Bezpieczeństwo infrastruktury sieciowej

Projekt sieci dla urzędu gminy

Autorzy: Bartłomiej Tokar, Adam Rzepka, Michał Mosiołek
Grupa dziekańska: 1ID24B
Github: https://github.com/micad132/BIS-PROJEKT

Spis treści

1. Wprowadzenie 3
2. Opis zagrożeń 3
3. Topologia sieci 4
4. Adresacja sieci 5
4.1 Adresacja sieci VLAN - adresy przydzielane z puli DHCP: 5
4.2 Multilayer-Switch1: 5
4.3 Multilayer-Switch2: 6
4.4 CORE1: 6
4.5 CORE2: 6
4.6 ISP1: 7
4.7 ISP2: 7
5. Opis konfiguracji urządzeń i technologii. 7
5.1 Enable Secret 7
5.2 Hostname 8
5.3 VLAN 8
5.4 Routing OSPF 9
5.5 Access-Pointy: (znajdujący się w podsieci Biuro1 VLAN10) 10
5.6 DHCP: 11
5.7 DNS: 13
5.8 SSH: 13
5.9 NTP: 14
5.10 SYSLOG: 15
5.11 AAA: 17
5.12 ACL (Access Control List) 18
5.13 Spanning Tree Protocol (STP): 19
5.13.1 PortFast: 19
5.13.2 BPDUguard (Bridge Protocol Data Unit Guard): 20
6. Konfiguracja (show-running config) urządzeń 20
6.1. Konfiguracja switcha admin: 20
6.2. Konfiguracja switcha MultiLayerSwitch1: 24
6.3. Konfiguracja routera CORE1: 28

1. Wprowadzenie

Tematem projektu było zaprojektowanie i zaimplementowanie infrastruktury sieciowej dla urzędu gminy. Głównym celem projektu była identyfikacja możliwych zagrożeń oraz implementacja odpowiednich zabezpieczeń sieci. W dokumentacji zawarte są szczegółowe informacje na temat zagrożeń, schemat sieci, użyta adresacja oraz zaimplementowane zabezpieczenia.

2. Opis zagrożeń

- **Nieautoryzowany dostęp:**

Atakujący, dążąc do nieautoryzowanego dostępu, może wykorzystać różne metody, takie jak brute force, ataki słownikowe lub wykorzystanie błędów w konfiguracji systemów. Przejście przez zabezpieczenia oparte na słabych hasłach lub nieaktualnych protokołach może umożliwić hakerowi uzyskanie poufnych informacji lub pełnej kontroli nad infrastrukturą sieciową, co z kolei niesie za sobą ryzyko utraty danych i poufności informacji.

- **Utrata dostępu do urządzenia:**

Utrata dostępu do kluczowych urządzeń, takich jak serwery czy routery, może wynikać nie tylko z awarii sprzętu, ale również z celowych ataków, takich jak ataki fizyczne na obiekty. To z kolei może prowadzić do poważnych przerw w świadczeniu usług, utraty dostępności dla użytkowników, a także potencjalnej utraty danych w przypadku braku odpowiednich mechanizmów backupu.

- **Awaria urządzenia:**

Awarie urządzeń sieciowych, spowodowane problemami sprzętowymi, przeciążeniem bądź błędami w konfiguracji, mogą prowadzić do znacznych przerw w działaniu sieci. Te przerwy mogą z kolei skutkować utratą dostępności usług dla użytkowników oraz prowadzić do potencjalnych strat finansowych dla przedsiębiorstw, które zależą od stabilności swoich infrastruktur.

- **Ataki sieciowe typu MAC:**

Ataki typu MAC, obejmujące podszywanie się pod adresy MAC urządzeń, umożliwiają nieautoryzowany dostęp do sieci. Tego rodzaju ataki mogą zakłócić integralność i poufność danych przesyłanych w sieci, a także prowadzić do skierowania ruchu na złośliwe serwery, co potencjalnie zwiększa ryzyko utraty danych i naruszenia bezpieczeństwa sieci.

- **Ataki DDoS (Distributed Denial of Service):**

Ataki DDoS, polegające na przeciążeniu sieci poprzez generowanie ogromnej ilości ruchu, mogą skutkować znacznym spadkiem dostępności usług. To nie tylko prowadzi do niedogodności dla użytkowników, ale także może powodować straty finansowe dla firm zależnych od nieprzerwanej dostępności swoich usług online.

