

ROUTER

a. Połącz się z ruterem konsolowo i przejdź do trybu uprzywilejowanego.

```
Router> enable
```

```
Router#
```

b. Ustaw właściwy czas na routerze.

```
Router# clock set 10:40:30 6 February 2013
```

```
Router#
```

c. Przejdź do trybu konfiguracji globalnej.

```
Router# config t
```

```
Router(config)#
```

1) Skonfiguruj nazwę hosta na routerze zgodną z przyjętą topologią i Tabelą adresacji.

```
Router(config)# hostname R1
```

```
R1(config)#
```

2) Wyłącz wyszukiwanie DNS.

```
R1(config)# no ip domain-lookup
```

3) Utwórz komunikat dnia (MOTD banner), który będzie ostrzegał przed nieautoryzowanym dostępem do urządzenia.

```
R1(config)# banner motd #Uwaga! Nieautoryzowany dostep zabroniony.#
```

4) Ustaw szyfrowane hasło class na dostępie do trybu uprzywilejowanego.

```
R1(config)# enable secret class
```

5) Ustaw hasło dostępu konsolowego cisco i uaktywnij dostęp do logowania na konsolę.

```
R1(config)# line con 0
```

```
R1(config-line)# password cisco
```

```
R1(config-line)# login
```

6) Włącz szyfrowanie haseł jawnych.

```
R1(config)# service password-encryption
```

7) Utwórz domenę o nazwie cisco.com dla dostępu SSH. Lab – Korzystanie z interfejsu CLI do zbierania informacji o urządzeniach i topologii sieci

```
R1(config)# ip domain-name cisco.com
```

8) Utwórz użytkownika o nazwie admin z szyfrowanym hasłem cisco na dostępie SSH.

```
R1(config)# username admin secret cisco
```

9) Wygeneruj klucz RSA o długości 1024 bitów.

```
R1(config)# crypto key generate rsa modulus 1024
```

d. Skonfiguruj linie terminalowe vty.

1) Użyj lokalnej bazy danych do uwierzytelniania na dostępie SSH.

```
R1(config)# line vty 0 4
```

R1(config-line)# login local

2) Włącz tylko tryb logowania SSH.

R1(config-line)# transport input ssh

e. Powrót do trybu konfiguracji globalnej.

R1(config-line)# exit

1) Utwórz interfejs Loopback 0 i skonfiguruj adres IP bazując na Tabeli adresacji.

R1(config)# interface loopback 0

R1(config-if)# ip address 209.165.200.225 255.255.255.224

2) Skonfiguruj i uaktywnij interfejs G0/1 routera.

R1(config-if)# int g0/1

R1(config-if)# ip address 192.168.1.1 255.255.255.0

R1(config-if)# no shut

3) Skonfiguruj opisy interfejsów G0/1 i L0.

R1(config-if)# description Łacze do LAN

R1(config-if)# int lo0

R1(config-if)# description Emulacja łącza do ISP

4) Zapisz plik konfiguracji bieżącej do pliku konfiguracji startowej.

R1(config-if)# end

R1# copy run start

konfiguracja adresu IPv6

Przypisz adresy IPv6 do interfejsów sieciowych na R1.

a. Przypisz globalne adresy unicastowe IPv6, zgodne z Tabelą Adresacji, do obu interfejsów Ethernet na R1.

R1(config)# interface g0/0

R1(config-if)# ipv6 address 2001:db8:acad:a::1/64

R1(config-if)# no shutdown

R1(config-if)# interface g0/1

R1(config-if)# ipv6 address 2001:db8:acad:1::1/64

R1(config-if)# no shutdown

R1(config-if)# end

R1#

b. Wyдай komendę show ipv6 interface brief, aby zweryfikować prawidłowość ustawionych adresów IPv6 na obu interfejsach.

R1# show ipv6 interface brief

W celu dopasowania adresu lokalnego dla łącza do adresu unicastowego danego interfejsu, wpisz

ręcznie adresy lokalne dla łącza na każdym z interfejsów Ethernet w R1.

```
R1# config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)# interface g0/0
```

```
R1(config-if)# ipv6 address fe80::1 link-local
```

```
R1(config-if)# interface g0/1
```

```
R1(config-if)# ipv6 address fe80::1 link-local
```

```
R1(config-if)# end
```

```
R1#
```

Uwaga: Każdy interfejs routera należy do oddzielnej sieci. Pakiety posiadające adres lokalny dla łącza nigdy nie opuszczają sieci lokalnej; dlatego, można używać tego samego adresu lokalnego dla łącza na obu interfejsach.

e. Ponownie wydaj komendę show ipv6 interface g0/0. Zauważ, że adres lokalny dla łącza został zmieniony na FE80::1 oraz że tym razem lista zawiera tylko jedną grupę multicastową Solicited Nodes.

```
R1# show ipv6 interface g0/0
```

Uruchom routing IPv6 na R1 używając komendy IPv6 unicast-routing.

```
R1 # configure terminal
```

```
R1(config)# ipv6 unicast-routing
```

```
R1(config)# exit
```

```
R1#
```

