Ćwiczenie – Konfiguracja aspektów bezpieczeństwa przełącznika

1. Topologia



1. Tabela adresacji

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Urządzenie | Interfejs | Adres IP | Maska podsieci | Brama domyślna |
| R1 | G0/1 | 172.16.99.1 | 255.255.255.0 | N/A |
| S1 | VLAN 99 | 172.16.99.11 | 255.255.255.0 | 172.16.99.1 |
| PC-A | NIC | 172.16.99.3 | 255.255.255.0 | 172.16.99.1 |

1. Cele nauczania

Część 1: Budowa sieci oraz inicjalizacja urządzeń

Część 2: Konfiguracja podstawowych ustawień urządzeń oraz weryfikacja łączności

Część 3: Konfiguracja i weryfikacja protokołu SSH na przełączniku S1

* Konfiguracja dostępu przy użyciu SSH.
* Modyfikacja parametrów protokołu SSH.
* Weryfikacja konfiguracji SSH.

Część 4: Konfiguracja i weryfikacja aspektów bezpieczeństwa na przełączniku S1

* Konfiguracja i weryfikacja ogólnych aspektów bezpieczeństwa.
* Konfiguracja i weryfikacja bezpieczeństwa portów przełącznika.
1. Wprowadzenie

Powszechną praktyką jest ograniczanie dostępu oraz instalacja aplikacji zwiększających bezpieczeństwo na komputerach i serwerach. Ważne jest, aby urządzenia sieciowe np. przełączniki czy routery również zostały odpowiednio zabezpieczone.

Na tym laboratorium zapoznasz się z konfiguracją aspektów bezpieczeństwa na przełącznikach. Skonfigurujesz połączenie SSH oraz zabezpieczysz sesję HTTPS. Skonfigurujesz również i zweryfikujesz zabezpieczenia na portach przełącznika, aby zablokować urządzenia, których adres MAC jest nieznany.

**Uwaga**: Preferowane routery to model Cisco 1941 Integrated Services Router (ISR) z systemem Cisco IOS Release 15.2(4)M3 (universalk9 image), natomiast przełączniki to model Cisco Catalyst 2960s z systemem Cisco IOS Release 15.0(2) (lanbasek9 image). Inne urządzenia i systemy mogą być również używane. W zależności od modelu i wersji IOS dostępne komendy mogą się różnić od prezentowanych w instrukcji.

**Uwaga**: Upewnij się, że startowa konfiguracja przełączników została skasowana. Jeśli nie jesteś pewny, poproś o pomoc prowadzącego.

1. Wymagane zasoby
* 1 router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 lub kompatybilny)
* 1 przełącznik (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 lub kompatybilny)
* 1 komputer (Windows 7, Vista, lub XP)
* Kable konsolowe do konfiguracji urządzeń Cisco IOS poprzez porty konsolowe
* Kable sieciowe zgodnie z pokazaną topologią

Część 1: Budowa sieci oraz inicjalizacja urządzeń

W części 1 zestawisz topologię sieciową oraz w razie konieczności skasujesz konfiguracje urządzeń sieciowych.

Krok 1: Okablowanie sieci zgodnie z topologią.

Krok 2: Inicjalizacja i ponowne uruchomienie routera i przełącznika.

Jeżeli na urządzeniach została zapisana wcześniej konfiguracja skasuj ją i uruchom je ponownie.

Część 2: Konfiguracja podstawowych ustawień urządzeń oraz weryfikacja łączności

W części 2 skonfigurujesz podstawowe ustawienia na routerze, przełączniku I komputerze. Adresy IP oraz nazwy urządzeń muszą być zgodne z tabelą adresacji i rysunkiem z pierwszej strony instrukcji.

Krok 1: Konfiguracja adresu IP na komputerze PC-A.

Krok 2: Konfiguracja podstawowych ustawień routera R1.