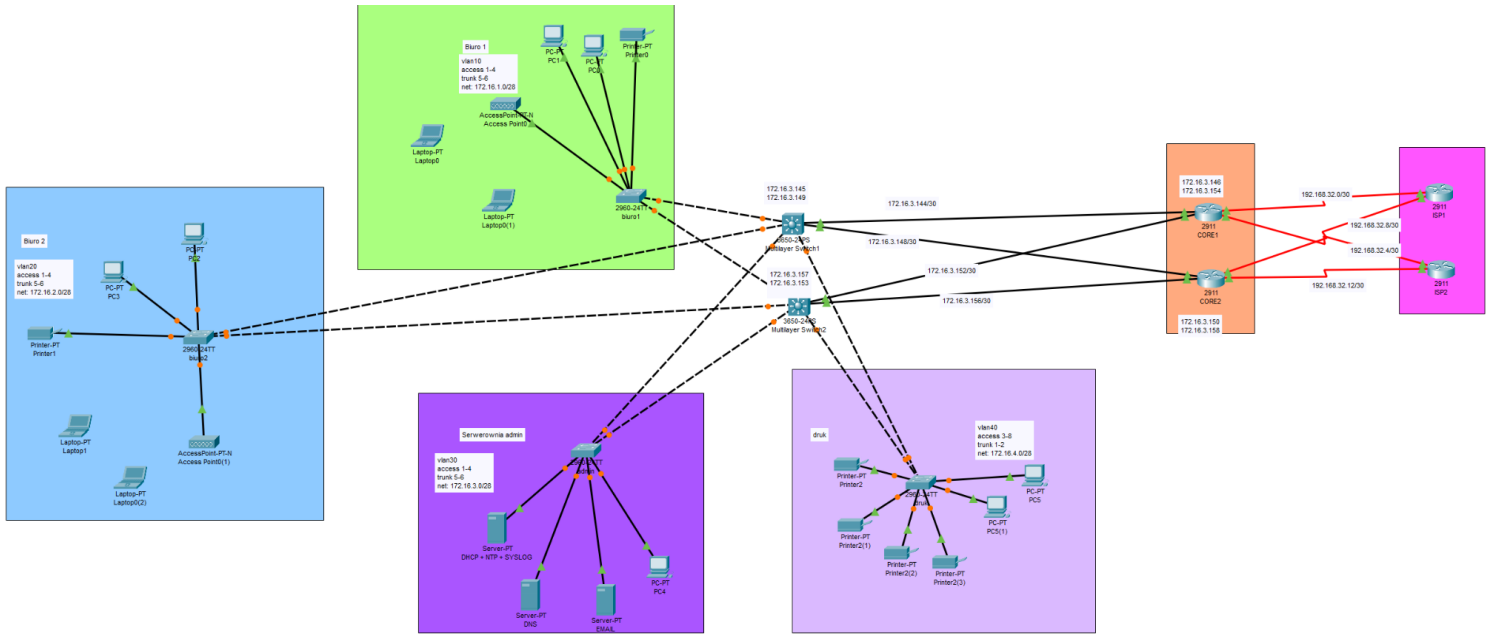
- **Ataki społeczne**

Ataki społeczne, takie jak phishing, stanowią poważne zagrożenie, gdyż wykorzystują manipulacje psychologiczne w celu uzyskania poufnych informacji od użytkowników. Mogą prowadzić do kradzieży danych, w tym loginów i haseł, co z kolei umożliwia nieautoryzowany dostęp do systemów oraz potencjalnie powoduje utratę poufności danych.

- **Ataki na warstwę fizyczną**

Ataki na warstwę zewnętrzną to próby naruszenia fizycznych elementów infrastruktury sieciowej, które stanowią jej podstawę. Ataki tego typu mają bardzo duży wpływ na dostępność sieci.

3. Topologia sieci



Rysunek 1. Topologia sieci

Sieć podzielona jest na cztery sieci VLAN, odpowiadająca odpowiednim pokojom w urzędzie gminy. W każdym VLANie znajdują się urządzenia końcowe, typowe dla urzędu - takie jak drukarki, komputery i serwery. Poza siecią administracyjną, w każdym VLANie adresy przydzielane są dynamicznie, za pomocą DHCP. Infrastruktura sieci oparta jest na modelu sieci hierarchicznej. Routery ISP symulują dostawcę internetowego.

4. Adresacja sieci

4.1 Adresacja sieci VLAN - adresy przydzielane z puli DHCP:

Numer:	Nazwa:	Pula adresów:
10	Biuro1	172.16.1.0/28
20	Biuro2	172.16.2.0/28
30	Admin	172.16.3.0/28
40	Druk	172.16.4.0/28

Tabela 1. Adresacja VLAN

4.2 Multilayer-Switch1:

Nazwa interfejsu:	Adres:
Ge1/0/5	172.16.3.145/30
Ge1/0/6	172.16.3.149/30
Vlan10	172.16.1.1/28
Vlan20	172.16.2.1/28
Vlan30	172.16.3.1/28
Vlan40	172.16.4.1/28

Tabela 2. Adresacja Multilayer 1

4.3 Multilayer-Switch2:

Nazwa interfejsu:	Adres:
Ge1/0/5	172.16.3.157/30
Ge1/0/6	172.16.3.153/30
Vlan10	172.16.1.1/28
Vlan20	172.16.2.1/28
Vlan30	172.16.3.1/28
Vlan40	172.16.4.1/28

Tabela 3. Adresacja Multilayer 2

4.4 CORE1:

Nazwa interfejsu:	Adres:
Ge0/0	172.16.3.146/30
Ge0/1	172.16.3.154/30
Se0/3/0	192.168.32.1/30
Se0/3/1	192.168.32.5/30

Tabela 4 Adresacja CORE1

4.5 CORE2:

Nazwa interfejsu:	Adres:
Ge0/0	172.16.3.150/30
Ge0/1	172.16.3.158/30
Se0/3/0	192.168.32.9/30
Se0/3/1	192.168.32.13/30

Tabela 5 Adresacja CORE2

4.6 ISP1:

Nazwa interfejsu:	Adres:
Se0/3/0	192.168.32.2/30
Se0/3/1	192.168.32.10/30

Tabela 6 Adresacja ISP1

4.7 ISP2:

Nazwa interfejsu:	Adres:
Se0/3/0	192.168.32.6/30
Se0/3/1	192.168.32.14/30

Tabela 7 Adresacja ISP2

5. Opis konfiguracji urządzeń i technologii.

5.1 Enable Secret

Enable secret jest bardziej bezpiecznym podejściem, ponieważ hasło jest przechowywane w postaci zaszyfrowanej (jednokierunkowe funkcje skrótu, takie jak MD5 lub SHA). Jest bardziej zalecane od enable password ze względu na większe bezpieczeństwo. Hasło enable secret nadpisuje enable password, jeśli oba są skonfigurowane. W przypadku konfliktu, enable secret jest preferowane. W praktyce zaleca się korzystanie z enable secret zamiast enable password, aby zwiększyć bezpieczeństwo dostępu do trybu EXEC. Ponadto, zawsze ważne jest stosowanie silnych, trudnych do odgadnięcia haseł w celu zabezpieczenia dostępu do urządzeń sieciowych.

```
!
enable password 7 0822455D0A16
!
```

Rysunek 2. Enable password przykład

5.2 Hostname

Konfigurowanie hostname w urządzeniach sieciowych, takich jak routery, ma kilka istotnych celów:

Identyfikacja urządzenia w sieci:
Hostname pomaga jednoznacznie zidentyfikować urządzenie w lokalnej sieci. Zamiast korzystać z adresu IP, możesz używać czytelnych dla ludzi nazw, co ułatwia zarządzanie i identyfikację urządzeń.

Łatwiejsze zarządzanie:
Posiadanie nazw hosta ułatwia administratorom sieci śledzenie i zarządzanie różnymi urządzeniami w sieci. Dzięki temu można szybko rozpoznać, które urządzenie jest które, co jest szczególnie przydatne w większych sieciach.

