



CYBERBEZPIECZEŃSTWO 2.0

Termin zajęć CZ_9:15-11:00	Programowanie bezpiecznych internetowych transmisji danych
Osoby wykonujące ćwiczenie:	Krakasevich Aleksandr - 272287
Prowadzący:	dr hab. inż. Radosław Wróbel

Spis treści

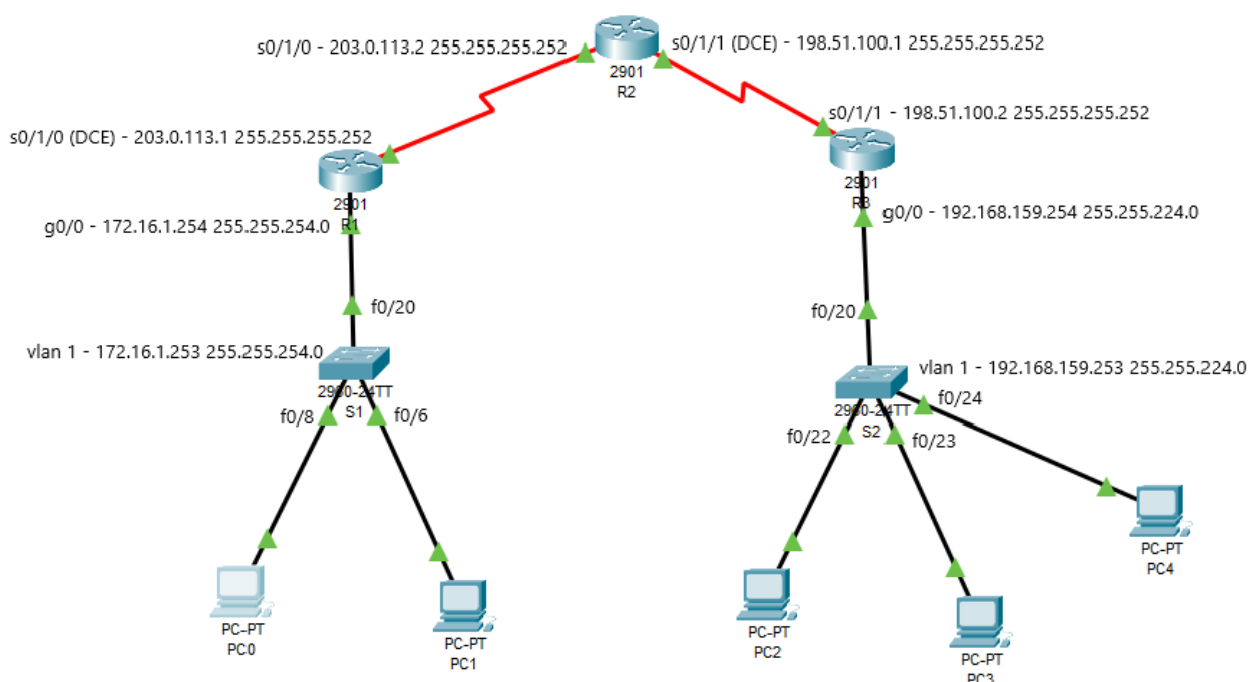
Wstęp	2
Ćześć 1: Tworzenie topologii i podstawowa konfiguracja urządzeń	3
Część 2: Konfiguracja OSPF	3
Część 3: Konfiguracja DHCP.....	4
Część 4: Konfiguracja przełączników.....	4
Część 5: Weryfikacja łączności	4
Część 6: Konfiguracja OSPF	4
Część 6: Konfiguracja DHCP.....	5
Część 7: Konfiguracja przełączników.....	5
Część 8: Weryfikacja łączności	5
Omówienie konfiguracji	6
Konfiguracja urządzeń (show run).....	7
Wnioski.....	20

Wstęp

Celem pracy jest zaprojektowanie, skonfigurowanie i przetestowanie sieci komputerowej w środowisku symulacyjnym, obejmującej zastosowanie dynamicznego routingu, adresacji IP oraz usług sieciowych, takich jak DHCP. Projekt zakłada stworzenie sieci obsługującej dwa segmenty lokalne o dużej liczbie hostów: pierwszy segment, po lewej stronie topologii, ma obsługiwać 500 hostów, natomiast drugi segment, po prawej stronie, ma obsługiwać 5000 hostów. W każdym segmencie dynamiczne przydzielanie adresów IP realizowane jest za pomocą serwera DHCP.

