Politechnika Świętokrzyska w Kielcach

Wydział Zarządzania i Modelowania Komputerowego

Sieci Komputerowe

Laboratorium

Konfigurowanie dostępu do urządzeń sieciowych za pomocą SSH

Politechnika Świętokrzyska
Kielce University of Technology

Przygotowali:

Imię i Nazwisko	Nr albumu
Radosław Kulig	093795
Katarzyna Nowakowska	096946

Kierunek: Inżynieria Danych

Studia: stacjonarne

Data wykonania ćwiczenia: 18.01.2026

Oświadczam, że:

Sprawozdanie niniejsze zostało wykonane przeze mnie osobiście. Zamieszczone w sprawozdaniu wyniki badań zostały uzyskane przeze mnie podczas wykonywania zadań laboratoryjnych.
Radosław Kulig
Katarzyna Nowakowska

Lab 16.4.7 Odczytywanie adresów MAC urządzeń sieciowych

Wstęp teoretyczny

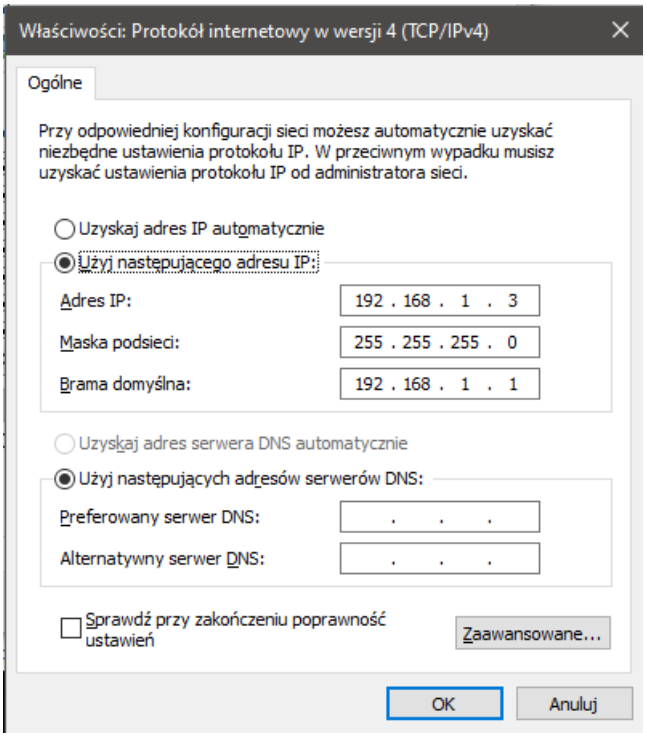
Zdalne zarządzanie urządzeniami sieciowymi jest kluczowym elementem administracji sieci komputerowych. W przeszłości powszechnie stosowany protokół Telnet umożliwiał zdalny dostęp do routerów i przełączników, jednak nie zapewniał on szyfrowania przesyłanych danych, co narażało hasła oraz konfigurację urządzeń na przechwycenie. Rozwiązaniem tego problemu jest protokół Secure Shell (SSH), który umożliwia bezpieczne zestawienie połączenia dzięki szyfrowaniu transmisji oraz mechanizmom uwierzytelniania użytkownika i urządzenia. W ramach ćwiczenia skonfigurowano podstawowe parametry routera i przełącznika Cisco oraz uruchomiono usługę SSH, co pozwoliło na bezpieczny zdalny dostęp do urządzeń sieciowych w lokalnej sieci IP.