Współpraca z DNS:
Hostname są często używane w systemie Domain Name System (DNS), który przekształca czytelne dla ludzi nazwy hostów na adresy IP i odwrotnie. Konfiguracja hostname na routerze może ułatwić integrację z DNS.

```
!
hostname CORE2
!
```

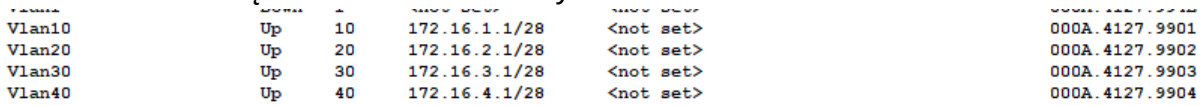
Rysunek 3. Ustawianie hostname

5.3 VLAN

VLANy, czyli Virtual Local Area Networks, to technologia stosowana w sieciach komputerowych, która umożliwia podział fizycznej sieci lokalnej na logiczne, odseparowane od siebie podsieci. VLANy pozwalają na grupowanie urządzeń w sieci na podstawie kryteriów logicznych, takich jak departament, funkcja, projekt czy też typ urządzenia. Dzięki temu możliwe jest zwiększenie elastyczności, bezpieczeństwa i wydajności sieci. Segmentacja sieci jest jednym z głównych powodów używania VLANów. VLANy umożliwiają podział jednej fizycznej sieci na wiele logicznych sieci. Każda taka sieć, będąca osobnym VLANem, działa jak niezależna podsieć, co pomaga w ograniczaniu kolizji i nadmiernego ruchu sieciowego. LANy pozwalają na izolowanie grup urządzeń, co może znacząco poprawić bezpieczeństwo sieci. Dzięki temu, że urządzenia w jednym VLANie nie widzą ani nie mają bezpośredniego dostępu do urządzeń w innych VLANach, można zminimalizować ryzyko nieautoryzowanego dostępu. ważnym aspektem VLANów jest również zarządzanie ruchem. Korzystanie z VLANów pozwala na bardziej skuteczne zarządzanie ruchem sieciowym. Administracja może kontrolować, jakie urządzenia komunikują się ze sobą w obrębie danego VLANu, co ma znaczący wpływ na efektywne wykorzystanie

pasma. Dzięki VLANom można łatwo rozbudowywać sieć. Nowe urządzenia lub grupy urządzeń można przypisywać do istniejących VLANów bez konieczności przeprowadzania zmian w samej infrastrukturze sieciowej.

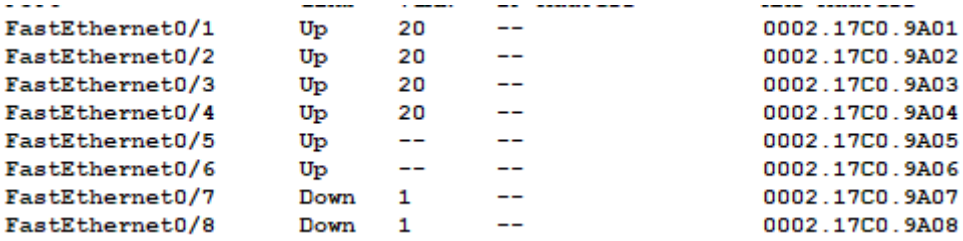
W sieci zaimplementowane zostały cztery sieci VLAN - Biuro 1, Biuro 2, Admin oraz Druk. Każdy z VLANów posiada przydzieloną pulę adresów IP. Dzięki temu prościej zarządzać połączeniami, oraz zabezpieczyć urządzenia sieciowe. VLANy zadeklarowane są na switchach multilayer:



Vlan10	Up	10	172.16.1.1/28	<not set>	000A.4127.9901
Vlan20	Up	20	172.16.2.1/28	<not set>	000A.4127.9902
Vlan30	Up	30	172.16.3.1/28	<not set>	000A.4127.9903
Vlan40	Up	40	172.16.4.1/28	<not set>	000A.4127.9904

Rysunek 4. VLAN

Aby dodatkowo zabezpieczyć sieć, wszystkie nieużywane porty na urządzeniach są wyłączone, na przykładzie switcha biuro2:



FastEthernet0/1	Up	20	--	0002.17C0.9A01
FastEthernet0/2	Up	20	--	0002.17C0.9A02
FastEthernet0/3	Up	20	--	0002.17C0.9A03
FastEthernet0/4	Up	20	--	0002.17C0.9A04
FastEthernet0/5	Up	--	--	0002.17C0.9A05
FastEthernet0/6	Up	--	--	0002.17C0.9A06
FastEthernet0/7	Down	1	--	0002.17C0.9A07
FastEthernet0/8	Down	1	--	0002.17C0.9A08

Rysunek 5. Wyłączenie nieużywanych portów

5.4 Routing OSPF

OSPF, czyli Open Shortest Path First, jest jednym z protokołów routingu dynamicznego stosowanych w sieciach komputerowych. To protokół wewnętrzny, używany głównie w środowiskach IP, który umożliwia routerom wymianę informacji o stanie sieci oraz automatyczne wyznaczanie najkrótszych ścieżek (tras) do osiągnięcia dostępnych celów. W przypadku urządzeń Cisco, OSPF jest powszechnie stosowanym protokołem routingu, a jego implementacja jest obszernie wspierana w systemie operacyjnym Cisco IOS (Internetwork Operating System). Sieć OSPF jest zorganizowana w tzw. obszary (areas). Każdy obszar to logiczna grupa routerów i sieci, a stosowanie obszarów umożliwia skalowanie i zwiększenie efektywności routingu w dużych sieciach. Router, który łączy różne obszary, nazywany jest routerem granicznym (ABR - Area Border Router). OSPF w systemie Cisco IOS jest realizowany jako osobny proces. Każdy proces OSPF ma swoje unikalne identyfikatory, a konfiguracja OSPF obejmuje ustalanie parametrów tego procesu, takich jak router ID, obszary, priorytety routerów, itp.