Praca uwzględnia stworzenie topologii sieci, przypisanie odpowiednich adresów IP w taki sposób, aby spełniały wymagania co do liczby hostów, konfigurację urządzeń sieciowych (przełączników i routerów), a także rozwiązywanie potencjalnych problemów związanych z konfiguracją. Ważnym elementem jest weryfikacja poprawności działania sieci poprzez testowanie łączności między urządzeniami oraz przygotowanie sprawozdania dokumentującego cały proces.

Task	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Adresacja																											
Podstawowa konfiguracja urządzeń																											
Konfiguracja S1, R1, R2 (lewej strony)																											
Rozwiązywanie problemów																											
Konfiguracja S2, R3, R2																											
Rozwiązywanie problemów																											
Sprawozdanie																											



1. topologia sieci

Urządzenie	Interfejs	Adres IP	Maska podsieci
R1	g0/0	172.16.1.254	255.255.254.0
	s0/1/0 (DCE)	203.0.113.1	255.255.255.252
R2	s0/1/0	203.0.113.2	255.255.255.252
	s0/1/1 (DCE)	198.51.100.1	255.255.255.252
R3	g0/0	192.168.159.254	255.255.224.0
	s0/1/1	198.51.100.2	255.255.255.252
S1	VLAN 1	172.16.1.253	255.255.254.0
S2	VLAN 1	192.168.159.253	255.255.224.0

Ćześć 1: Tworzenie topologii i podstawowa konfiguracja urządzeń

Krok 1: Podstawowe ustawienia urządzeń

- Wyłączyłem rozwiązywanie nazw domenowych.
no ip domain lookup (R1, R2, R3, S1, S2)
- Przypisałem nazwy urządzeniom.
hostname (R1/R2/R3/S1/S2)
- Zaszyfrowałem hasła zapisane jawnym tekstem.
service password-encryption (R1, R2, R3, S1, S2)
- Przypisałem 'Cisco123' jako zaszyfrowane hasło trybu uprzywilejowanego EXEC.
enable secret Cisco123 (R1, R2, R3, S1, S2)
- Jako hasło do konsoli i vty ustawiłem 'Cisco' i włączyłem logowanie .
line con 0
password Cisco
login
line vty 0 15
password Cisco
login
(R1, R2, R3, S1, S2)
- Utworzyłem baner MOTD.
banner motd #Unauthorized Access is Prohibited# (R1, R2, R3, S1, S2)
- Skonfigurowałem adresy IP dla interfejsów zgodnie z tabelą adresacji. Dla wszystkich interfejsów szeregowych DCE ustawiłem taktowanie na 2000000.
- Wyłączyłem nieurzywane porty.
- Zapisałem konfigurację.
copy running-config startup-config (R1, R2, R3, S1, S2)

Część 2: Konfiguracja OSPF

Rozpocząłem konfigurację sieci od lewej strony (S1, R1, R2), aby sprawdzić poprawność połączeń między nimi i upewnić się, że komunikacja w sieci działa zgodnie z założeniami.

Krok 1: Włączenie OSPF na routerach

- Na routerze R1:
router ospf 1
router-id 1.1.1.1
network 203.0.113.0 0.0.0.3 area 0
network 172.16.0.0 0.0.1.255 area 0

- Na routerze R2:
`router ospf 1`
`router-id 2.2.2.2`
`network 203.0.113.0 0.0.0.3 area 0`

Krok 2: Uwierzelnianie OSPF za pomocą MD5

Na routerze R1:

```
interface s0/1/0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 Cisco12345
```

Krok 3: Weryfikacja OSPF

- Sprawdziłem przyległości OSPF
`show ip ospf neighbor`
- Zweryfikołem ustawienia protokołu OSPF
`show ip protocols`