* + 1. Skonfiguruj nazwę urządzenia.
		2. Wyłącz niepożądane zapytania DNS (DNS lookup).
		3. Skonfiguruj adres IP zgodnie tabelą adresacji.
		4. Ustaw **class** jako hasło do trybu uprzywilejowanego EXEC
		5. Ustaw **cisco** jako hasło do połączeń konsolowych i wirtualnych (console i vty).
		6. Ustaw szyfrowanie haseł.
		7. Zapisz bieżącą konfigurację jako startową.

Krok 3: Konfiguracja podstawowych ustawień przełącznika S1.

Dobrą praktyką jest przypisanie adresu IP zarządzania do interfejsu VLAN innego niż VLAN 1. W tym kroku stworzysz interfejs VLAN 99 i przypiszesz mu adres IP.

* + 1. Skonfiguruj nazwę urządzenia.
		2. Wyłącz niepożądane zapytania DNS (DNS lookup).
		3. Ustaw **class** jako hasło do trybu uprzywilejowanego EXEC
		4. Ustaw **cisco** jako hasło do połączeń konsolowych i wirtualnych (console i vty).
		5. Skonfiguruj bramę domyślną dla S1 używając adresu IP routera R1.
		6. Ustaw szyfrowanie haseł.
		7. Zapisz bieżącą konfigurację jako startową.
		8. Stwórz VLAN 99 nazwij go jako **Management**.

S1(config)# **vlan 99**

S1(config-vlan)# **name Management**

S1(config-vlan)# **exit**

S1(config)#

* + 1. Ustaw adres IP zarzadzania dla VLAN 99 zgodnie z tabelą adresacji oraz włącz interfejs.

S1(config)# **interface vlan 99**

S1(config-if)# **ip address 172.16.99.11 255.255.255.0**

S1(config-if)# **no shutdown**

S1(config-if)# **end**

S1#

* + 1. Wydaj komendę **show vlan** na S1. Jaki jest status VLAN 99? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
		2. Wydaj komendę **show ip interface brief** na S1. Jaki jest status i protokół interfejsu VLAN 99?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dlaczego protokół ma wartość „down”, pomimo wydania komendy **no shutdown**?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Przypisz porty F0/5 i F0/6 do VLAN 99.

S1# **config t**

S1(config)# **interface f0/5**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 99**

S1(config-if)# **interface f0/6**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 99**

S1(config-if)# **end**

* + 1. Wydaj komendę **show ip interface brief** na S1. Jaki jest status i protokół interfejsu VLAN 99? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Uwaga**: Może wystąpić opóźnienie przy zmianie statusu portu.

Krok 4: Weryfikacja łączności pomiędzy urządzeniami.

* + 1. Użyj polecenia ping na PC-A w celu sprawdzenia łączności do R1. Czy wynik polecenia ping był pozytywny? \_\_\_\_\_\_\_\_\_\_\_\_\_\_
		2. Użyj polecenia ping na PC-A w celu sprawdzenia łączności do S1. Czy wynik polecenia ping był pozytywny? \_\_\_\_\_\_\_\_\_\_\_\_\_\_
		3. Użyj polecenia ping na S1 w celu sprawdzenia łączności do R1. Czy wynik polecenia ping był pozytywny? \_\_\_\_\_\_\_\_\_\_\_\_\_\_
		4. Na komputerze PC-A otwórz przeglądarkę internetową i wpisz adres http://172.16.99.11. Jeżeli pojawi się komunikat z prośbą o nazwę użytkownika i hasło, pole nazwa użytkownika pozostaw puste, a jako hasło wpisz **class**. Jeżeli pojawi się komunikat z zapytanie o zabezpieczone połączenie wybierz Nie. Czy uzyskałeś dostęp do interfejsu www przełącznika S1? \_\_\_\_\_\_\_\_\_\_\_\_\_\_
		5. Zamknij przeglądarkę na PC-A.

**Uwaga**: Niezabezpieczony interfejs www na przełączniku jest domyślnie włączony. Powszechną praktyką jest wyłączenie tej usługi jak opisano w części 4.

Część 3: Konfiguracja i weryfikacja protokołu SSH na przełączniku S1

Krok 1: Konfiguracja dostępu SSH na S1.

