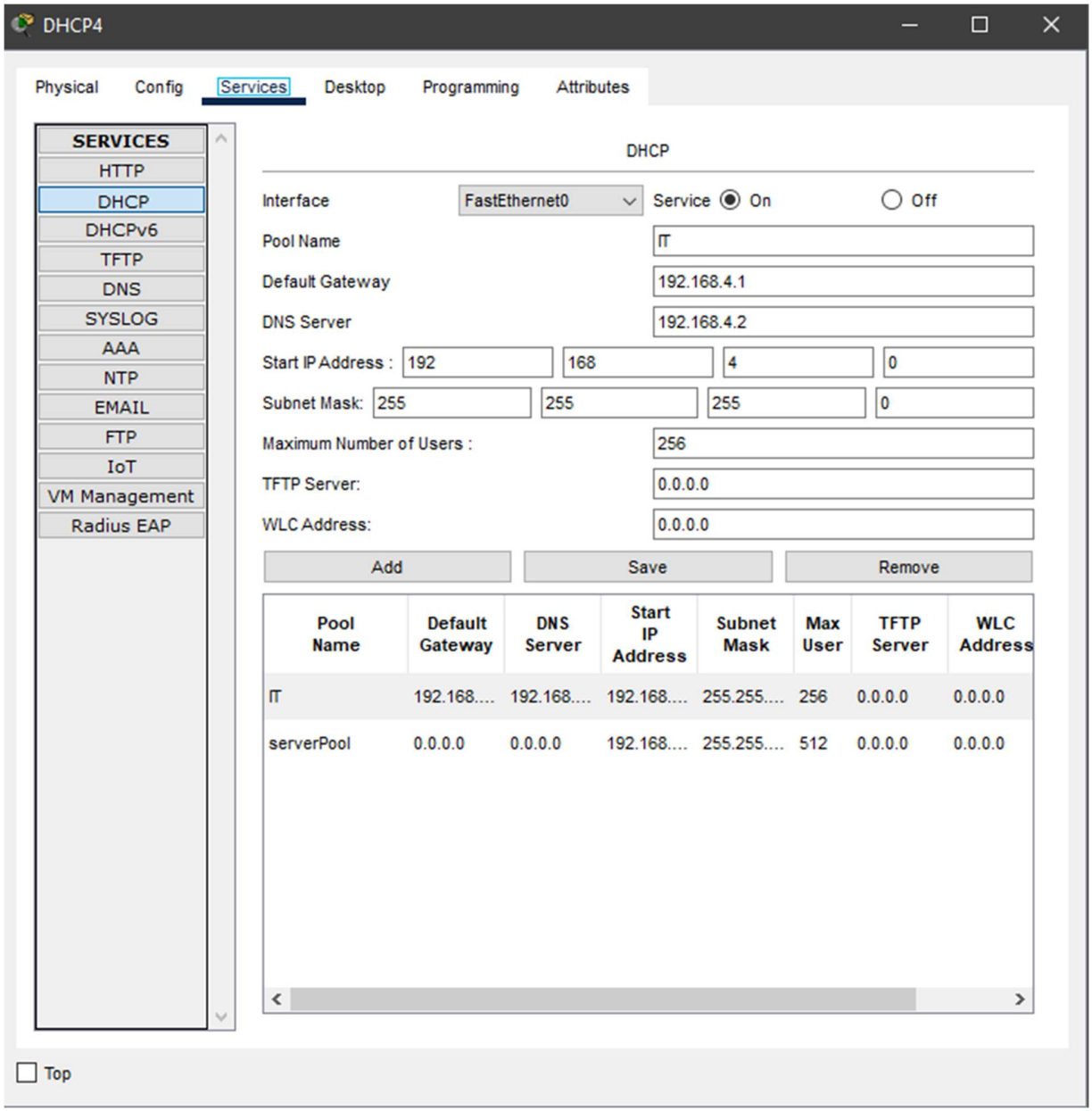


Rys. 13 Sprawdzenie logów z serwera Syslog

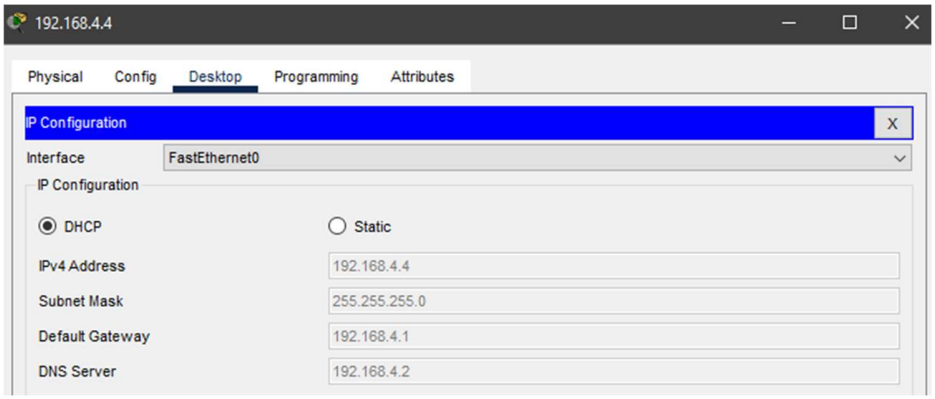
Serwer DHCP

DHCP (Dynamic Host Configuration Protocol) to protokół komunikacyjny, który umożliwia hostom uzyskanie od serwera danych konfiguracyjnych, takich jak adres IP hosta, adres IP bramy sieciowej, adres serwera DNS, maska podsieci. Dzięki DHCP, użytkownik nie musi wprowadzać tych danych ręcznie, aby korzystać z sieci.

Serwer DHCP skonfigurowaliśmy z GUI przy użyciu następujących ustawień:



Rys. 14 Ustawienia puli adresów dla serwera DHCP w dziale IT



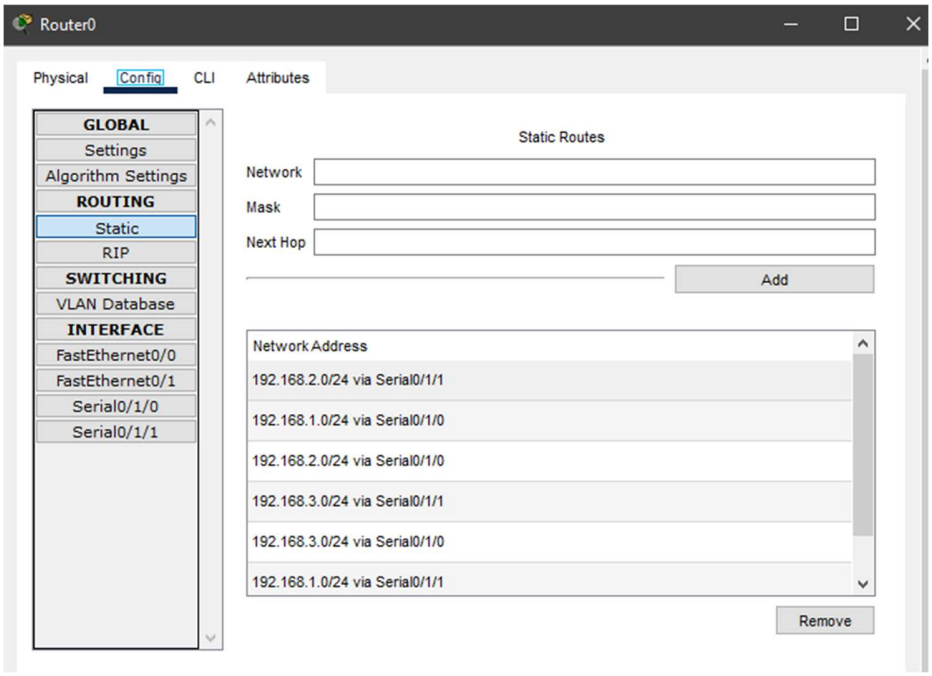
Rys. 15 Sprawdzenie działania serwera DHCP na podstawie jednego z komputerów w sieci

- Konfiguracja routingu

Routing statyczny to sposób wyznaczania ścieżek przesyłania danych w sieci, w którym administrator sieci wprowadza ręcznie wpisy do tablic routingu. Polega on na ręcznym wybraniu przez administratora sieci, jego zdaniem najlepszej trasy dla wysyłanych danych.

W ramach konfiguracji połączeń użyliśmy routingu statycznego który dodaliśmy za pomocą poniższej komendy:

R1(config)# ip route 192.168.4.0 255.255.255.0 se0/1/1 // Ta komenda mówi routerowi: "Aby dotrzeć do sieci 192.168.4.0/24, skieruj ruch przez interfejs se0/1/1" Komenda ta jest częścią konfiguracji routingu statycznego



Rys. 16 Adresy przypisane w ramach routingu statycznego

4. Analiza topologii pod kątem zagrożeń i możliwości skalowania

W ramach projektu zaimplementowaliśmy wiele mechanizmów oraz dodaliśmy obsługę szeregu technologii, które wpływają korzystnie na bezpieczeństwo stworzonej przez nas sieci. Niestety nie udało nam się wykonać konfiguracji sieci VLAN oraz zabezpieczyć się przed atakami z tym związanymi.