Konfiguracja routera

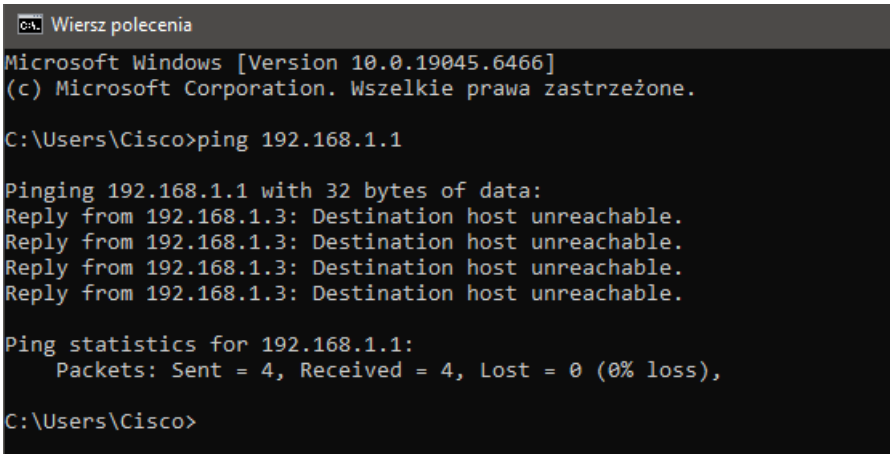
Ustalamy hasła, baner i konfigurujemy interface G0/1 routera.

```
Router>enable
Router#configre terminal
                ^
% Invalid input detected at '^' marker.

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#enable secret class
Router(config)#line console 0
Router(config-line)#passuord cisco
Router(config-line)#login
Router(config-line)#eit
                    ^
% Invalid input detected at '^' marker.

Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#passuord cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#service passuord-encryption
Router(config)#banner motd $ Authorized Users Only! $
Router(config)#interface g0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
*Mar 25 17:51:38.023: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
*Mar 25 17:51:41.107: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Mar 25 17:51:42.107: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

Konfiguracja PC-A.



Sprawdzamy połączenie sieci.



Ping nie powiódł się ponieważ przełącznik nie jest jeszcze skonfigurowany ani topologia nie jest odwzorowana.

Konfigurujemy dostęp do routera przez SSH.
Ustalamy nazwę urządzenia, domenę, generujemy klucz szyfrowania oraz nazwę i hasło użytkownika. Włączamy Telnet oraz SSH na liniach wejściowych VTY.

```
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

R1(config)#
*Mar 25 17:56:07.731: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#username admin secret Adm1nP@55
R1(config)#line vty 0 4
R1(config-line)#transport input telnet ssh
R1(config-line)#login local
R1(config-line)#end
R1#
*Mar 25 17:58:12.783: %SYS-5-CONFIG_I: Configured from console by console
```

Nie jesteśmy jeszcze w stanie ustanowić połączenia SSH do routera ponieważ przechodzi ono przez nieskonfigurowany jeszcze przełącznik.

Konfiguracja przełącznika

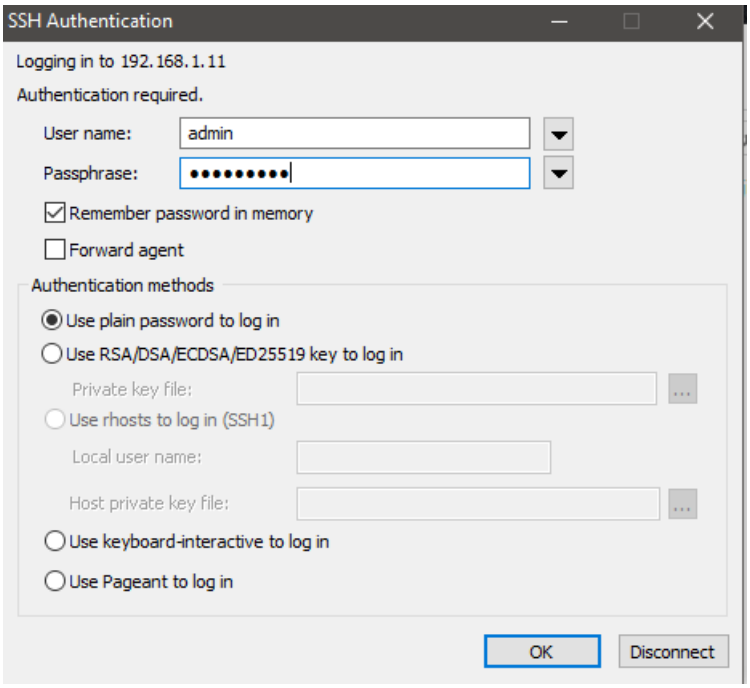
Konfigurujemy podstawowe ustawienia przełącznika.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#enable secret class
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#service password-encryption
Switch(config)#banner motd $ Authorized Users Only! $
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.11 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#
*Mar  1 00:36:20.459: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar  1 00:36:20.467: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

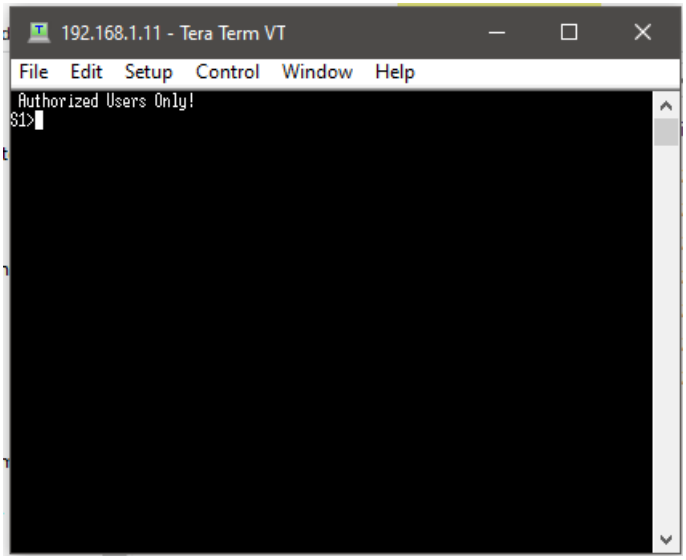
Konfigurujemy przełącznik dla połączeń poprzez SSH.