Część 3: Konfiguracja DHCP

Krok 1: Konfiguracja serwera DHCP na R1

- Na routerze R1:
`ip dhcp excluded-address 172.16.1.254 172.16.1.253`
`ip dhcp pool S1-POOL`
`network 172.16.0.0 255.255.254.0`
`default-router 172.16.1.254`

Krok 2: Weryfikacja DHCP

Na hostach zmieniłem tryb otrzymania adresu IP na tryb DHCP

PC -> Desktop -> IP Configuration -> DHCP

Część 4: Konfiguracja przełączników

Krok 1: Konfiguracja portów

- Na przełączniku S1:
`interface f0/6`
`switchport mode access`
`interface f0/8`
`switchport mode access`
`interface f0/20`
`switchport mode trunk`

Część 5: Weryfikacja łączności

Z komputerów zrobiłem ping na każdy interfejs po lewej stronie. Weryfikacja powiodła się sukcesem.

Na tym etapie konfiguracja miała na celu konfigurację po lewej stronie. Poprawne działanie tej konfiguracji zostało potwierdzone, przechodzimy do prawej strony (R2, R3, S2).

Część 6: Konfiguracja OSPF

Krok 1: Włączenie OSPF na R3

- Na routerze R3:
`router ospf 1`
`router-id 3.3.3.3`
`network 198.51.100.0 0.0.0.3 area 0`
`network 192.168.128.0 0.0.31.255 area 0`

Krok 2: Na R2 dodałem sieć do OSPF

- Na routerze R2:
`network 198.51.100.0 0.0.0.3 area 0`

Krok 3: Uwierzelnianie OSPF za pomocą MD5

- Na routerze R2:
`interface s0/1/1`
`ip ospf authentication message-digest`
`ip ospf message-digest-key 1 md5 Cisco12345`

Krok 4: Weryfikacja OSPF

- Sprawdziłem przyległości OSPF
`show ip ospf neighbor`
- Zweryfikołem ustawienia protokołu OSPF
`show ip protocols`

Część 6: Konfiguracja DHCP

Krok 1: Konfiguracja serwera DHCP na R3

- Na routerze R3:
`ip dhcp excluded-address 192.168.159.254 192.168.159.253`
`ip dhcp pool S2-POOL`
`network 192.168.128.0 255.255.224.0`
`default-router 192.168.159.254`

Krok 2: Weryfikacja DHCP

Na hostach zmieniłem tryb otrzymania adresu IP na tryb DHCP
 PC -> Desktop -> IP Configuration -> DHCP

Część 7: Konfiguracja przełączników

Krok 1: Konfiguracja portów

- Na przełączniku S2:
`interface f0/22`
`switchport mode access`
`interface f0/23`
`switchport mode access`
`interface f0/24`
`switchport mode access`
`interface f0/20`
`switchport mode trunk`

Część 8: Weryfikacja łączności

Weryfikacja powiodła się sukcesem.

Omówienie konfiguracji

Na przełączniku **S1** skonfigurowano interfejs VLAN 1 i przypisano mu adres IP 172.16.1.253 z maską 255.255.254.0 (/23). Adres 172.16.1.253 należy do klasy adresów prywatnych z zakresu 172.16.0.0 - 172.31.255.255 i został wybrany z podsieci o maskowaniu /23, które pozwala na obsługę 510 hostów w jednej podsieci. Maskę 255.255.254.0 zapewnia 9 bitów dostępnych na adresowanie hostów, co oznacza, że liczba dostępnych adresów wynosi $2^9 - 2 = 510$ (z czego dwa adresy są zarezerwowane: jeden na adres sieciowy, drugi na adres rozgłoszeniowy). W przypadku tej podsieci zakres adresów wynosi od 172.16.0.1 do 172.16.1.254, gdzie 172.16.0.0 to adres sieciowy, a 172.16.1.255 to adres rozgłoszeniowy. Wymagania projektu, zakładające obsługę 500 hostów w tej sieci, zostały spełnione, ponieważ adresacja /23 oferuje wystarczającą liczbę adresów IP.