Poniżej znajduje się lista tematów, które są istotne pod kątem zagrożeń i powinny być uwzględnione w dalszym rozwoju naszej sieci:

- Pierwszym krokiem, który warto rozważyć, jest skonfigurowanie sieci VLAN i zabezpieczenie jej przed atakami VLAN. VLANy są skutecznym narzędziem do izolowania ruchu w sieci i mogą pomóc w ochronie przed różnymi typami ataków, takimi jak ataki typu “man in the middle”. Można to osiągnąć poprzez skonfigurowanie odpowiednich list dostępu i zabezpieczeń portu na przełącznikach.
- Kolejnym krokiem jest regularne aktualizowanie oprogramowania na wszystkich urządzeniach sieciowych. Aktualizacje często zawierają łatki bezpieczeństwa, które naprawiają znane luki w zabezpieczeniach, więc regularne ich instalowanie jest kluczowe dla utrzymania bezpieczeństwa sieci.
- Dodatkowo, warto zainwestować w system monitorowania sieci, który będzie śledził ruch sieciowy i generował alerty na podstawie zdefiniowanych reguł. Taki system może pomóc w wykrywaniu nietypowych wzorców ruchu, które mogą wskazywać na potencjalne ataki.
- Wreszcie, regularne przeprowadzanie audytów bezpieczeństwa sieci jest kluczowe dla utrzymania jej bezpieczeństwa. Audyty te powinny obejmować przegląd konfiguracji urządzeń sieciowych, testy penetracyjne i przegląd polityk bezpieczeństwa.

Bezpieczeństwo sieci to proces ciągły, który wymaga regularnego przeglądu i aktualizacji. Dlatego ważne jest, aby zawsze być na bieżąco z najnowszymi zagrożeniami i praktykami zabezpieczania sieci.

Jednakże, zawsze istnieje ryzyko potencjalnych ataków, na które sieć może nie być odporna. Na przykład, sieć może być narażona na ataki typu Denial-of-Service (DoS) lub Distributed Denial-of-Service (DDoS), które mają na celu przeciążenie zasobów systemu, uniemożliwiając obsługę prawidłowych żądań usług. Ataki typu Man-in-the-Middle (MITM) mogą również stanowić zagrożenie, ponieważ atakujący może podsłuchiwać dane przesyłane między dwoma stronami. Ponadto, ataki typu Malware, Phishing, Spoofing, Identity-Based Attacks, Code Injection Attacks, Supply Chain Attacks, Insider Threats, DNS Tunneling, IoT-Based Attacks są również powszechne i mogą stanowić zagrożenie dla sieci. Dlatego ważne jest, aby regularnie aktualizować i audytować zabezpieczenia sieci, aby minimalizować ryzyko tych ataków.

5. Wnioski

Na podstawie wykonanych zadań w projektowych, można wyciągnąć następujące wnioski:

1. **Zabezpieczenia sieci**: Wykonane zadania skupiały się na konfiguracji i zabezpieczeniu sieci, co jest kluczowe dla utrzymania integralności i bezpieczeństwa danych. Zabezpieczenia oraz technologie takie jak STP, DHCP, MAC, listy dostępu, VPN, AAA,

SNMP, NTP, syslog, DHCP są niezbędne do ochrony sieci przed różnymi typami ataków i zapewnienia jej prawidłowego funkcjonowania.

2. **Konfiguracja sieci**: Projekt obejmował konfigurację różnych aspektów sieci, takich jak routing. Te elementy są kluczowe dla efektywnego zarządzania ruchem sieciowym i zasobami.
3. **Analiza zagrożeń**: Przeprowadzenie analizy infrastruktury pod kątem zagrożeń pozwoliło na identyfikację potencjalnych słabych punktów w sieci oraz zwiększenie świadomości jakie aspekty są okazały się kluczowe przy planowaniu dalszego skalowania projektu
4. **Skalowalność sieci**: Projekt uwzględniał również aspekt skalowalności sieci. Dzięki konfiguracji takich usług jak DHCP, sieć jest przygotowana do obsługi rosnącej liczby urządzeń i użytkowników.
5. **Punkty do poprawy**: Mimo że większość zadań została wykonana pomyślnie, nie udało się zabezpieczyć sieci przed atakiem VLAN. Ten element powinien być uwzględniony w dalszych planach zabezpieczeń.

Podsumowując, projekt sieciowy był skomplikowany i wymagał zastosowania wielu technik i protokołów sieciowych. Mimo pewnych wyzwań, większość zadań została wykonana pomyślnie, co przyczyniło się do zwiększenia bezpieczeństwa i efektywności sieci. Jednakże, zawsze istnieje miejsce na poprawę i dalsze zabezpieczanie sieci. Dlatego ważne jest, aby regularnie przeglądać i aktualizować zabezpieczenia sieci, aby zapewnić jej bezpieczeństwo i niezawodność.