Implementacja routingu OSPF na routerze CORE1 jest następująca:

```
!
router ospf 10
 router-id 3.3.3.3
 log-adjacency-changes
 network 172.16.3.144 0.0.0.3 area 0
 network 172.16.3.152 0.0.0.3 area 0
 network 192.168.32.0 0.0.0.3 area 0
 network 192.168.32.4 0.0.0.3 area 0
!
```

Rysunek 6. Implementacja OSPF

Dodatkowo, aby umożliwić komputerom z gminy komunikację z routerami ISP, na routerach utworzono drogi statyczne - na przykładzie CORE1:

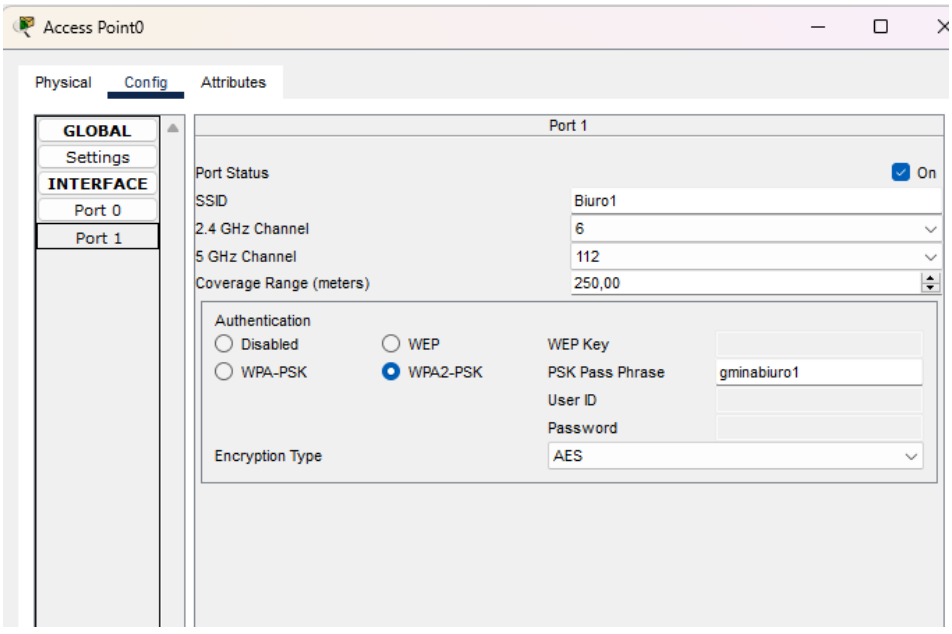
```
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/3/0
ip route 0.0.0.0 0.0.0.0 Serial0/3/1 70
!
```

Rysunek 7. Utworzenie dróg statycznych

5.5 Access-Pointy: (znajdujący się w podsieci Biuro1 VLAN10)

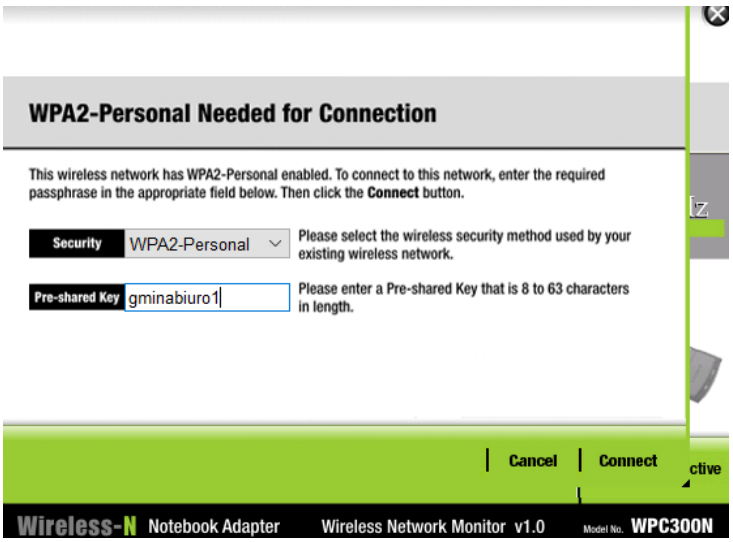
Dodatkowo bezpieczeństwo połączenia zostało zabezpieczone kluczem WPA2-PSK - dzięki czemu podłączenie do sieci bezprzewodowej jest możliwe dla osób, które znają hasło.

Przykład implementacji zabezpieczeń Access Point dla Biura 1:
SSID - Biuro1
PSK Pass Phrase - gminabiuro1



Rysunek 8. Access Point

Przykład bezprzewodowego połączenia urządzenia z Access Pointem:



Rysunek 9. WPA2

5.6 DHCP:

Protokół DHCP (Dynamic Host Configuration Protocol) to standardowy protokół używany w sieciach komputerowych do automatycznego przydzielania adresów IP oraz innych konfiguracji sieciowych (takich jak maska podsieci, domyślna brama, serwery DNS) dla urządzeń w sieci. Zamiast ręcznego przypisywania statycznych adresów IP do każdego urządzenia w sieci, serwer DHCP może dynamicznie przydzielać adresy IP z puli dostępnych adresów.

W naszym projekcie skonfigurowaliśmy strefy DHCP według VLANów:

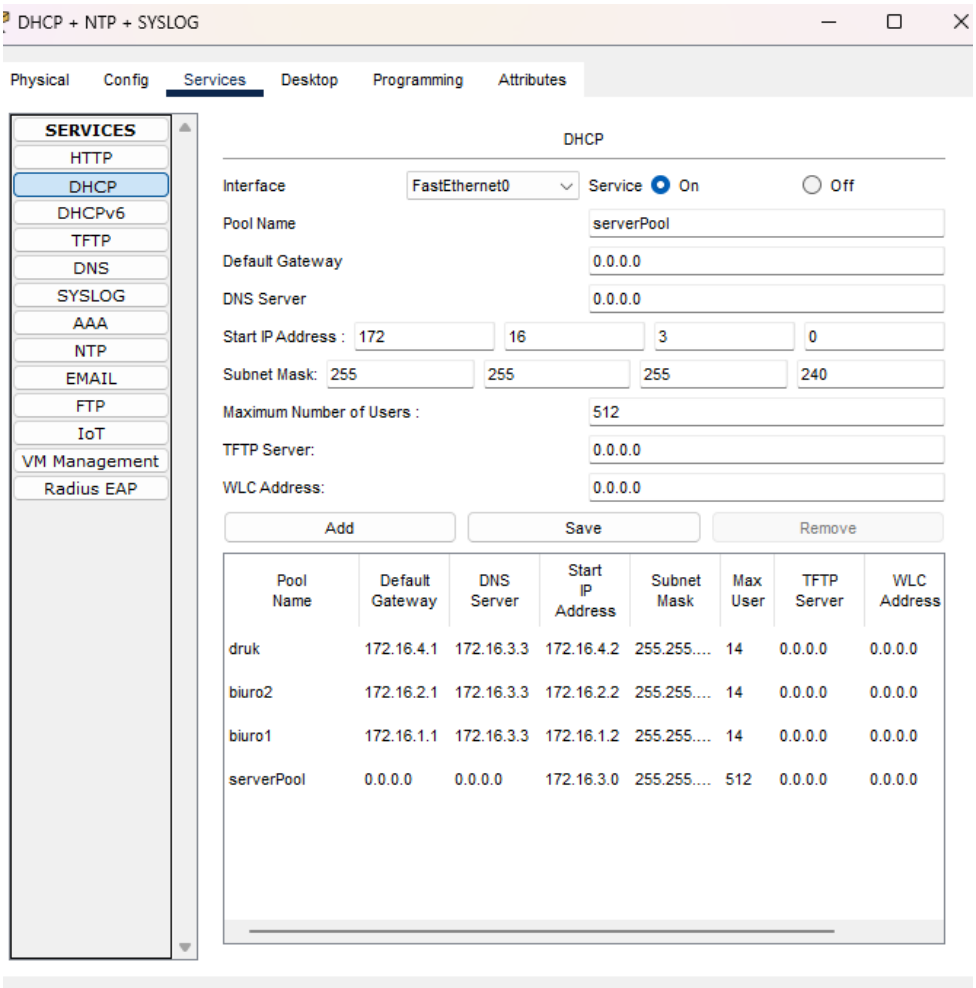
- DRUK (VLAN40) - adresy IP zaczynające się od 172.16.4.2
- BIURO2(VLAN20) - adresy IP zaczynające się od 172.16.2.2
- BIURO1(VLAN10) - adresy IP zaczynające się od 172.16.1.2