Switch

a. Połącz się z przełącznikiem konsolowo i przejdź do trybu uprzywilejowanego.

```
Switch> enable
```

```
Switch#
```

b. Ustaw właściwy czas na przełączniku.

```
Switch# clock set 10:52:30 6 February 2013
```

c. Przejdź do trybu konfiguracji globalnej.

```
Switch# config t
```

5) Skonfiguruj nazwę hosta na przełączniku zgodną z przyjętą topologią i Tabelą adresacji.

```
Switch(config)# hostname S1
```

6) Wyłącz wyszukiwanie DNS. Lab – Korzystanie z interfejsu CLI do zbierania informacji o urządzeniach i topologii sieci

```
S1(config)# no ip domain-lookup
```

7) Utwórz komunikat dnia (MOTD banner), który będzie ostrzegał przed nieautoryzowanym dostępem do urządzenia

S1(config)# banner motd #Uwaga! Nieautoryzowany dostep zabroniony.#

8) Ustaw szyfrowane hasło class na dostępie do trybu uprzywilejowanego.

S1(config)# enable secret class

9) Włącz szyfrowanie haseł jawnych.

S1(config)# service password-encryption

10) Utwórz domenę o nazwie cisco.com dla dostępu SSH.

S1(config)# ip domain-name cisco.com

11) Utwórz użytkownika o nazwie admin z szyfrowanym hasłem cisco na dostępie SSH.

S1(config)# username admin secret cisco

12) Wygeneruj klucz RSA o długości 1024 bitów.

S1(config)# crypto key generate rsa modulus 1024

13) Skonfiguruj adres IP przełącznika bazując na topologii i Tabeli adresacji.

S1(config)# interface vlan 1

S1(config-if)# ip address 192.168.1.11 255.255.255.0

S1(config-if)# no shut

14) Ustaw bramę domyślną na przełączniku.

S1(config)# ip default-gateway 192.168.1.1

15) Ustaw hasło dostępu konsolowego cisco i uaktywnij dostęp do logowania na konsolę.

S1(config-if)# line con 0

S1(config-line)# password cisco

S1(config-line)# login

c. Skonfiguruj linie terminalowe vty.

1) Użyj lokalnej bazy danych do uwierzytelniania na dostępie SSH.

S1(config-line)# line vty 0 15

S1(config-line)# login local

2) Włącz tylko tryb logowania SSH.

S1(config-line)# transport input ssh

3) Wejdź w odpowiedni tryb konfiguracji i skonfiguruj opisy interfejsów F0/5 i F0/6.

S1(config-line)# int f0/5

S1(config-if)# description Polaczenie do R1

S1(config-if)# int f0/6

S1(config-if)# description Polaczenie do PC-A

4) Zapisz plik konfiguracji bieżącej do pliku konfiguracji startowej.

S1(config-if)# end

S1# copy run start

Wyznaczanie adresu rozgłoszeniowego (broadcast), adresu sieci i liczby hostów w sieci.

Dany jest adres IP: 148.27.232.140 i maska podsieci: 255.255.192.0

Krok 1: Zamieniamy adres IP i maskę na system binarny, otrzymujemy:

148.27.232.140 - 10010100.00011011.11101000.10001100

255.255.192.0 - 11111111.11111111.11000000.00000000 (zapisujemy w układzie 4 razy po 8 liczb - 4 oktety 8 bitowe co daje nam liczbę 32 bitową)

Liczba 27 w systemie binarnym to 11011 w celu zapisu dopełniamy 0 do 8 liczb i otrzymujemy 00011011

Wyznaczamy adres sieci:

148.27.232.140 - 10010100.00011011.11101000.10001100

255.255.192.0 - 11111111.11111111.11000000.00000000

Do adresu sieci jest używanych 18 bitów (dlatego że w masce jest użytych 18 liczb 1)

Porównujemy adres IP z maską tam gdzie w masce 1 to przepisujemy z adresu bez zmian resztę dopełniamy 0 i otrzymujemy:

10010100.00011011.11000000.00000000 co w przeliczeniu na system dziesiętny daje nam: 148.27.192.0 - adres sieci

Wyznaczamy broadcast:

148.27.232.140 - 10010100.00011011.11101000.10001100

255.255.192.0 - 11111111.11111111.11000000.00000000

Porównujemy adres IP z maską tam gdzie w masce 1 to przepisujemy z adresu bez zmian a gdzie w masce 0 wpisujemy 1 i otrzymujemy: 10010100.00011011.11111111.11111111 co w przeliczeniu na system dziesiętny daje nam:

148.27.255.255 - adres rozgłoszeniowy

Wyznaczamy liczbę hostów:

Host minimalny: 148.27.192.1 (adres sieci + 1)

Host maksymalny: 148.27.255.254 (adres rozgłoszeniowy - 1)

Co daje nam liczbę hostów:

148.27.192.1 : 148.27.192.255 = liczba hostów 255

148.27.193.0 : 148.27.254.255 = liczba hostów 256 (liczba hostów w sieci o zakresie od 148.27.193.0 do

148.27.193.255) * 62 (liczba pełnych sieci od 193 do 254) równa się 15872 hostów.

148.27.255.0 : 148.27.255.254 = liczba hostów 255

Co po sumowaniu $255 + 15872 + 255 = 16382$ hostów