* + 1. Włączenie SSH na S1. W trybie globalnej konfiguracji utwórz domenę **CCNA-Lab.com**.

S1(config)# **ip domain-name CCNA-Lab.com**

* + 1. Utwórz lokalnego użytkownika dla połączeń SSH. Użytkownik powinien mieć uprawnienia administratora.

**Uwaga**: Użyte tu hasło nie jest silne. Takie powinno być używane tylko do celów dydaktycznych.

S1(config)# **username admin privilege 15 secret sshadmin**

* + 1. Dla interfejsu wirtualnego zezwól tylko na połączenia SSH i ustaw używanie lokalnej bazy danych podczas autentyfikacji użytkownika.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh**

S1(config-line)# **login local**

S1(config-line)# **exit**

* + 1. Wygeneruj klucz RSA o długości 1024 btów.

S1(config)# **crypto key generate rsa modulus 1024**

The name for the keys will be: S1.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)

S1(config)#

S1(config)# **end**

* + 1. Zweryfikuj konfigurację SSH i odpowiedz na pytania.

S1# **show ip ssh**

Jaka jest wersja SSH używana przez przełącznik? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ile jest dozwolonych prób logowania? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jaki jest domyślny czas nieaktywności (timeout) dla SSH? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Krok 2: Modyfikacja połączeń SSH na S1.

Zmodyfikuj domyślną konfigurację SSH.

S1# **config t**

S1(config)# **ip ssh time-out 75**

S1(config)# **ip ssh authentication-retries 2**

Ile jest dozwolonych prób logowania? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jaki jest czas nieaktywności (timeout) dla SSH? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Krok 3: Weryfikacja konfiguracji SSH na S1.

* + 1. Używając klienta SSH na komputerze PC-A (np. Putty), zestaw połączenie SSH do S1. Jeżeli otworzy się okno dotyczące klucza, zaakceptuj je. Zaloguj się używając nazwy **admin** oraz hasła **sshadmin**.

Czy połączenie powiodło się? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Co zostało wyświetlone na przełączniku S1?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Wpisz **exit** i zamknij sesję SSH na S1.

Część 4: Konfiguracja i weryfikacja aspektów bezpieczeństwa na przełączniku S1

W części 4 wyłączysz nieużywane porty oraz niektóre usługi a także skonfigurujesz reguły bezpieczeństwa na portach, bazujące na adresach MAC. Przełączniki mogą być przedmiotem ataków oraz nieautoryzowanego dostępu do portów. Skonfigurujesz liczbę adresów MAC, które może nauczyć się przełącznik i wyłączysz ten port, jeśli ta liczba zostanie przekroczona.

Krok 1: Konfiguracja ogólnych aspektów bezpieczeństwa na S1.

* + 1. Skonfiguruj baner (MOTD) na S1 z odpowiednią wiadomością ostrzegającą.
		2. Wydaj komendę **show ip interface brief** na S1. Które fizyczne porty są włączone (up)?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Wyłącz wszystkie nieużywane porty, użyj komendy **interface range** .

S1(config)# **interface range f0/1 – 4**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **interface range f0/7 – 24**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **interface range g0/1 – 2**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **end**

S1#

* + 1. Wydaj komendę **show ip interface brief** na S1. Jaki jest status portów od F0/1 do F0/4?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Wydaj komendę **show ip http server status**.

Jaki jest status serwera HTTP? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jaki port jest używany przez serwer? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jaki jest status serwera HTTPS? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jaki port jest używany przez serwer HTTPS? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Sesja HTTP wysyła wszystko jawnym tekstem. Wyłącz serwer HTTP na przełączniku.

S1(config)# **no ip http server**

* + 1. Otwórz przeglądarkę internetową na PC-A, i wpisz adres http://172.16.99.11. Jaki jest rezultat?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Na komputerze PC-A wpisz w przeglądarce adres https://172.16.99.11. Zaakceptuj certyfikat. Zaloguj się bez użytkownika i z hasłem **class**. Jaki jest rezultat?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Zamknij przeglądarkę na PC-A.