```
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#crypto key generate rsa modulus 1024
                                   ^
% Invalid input detected at '^' marker.

S1(config)#crypto key generate rsa modulus 1024
                                   ^
% Invalid input detected at '^' marker.

S1(config)#crypto key generate rsa modulus 1024
                                   ^
% Invalid input detected at '^' marker.

S1(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: modulus 1024
% A decimal number between 360 and 2048.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar  1 00:40:15.877: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#username admin secret Adm1nP@55
S1(config)#line vty 0 15
S1(config-line)#transport input telnet ssh
S1(config-line)#login local
S1(config-line)#end
S1#
*Mar  1 00:41:39.712: %SYS-5-CONFIG_I: Configured from console by console
```

Ustawiamy połączenie SSH do przełącznika.

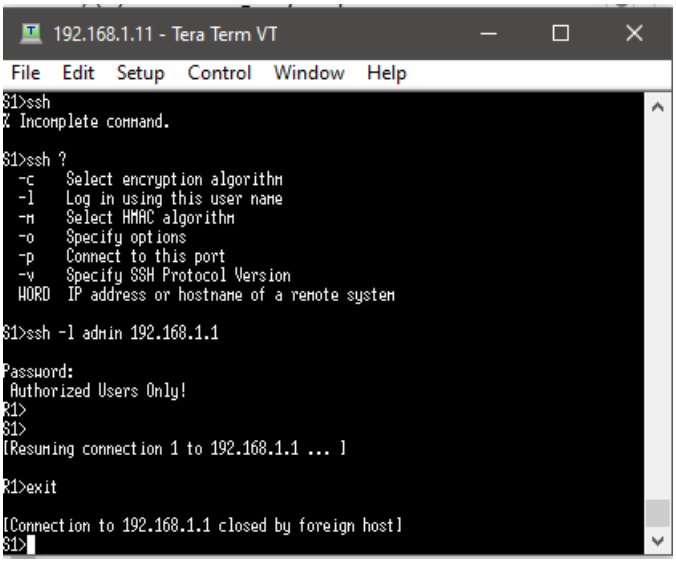


Udało się ustanowić sesję SSH.



Uruchamianie SSH z linii poleceń CLI w przełączniku

Wyświetlamy opcje parametrów polecenia ssh i łączymy się przez SSH z R1.
Przełączamy się między S1 a R1 bez zamykania sesji SSH za pomocą kombinacji klawiszy *Crtl+Shift+6*.



Wnioski

Podczas realizacji ćwiczenia zapoznano się z zasadami bezpiecznego zdalnego zarządzania urządzeniami sieciowymi z wykorzystaniem protokołu SSH. Przeprowadzona konfiguracja routera oraz przełącznika Cisco pozwoliła na zrozumienie znaczenia poprawnych ustawień podstawowych, takich jak adresacja IP, hasła dostępu, banery informacyjne oraz konfiguracja linii VTY. Wykazano, że brak pełnej konfiguracji wszystkich elementów topologii uniemożliwia poprawną komunikację w sieci, co potwierdziły początkowe nieudane próby połączeń. Po prawidłowym skonfigurowaniu przełącznika możliwe było ustanowienie bezpiecznej sesji SSH zarówno z komputera PC, jak i bezpośrednio z poziomu CLI przełącznika. Ćwiczenie potwierdziło przewagę protokołu SSH nad Telnetem w kontekście bezpieczeństwa transmisji oraz podkreśliło jego kluczową rolę w administracji nowoczesnych sieci komputerowych.