Na przełączniku **S2** skonfigurowano interfejs VLAN 1, któremu przypisano adres IP 192.168.159.253 z maską 255.255.224.0 (/19). Adres 192.168.159.253 jest ostatnim dostępnym adresem w podsieci. Maskę /19 oznacza, że pierwsze 19 bitów adresu IP są zarezerwowane na identyfikację sieci, a pozostałe 13 bitów służą do adresowania hostów. Taki podział pozwala na utworzenie podsieci z $2^{13} = 8192$ adresami, z których 8190 może być używane przez hosty (po odjęciu adresu sieciowego i adresu rozgłoszeniowego). W przypadku tej podsieci zakres adresów wynosi od 192.168.128.1 do 192.168.159.254, gdzie 192.168.128.0 to adres sieciowy, a 192.168.159.255 to adres rozgłoszeniowy. Sieć lokalna przełącznika S2 wymaga adresacji dla 5000 hostów, co oznacza, że minimalna liczba adresów IP musi być równa lub większa od 5000. Maskę /19, oferującą 8190 adresów hostów, w pełni spełnia te wymagania, zapewniając także odpowiedni zapas na przyszłą rozbudowę. Mniejsza maska, taka jak /20 (obsługująca tylko 4094 hosty), nie byłaby wystarczająca.

Na routerze **R1** skonfigurowano interfejsy sieciowe, serwer DHCP, routing OSPF oraz zabezpieczenia, co umożliwia pełną funkcjonalność w sieci. Interfejs GigabitEthernet0/0 został przypisany do sieci lokalnej 172.16.0.0/23 z adresem 172.16.1.254, który pełni rolę bramy domyślnej dla urządzeń w sieci LAN. Interfejs Serial0/1/0 skonfigurowano z adresem 203.0.113.1/30, należącym do sieci publicznej łączącej routery R1 i R2. Router pełni również funkcję serwera DHCP dla sieci 172.16.0.0/23. Wykluczono adresy 172.16.1.254 (brama domyślna) i 172.16.1.253 (adres przełącznika S1), aby zapobiec ich przydzieleniu hostom. Utworzono pulę DHCP o nazwie S1-POOL, która przydziela adresy hostom w zakresie od 172.16.0.1 do 172.16.1.252. Brama domyślna dla tych hostów została ustawiona na 172.16.1.254.

Na routerze **R3** skonfigurowano interfejsy sieciowe, serwer DHCP, routing OSPF oraz zabezpieczenia, aby zapewnić pełną funkcjonalność w sieci. Interfejs GigabitEthernet0/0 został przypisany do sieci lokalnej 192.168.128.0/19 z adresem 192.168.159.254, który pełni rolę bramy domyślnej dla urządzeń w sieci LAN. Dla połączenia punkt-punkt z routerem R2 skonfigurowano interfejs Serial0/1/1, przypisując mu adres 198.51.100.2/30, który należy do sieci publicznej. Router R3 pełni funkcję serwera DHCP dla sieci lokalnej 192.168.128.0/19. Wykluczono adresy 192.168.159.254 (brama domyślna) i 192.168.159.253 (adres przełącznika S2), aby uniknąć ich przydzielenia hostom. Utworzono pulę DHCP o nazwie S2-POOL, która przydziela adresy hostom w zakresie 192.168.128.1 – 192.168.159.252. Brama domyślna dla tych hostów została ustawiona na 192.168.159.254.

Na routerze **R2** skonfigurowano interfejsy Serial0/1/0 oraz Serial0/1/1, które łączą router R2 odpowiednio z routerem R1 i R3, oraz włączono routing OSPF. Konfiguracja została przeprowadzona w dwóch etapach, obejmujących połączenie punkt-punkt z routerem R1 oraz konfigurację z routerem R3, przy czym każda z nich uwzględnia odpowiednią adresację. Interfejs Serial0/1/0 został przypisany

do sieci 203.0.113.0/30. Przypisano adres IP 203.0.113.2 z maską 255.255.255.252 (/30), co pozwala na efektywne wykorzystanie adresów IP w tej sieci. Maską /30 zapewnia cztery adresy w podsieci: 203.0.113.1 dla routera R1 oraz 203.0.113.2 dla routera R2. Adres 203.0.113.0 to adres sieciowy, a 203.0.113.3 to adres rozgłoszeniowy. Interfejs Serial0/1/1 został przypisany do sieci 198.51.100.0/30. Przypisano adres IP 198.51.100.1 z maską 255.255.255.252 (/30), co pozwala na efektywne wykorzystanie przestrzeni adresowej przy minimalnym marnotrawstwie. Maską /30 zapewnia 4 adresy w podsieci: 198.51.100.2 dla routera R3 oraz 198.51.100.1 dla routera R2. Adres 198.51.100.0 to adres sieciowy, a 198.51.100.3 to adres rozgłoszeniowy.