Dodatkowo, na Multilayer-Switch, do wszystkich sieci VLAN dodano adres serwera DHCP jako helper-address aby pomóc zidentyfikować serwer DHCP.

```
interface Vlan10
 mac-address 000a.4127.9901
 ip address 172.16.1.1 255.255.255.240
 ip helper-address 172.16.3.2
!
interface Vlan20
 mac-address 000a.4127.9902
 ip address 172.16.2.1 255.255.255.240
 ip helper-address 172.16.3.2
!
interface Vlan30
 mac-address 000a.4127.9903
 ip address 172.16.3.1 255.255.255.240
 ip helper-address 172.16.3.2
!
interface Vlan40
 mac-address 000a.4127.9904
 ip address 172.16.4.1 255.255.255.240
 ip helper-address 162.16.3.2
!
```

Rysunek 10. Dodanie helper-address

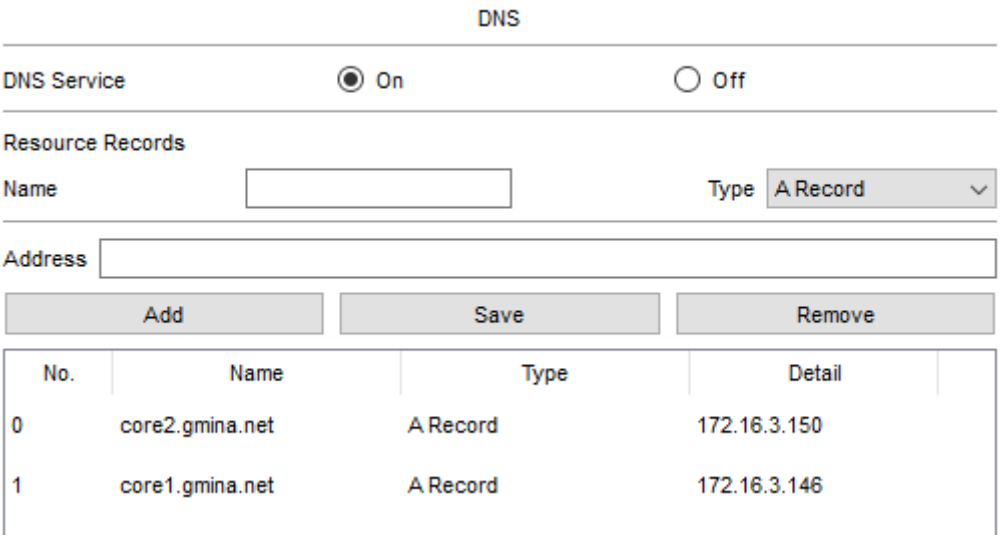
Konfiguracja serwera DHCP jest następująca:



Rysunek 11. Konfiguracja DHCP

5.7 DNS:

W sieci skonfigurowany został serwer DNS, znajdujący się w sieci administracyjnej. Dzięki niemu umożliwiona jest translacja nazw domen. Dla przykładu działania skonfigurowano domeny dla routerów CORE1 i CORE2, aby móc łączyć się z SSH za pomocą domen, a nie adresów IP:



Rysunek 12. DNS

5.8 SSH:

Jest protokołem sieciowym, który zapewnia bezpieczny sposób zdalnego logowania się do komputerów lub urządzeń sieciowych przez internet. Umożliwia to szyfrowane połączenie między klientem a serwerem, co zapewnia bezpieczeństwo podczas przesyłania danych.

Przykład konfiguracji SSH na routerze CORE1:

```
line vty 0 4
 transport input ssh
```

Rysunek 13. Konfiguracja SSH

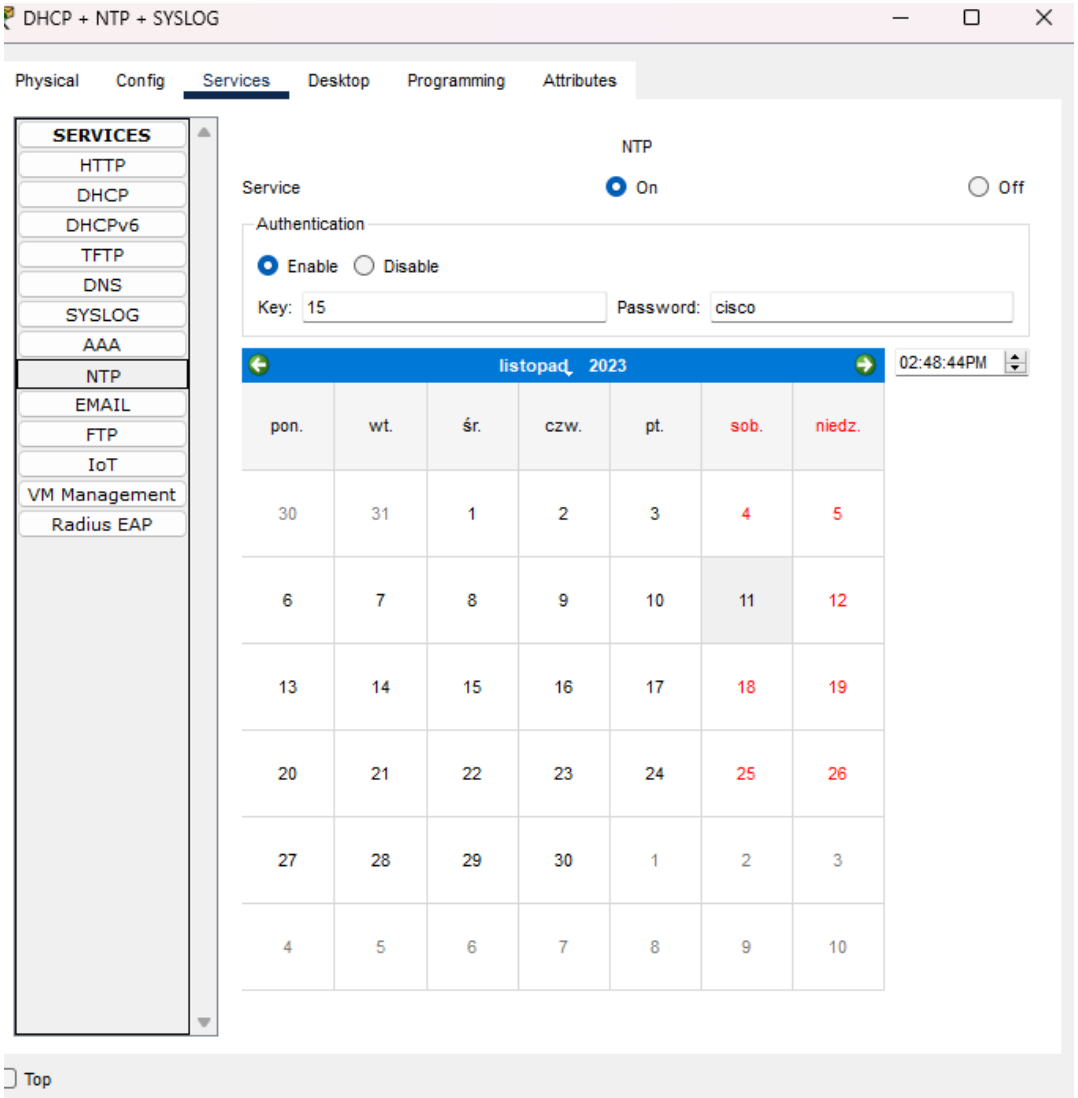
Przykład połączenia SSH z CORE2:

```
[Connection to 172.16.3.146 closed by foreign host]
C:\>ssh -l admin core2.gmina.net

Trying 172.16.3.150 ...
Password:

autoryzacja wymagana
```

Rysunek 14. SSH CORE2

5.9 NTP:

NTP (Network Time Protocol) to protokół komunikacyjny używany do synchronizacji zegarów komputerowych w sieciach komputerowych. NTP zapewnia spójność czasu na różnych urządzeniach w sieci, co jest istotne dla np. logów systemowych. Dzięki NTP urządzenia mogą uzyskiwać dokładny czas z dedykowanych serwerów czasowych, co pomaga w unikaniu problemów związanych z niespójnym czasem między różnymi systemami.



Rysunek 15. NTP

Konfiguracja usługi NTP na routerach CORE oraz przełącznikach MULTILAYER:

CORE1#conf t
Enter configuration commands, one per line. End with CNTL/Z.

CORE1(config)#ntp authenticate
CORE1(config)#ntp authentication-key 15 md5 cisco
CORE1(config)#ntp trusted-key 15
CORE1(config)#ntp server 172.16.3.2 key 15
CORE1(config)#exit

Status ntp na routerze CORE1:

```
CORE1#show ntp status
Clock is synchronized, stratum 2, reference is 172.16.3.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E8CD4043.00000046 (14:50:43.070 UTC Sat Nov 11 2023)
clock offset is 0.00 msec, root delay is 1.00  msec
root dispersion is 17.22 msec, peer dispersion is 0.00 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 1 sec ago.
CORE1#
```

Rysunek 16. NTP CORE1

5.10 SYSLOG:

Syslog to protokół używany do zbierania, przesyłania i zarządzania logami zdarzeń w sieciach komputerowych. Protokół ten pozwala różnym urządzeniom komunikować się i przesyłać informacje dotyczące zdarzeń, błędów, ostrzeżeń i innych danych dziennika zdarzeń do centralnego systemu lub narzędzia do zarządzania logami. W naszym przypadku serwerem zbierającym logi jest serwer o nazwie: DHCP + NTP + SYSLOG

CORE1,CORE2, MutliLayerSwitch1,MultiLayerSwitch2, switche vlanowe:

logging 172.16.3.2
logging on
logging trap debuging

Następnie na MultiLayerSwitch1 i MultiLayerSwitch2 dodany został loopback:

Loopback to ,,wirtualny” interfejs sieciowy w urządzeniu, który umożliwia komunikację z samym sobą. Używany jest głównie do testowania i debugowania aplikacji sieciowych.

MultiLayerSwitch1:

interface loopback0
ip address 192.168.10.1 255.255.255.255

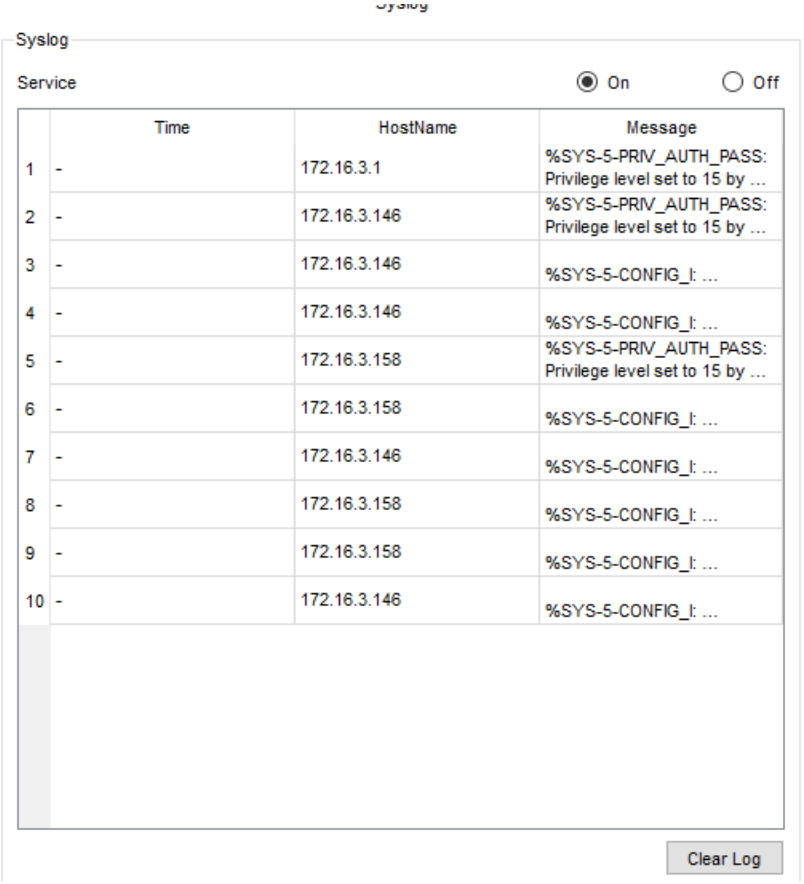
no shutdown
logging source-interface loopback0