Konfiguracja urządzeń (show run)

S1

```
S1#show run
Building configuration...

Current configuration : 1587 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERn$RldxcCZEZsTFTETUyRaA50
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
shutdown
!
```



```
interface FastEthernet0/6
switchport mode access
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
switchport mode access
!
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
switchport mode trunk
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
```

```

interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
ip address 172.16.1.253 255.255.254.0
!
banner motd ^CUnauthorized Access is Prohibited^C
!
!
!
line con 0
password 7 0802455D0A16
login
!
line vty 0 4
password 7 0802455D0A16
login
line vty 5 15
password 7 0802455D0A16
login
!
!
!
!
End

```

S2

```

S2#show run
Building configuration...

```

```

Current configuration : 1604 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S2
!
enable secret 5 $1$mERr$RldxcCZEZsTFTETUyRaA50
!
!

```

```
!  
no ip domain-lookup  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
interface FastEthernet0/1  
shutdown  
!  
interface FastEthernet0/2  
shutdown  
!  
interface FastEthernet0/3  
shutdown  
!  
interface FastEthernet0/4  
shutdown  
!  
interface FastEthernet0/5  
shutdown  
!  
interface FastEthernet0/6  
shutdown  
!  
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
switchport mode trunk
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
switchport mode access
!
interface FastEthernet0/23
switchport mode access
!
interface FastEthernet0/24
switchport mode access
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
ip address 192.168.159.253 255.255.224.0
!
banner motd ^CUnauthorized Access is Prohibited^C
!
!
!
line con 0
password 7 0802455D0A16
login
!
line vty 0 4
password 7 0802455D0A16
login
line vty 5 15
password 7 0802455D0A16

```

```
login
!  
!  
!  
!  
end
```

R1

```
R1#show run
Building configuration...

Current configuration : 1709 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$RldxcCZEZsTFTETUyRaA50
!
!
ip dhcp excluded-address 172.16.1.254 172.16.1.253
!
ip dhcp pool S1-POOL
network 172.16.0.0 255.255.254.0
default-router 172.16.1.254
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISC02901/K9 sn FTX15245R3V-
!
!
!
!
!
!
!
!
no ip domain-lookup
```

```

!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 172.16.1.254 255.255.254.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/0
ip address 203.0.113.1 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 Cisco12345
clock rate 2000000
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2/1
no ip address
clock rate 2000000
shutdown
!

```

```

interface Serial0/3/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 203.0.113.0 0.0.0.3 area 0
network 172.16.0.0 0.0.1.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CUnauthorized Access is Prohibited^C
!
!
!
!
line con 0
password 7 0802455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0802455D0A16
login
!
!
!
end

```

R2

```

R2#show run
Building configuration...

```

```

Current configuration : 1640 bytes

```

```

!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2
!
!
!
enable secret 5 $1$mERn$RldxcCZEZsTFTETUyRaA50
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISC02901/K9 sn FTX1524ZRH0-
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address

```



```
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/0
ip address 203.0.113.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 Cisco12345
!
interface Serial0/1/1
ip address 198.51.100.1 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 Cisco12345
clock rate 2000000
!
interface Serial0/2/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 2.2.2.2
```

```

log-adjacency-changes
network 203.0.113.0 0.0.0.3 area 0
network 198.51.100.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CUnauthorized Access is Prohibited^C
!
!
!
!
line con 0
password 7 0802455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0802455D0A16
login
!
!
!
end

```

R3

```

R3#show run
Building configuration...

Current configuration : 1710 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3
!
!
!
enable secret 5 $1$mERn$RldxcCZEZsTFTETUyRaA50
!
!
ip dhcp excluded-address 192.168.159.254 192.168.159.253
!
ip dhcp pool S2-POOL

```

```

network 192.168.128.0 255.255.224.0
default-router 192.168.159.254
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISC02901/K9 sn FTX15249PK3-
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 192.168.159.254 255.255.224.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown

```

```

!
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/1
ip address 198.51.100.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 Cisco12345
!
interface Serial0/2/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2/1
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
network 198.51.100.0 0.0.0.3 area 0
network 192.168.128.0 0.0.31.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CUnauthorized Access is Prohibited^C
!
!
!

```

```
!  
line con 0  
password 7 0802455D0A16  
login  
!  
line aux 0  
!  
line vty 0 4  
password 7 0802455D0A16  
login  
!  
!  
!  
end
```

Wnioski

Realizacja projektu umożliwiła praktyczne zastosowanie wiedzy teoretycznej z zakresu projektowania i konfiguracji sieci komputerowych, a także pozwoliła na doskonalenie umiejętności w obsłudze urządzeń sieciowych, takich jak routery i przełączniki. W efekcie powstała w pełni funkcjonalna sieć spełniająca założenia projektowe, w tym obsługująca dwa segmenty lokalne – jeden przeznaczony dla 500 hostów, a drugi dla 5000 hostów. Projekt zakładał zastosowanie dynamicznego routingu OSPF z uwierzytelnianiem MD5, co zapewnia bezpieczeństwo wymiany informacji o trasach, oraz wdrożenie serwerów DHCP w celu automatycznego przydzielania adresów IP w obu segmentach sieci.

W trakcie pracy napotkałem pewne trudności związane z konfiguracją urządzeń sieciowych. Jednym z głównych problemów było poprawne działanie serwera DHCP na przełączniku S2, gdzie początkowo hosty nie otrzymywały adresów IP, co wynikało z nieprawidłowej konfiguracji portów. Problem został rozwiązany poprzez ustawienie portów w trybie access i przypisanie ich do odpowiedniego VLAN-u. Kolejną trudnością było zestawienie połączenia między routerami R2 i R3, gdzie konieczne było poprawne skonfigurowanie protokołu OSPF z uwierzytelnianiem MD5. Nieprawidłowo skonfigurowane hasło MD5 na jednym z routerów powodowało brak sąsiedztwa OSPF, co udało się naprawić po analizie konfiguracji.

Ważnym aspektem projektu było dobranie odpowiedniej adresacji IP, uwzględniającej wymagania dotyczące liczby hostów. W pierwszym segmencie zastosowano maskę 255.255.254.0 (/23), która umożliwia adresowanie 510 hostów, co w pełni spełnia wymagania obsługi 500 hostów. W drugim segmencie wykorzystano maskę 255.255.224.0 (/19), która zapewnia 8190 adresów, umożliwiając obsługę 5000 hostów z dużym zapasem na przyszłą rozbudowę sieci.

Podczas konfiguracji routerów szczególną uwagę poświęcono implementacji dynamicznego routingu OSPF. Uwierzytelnianie MD5 w tym protokole okazało się skutecznym zabezpieczeniem przed nieautoryzowanymi modyfikacjami tras w sieci. Testy łączności między urządzeniami potwierdziły poprawność konfiguracji i wydajność zaprojektowanej sieci.

Realizacja projektu pozwoliła również na zrozumienie znaczenia organizacji pracy i systematycznego podejścia do rozwiązywania problemów. Analiza konfiguracji i dokładne sprawdzanie błędów w poszczególnych etapach okazały się kluczowe dla osiągnięcia poprawnych wyników. Zastosowanie wykresu Gantta umożliwiło przejrzyste zarządzanie harmonogramem projektu oraz lepszą organizację czasu pracy.

Podsumowując, projekt spełnił wszystkie założenia, a wynikowa sieć jest funkcjonalna, skalowalna i zgodna z wymaganiami. Trudności napotkane w trakcie realizacji projektu pozwoliły na lepsze zrozumienie zagadnień związanych z konfiguracją sieci i rozwiązywaniem problemów, co przyczyniło się do poszerzenia praktycznej wiedzy w tym obszarze.