MultiLayerSwitch2:

interface loopback0
ip adress 192.168.10.1 255.255.255.255
no shutdown
logging on
logging userinfo

Syslog na CORE1, CORE2:

logging 172.16.3.2
logging on
logging trap debugging
logging userinfo
do wr



Rysunek 17. SYSLOG

5.11 AAA:

Są to usługi, która zapewniają autentykację (Authentication), autoryzację (Authorization) oraz zarządzanie rachunkami (Accounting) dla użytkowników, którzy próbują uzyskać dostęp do zasobów sieciowych.

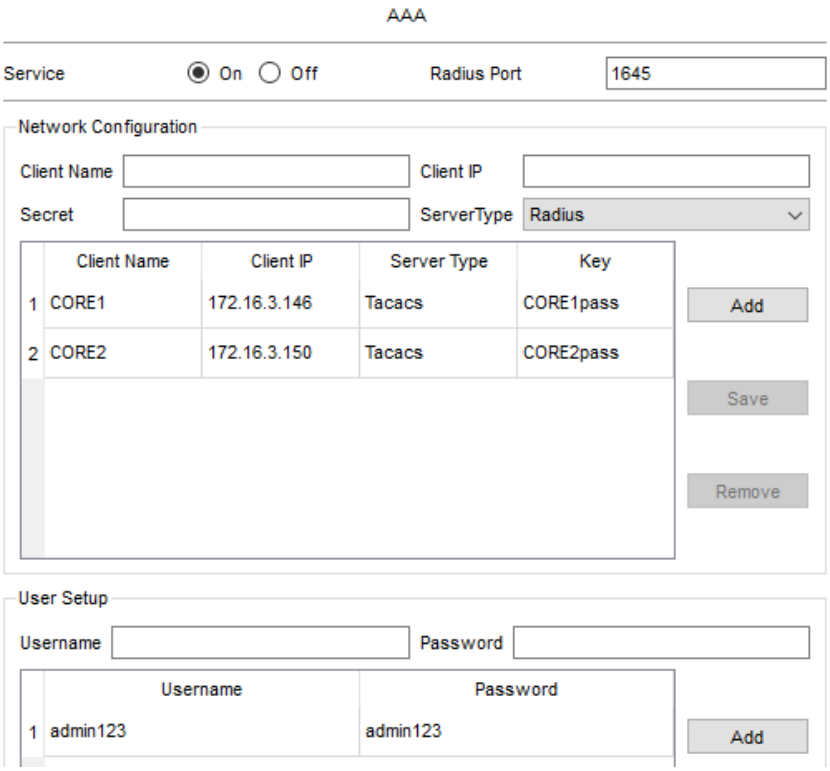
- Autentykacja (Authentication) - zapewnia proces weryfikacji tożsamości użytkownika poprzez proces uwierzytelniania przy użyciu haseł, certyfikatów, tokenu, biometryki czy innych metod.

- Autoryzacja (Authorization) - Po udanej autentykacji określa, jakie zasoby lub usługi dany użytkownik ma prawo wykorzystać. Dodatkowo określa poziomy dostępu, uprawnienia i zakres działań, które dany użytkownik może wykonywać w sieci.

- Zarządzanie rachunkami (Accounting) - polega na rejestrowaniu aktywności użytkowników w sieci, takich jak logowanie, wykorzystywanie zasobów czy inne operacje. Informacje te mogą być wykorzystywane do audytów, monitorowania aktywności, analizy wykorzystania zasobów i tworzenia raportów.

```
aaa new-model
!
aaa authentication login default group tacacs+ local
!
!
tacacs-server host 172.16.3.2
tacacs-server key COREIpass
!
```

Rysunek 18. Konfiguracja AAA



Rysunek 19. AAA

5.12 ACL (Access Control List)

ACL to lista kontroli dostępu. Służy ona do zarządzania uprawnieniami innych użytkowników sieci i Internetu. Dzięki zastosowaniu list ACL można ograniczyć i kontrolować dostęp do zasobów sieci. W projekcie listy ACL zostały zastosowane, aby ograniczyć dostęp SSH do routerów CORE1 i 2 użytkownikom spoza VLAN Admin.

Implementacja listy ACL SSH na CORE1:

```
CORE1#show access-lists
Extended IP access list SSH
    10 permit tcp 172.16.3.0 0.0.0.15 any eq 22 (2 match(es))
    20 deny tcp any any eq 22 (6 match(es))
```

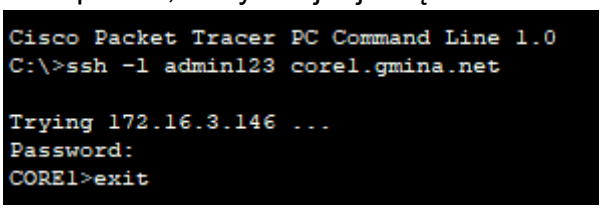
Rysunek 20. Implementacja ACL

Zabezpieczenie dostępu SSH za pomocą listy ACL w konfiguracji:

```
!
line vty 0 4
 access-class SSH in
 transport input ssh
```

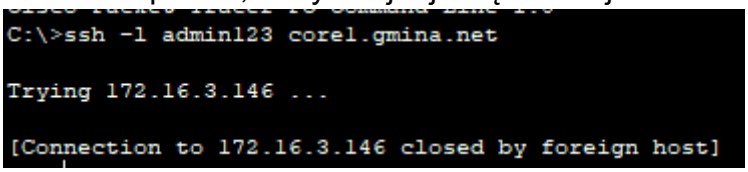
Rysunek 21. Zabezpieczenie SSH

Próba dostępu SSH z komputera, który znajduje się w VLAN ADMIN:



Rysunek 22. Testowanie Dostępu

Próba dostępu SSH z komputera, który znajduje się w innej sieci VLAN:



Rysunek 23. Testowanie Dostępu

5.13 Spanning Tree Protocol (STP):

Protokół drzewa rozpinającego, używany do zapobiegania pętlom w sieciach komputerowych opartych na technologii Ethernet. Protokół ten wybiera jedną główną ścieżkę w drzewie rozpinającym, eliminując tym samym pętle, które mogą prowadzić do problemów w sieci

Przykład konfiguracji STP na switchu Biuro1:

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 000A.F3EA.E50E
 switchport port-security aging time 10
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

5.13.1 PortFast:

Funkcja stosowana w protokole STP (Spanning Tree Protocol), który jest używany w sieciach komputerowych w celu eliminowania pętli i zapewnienia bezpieczeństwa w topologiach drzewa rozpinającego.

5.13.2 BPDUguard (Bridge Protocol Data Unit Guard):

Funkcja stosowana w protokole STP (Spanning Tree Protocol) w sieciach komputerowych. Jej głównym celem jest zabezpieczenie przed sytuacjami, w których na porcie przełącznika, który nie powinien być połączony z innym przełącznikiem, pojawiają się komunikaty BPDU.

BPDU to Bridge Protocol Data Unit, czyli jednostka danych protokołu mostu, używanego w protokołach drzewa rozpinającego, takich jak STP. Komunikaty BPDU są wymieniane między przełącznikami w celu ustalenia i utrzymania drzewa rozpinającego, a także do eliminacji pętli w sieci.

BPDUguard monitoruje porty przełącznika i gdy wykryje, że na porcie pojawiły się komunikaty BPDU, traktuje to jako potencjalne zagrożenie pętli i reaguje poprzez dezaktywację tego portu.

6. Konfiguracja (show-running config) urządzeń

6.1. Konfiguracja switcha admin:

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname admin
!
enable password 7 0822455D0A16
!
!
!
no ip domain-lookup
!
!
ip dhcp snooping vlan 30
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
```

switchport access vlan 30
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0001.9600.1B0D
switchport port-security aging time 10
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/2
switchport access vlan 30
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security aging time 10
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/3
switchport access vlan 30
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security aging time 10
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/4
switchport access vlan 30
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0003.E458.5149
switchport port-security aging time 10
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/5
ip dhcp snooping trust
ip dhcp snooping limit rate 10

switchport mode trunk
!
interface FastEthernet0/6
ip dhcp snooping trust
ip dhcp snooping limit rate 10
switchport mode trunk
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19

```
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^Cwymaga autoryzacji^C
logging trap debugging
logging 172.16.3.2
!
!
!
line con 0
password 7 0822455D0A16
login
!
line vty 0 4
login
line vty 5 15
login
!
!
!
ntp authenticate
ntp trusted-key 15
```

ntp server 172.16.3.2 key 15
!
end

6.2. Konfiguracja switcha MultiLayerSwitch1:

version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MultiLayerSwitch1
!
logging userinfo
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name psk.net

```
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Loopback0
ip address 192.168.10.1 255.255.255.255
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
!
interface GigabitEthernet1/0/5
no switchport
ip address 172.16.3.145 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/6
no switchport
ip address 172.16.3.149 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
```

interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
shutdown
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 000a.4127.9901
ip address 172.16.1.1 255.255.255.240
ip helper-address 172.16.3.2
!
interface Vlan20
mac-address 000a.4127.9902

```
ip address 172.16.2.1 255.255.255.240
ip helper-address 172.16.3.2
!
interface Vlan30
mac-address 000a.4127.9903
ip address 172.16.3.1 255.255.255.240
ip helper-address 172.16.3.2
!
interface Vlan40
mac-address 000a.4127.9904
ip address 172.16.4.1 255.255.255.240
ip helper-address 162.16.3.2
!
router ospf 10
router-id 2.2.2.2
log-adjacency-changes
network 172.16.1.0 0.0.0.127 area 0
network 172.16.2.0 0.0.0.127 area 0
network 172.16.3.0 0.0.0.127 area 0
network 172.16.4.0 0.0.0.127 area 0
network 172.16.3.144 0.0.0.3 area 0
network 172.16.3.148 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0/5
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1/0/6 70
!
ip flow-export version 9
!
!
!
banner motd ^Cwymaga autoryzacji^C
!
!
!
!
logging trap debugging
logging 172.16.3.2
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
```

line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
!
!
ntp authentication-key 15 md5 0822455D0A16 7
ntp authenticate
ntp trusted-key 15
ntp server 172.16.3.2 key 15
!
end

6.3. Konfiguracja routera CORE1:

no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname CORE1
!
logging userinfo
!
!
enable password 7 0822455D0A16
!
!
!
!
!
aaa new-model
!
aaa authentication login default group tacacs+ local
!
!
!

```
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX1524NPY7-
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
no ip domain-lookup
ip domain-name psk.net
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 172.16.3.146 255.255.255.252
ip access-group SSH out
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 172.16.3.154 255.255.255.252
ip access-group SSH out
duplex auto
```

speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 192.168.32.1 255.255.255.252
clock rate 2000000
!
interface Serial0/3/1
ip address 192.168.32.5 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 10
router-id 3.3.3.3
log-adjacency-changes
network 172.16.3.144 0.0.0.3 area 0
network 172.16.3.152 0.0.0.3 area 0
network 192.168.32.0 0.0.0.3 area 0
network 192.168.32.4 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/3/0
ip route 0.0.0.0 0.0.0.0 Serial0/3/1 70
!
ip flow-export version 9
!
!
ip access-list extended SSH
permit tcp 172.16.3.0 0.0.0.15 any eq 22
deny tcp any any eq 22
!
banner motd ^Cautoryzowany dostep^C
!
tacacs-server host 172.16.3.2
tacacs-server key CORE1pass
!

```
!
!
logging trap debugging
logging 172.16.3.2
line con 0
password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
access-class SSH in
transport input ssh
line vty 5 15
transport input ssh
!
!
ntp authentication-key 15 md5 0822455D0A16 7
ntp authenticate
ntp trusted-key 15
ntp server 172.16.3.2 key 15
!
end
```