Krok 2: Konfiguracja i weryfikacja bezpieczeństwa portu na S1.

* + 1. Zapisz adres MAC interfejsu G0/1 routera R1. Użyj komendy **show interface g0/1 na routerze R1**.

R1# **show interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

 Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia 3047.0da3.1821)

Jaki jest adres MAC interfejsu G0/1 routera R1? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Na przełączniku S1 w trybie uprzywilejowanym użyj komendy **show mac address-table**. Znajdź dynamiczne wpisy dla portów F0/5 i F0/6. Wypisz je poniżej.

F0/5 - adresy MAC: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

F0/6 – adresy MAC: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Skonfiguruj podstawowe bezpieczeństwo portów.

**Uwaga**: Ta procedura powinna być wykonana na wszystkich używanych portach przełącznika. Port F0/5 pokazany jest tu jako przykład.

* + - 1. Wejdź do trybu konfiguracji interfejsu, który jest połączony z routerem R1.

S1(config)# **interface f0/5**

* + - 1. Wyłacz port.

S1(config-if)# **shutdown**

* + - 1. Włącz bezpieczeństwo portu F0/5.

S1(config-if)# **switchport port-security**

**Uwaga**: Wpisanie komendy **switchport port-security** ustawia maksymalna liczbę adresów MAC na 1 oraz wyłącza port po przekroczeniu tej liczby. Komendy **switchport port-security maximum** oraz **switchport port-security violation** są używane do zmiany domyślnych ustawień.

* + - 1. Skonfiguruj statyczny wpis adresu MAC interfejsu G0/1 routera R1 odczytanego w kroku 2a.

S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx

(xxxx.xxxx.xxxx adres MAC interfejsu G0/1 routera R1)

**Uwaga**: Opcjonalnie można użyć komendy **switchport port-security mac-address sticky**  w celu dodania wszystkich bezpiecznych adresów MAC, które są poznawane przez port przełącznika.

* + - 1. Włącz port przełącznika.

S1(config-if)# **no shutdown**

S1(config-if)# **end**

* + 1. Zweryfikuj bezpieczeństwo portu F0/5 na przełączniku S1 używając komendy **show port-security interface**.

S1# **show port-security interface f0/5**

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 : 1

Configured MAC Addresses : 1

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0

Jaki jest status portu F0/5? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Na routerze R1 użyj polecenia ping na adres komputera PC-A.

R1# **ping 172.16.99.3**

* + 1. Sprawdź bezpieczeństwo przełącznika, zmieniając adres MAC interfejsu G0/1 routera R1. Wejdź do trybu konfiguracji interfejsu G0/1 i wyłącz go.

R1# **config t**

R1(config)# **interface g0/1**

R1(config-if)# **shutdown**

* + 1. Skonfiguruj nowy adres MAC interfejsu. Użyj adresu **aaaa.bbbb.cccc**

R1(config-if)# **mac-address aaaa.bbbb.cccc**

* + 1. Jeżeli możliwe otwórz jednocześnie połączenie konsolowe do przełącznika S1. Zobaczysz różne wiadomości pojawiające się na przełączniku związane z naruszeniem bezpieczeństwa. Włącz interfejs G0/1 na routerze R1.

R1(config-if)# **no shutdown**

* + 1. Na routerze R1 użyj polecenia ping na adres komputera PC-A. Czy wynik był pozytywny? Dlaczego tak lub dlaczego nie?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Na przełączniku zweryfikuj bezpieczeństwo portu następującymi komendami.

S1# **show port-security**

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

 (Count) (Count) (Count)

--------------------------------------------------------------------

 Fa0/5 1 1 1 Shutdown

----------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) :0

Max Addresses limit in System (excluding one mac per port) :8192

S1# **show port-security interface f0/5**

Port Security : Enabled

Port Status : Secure-shutdown

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 1

Sticky MAC Addresses : 0

Last Source Address:Vlan : aaaa.bbbb.cccc:99

Security Violation Count : 1

S1# **show interface f0/5**

FastEthernet0/5 is down, line protocol is down (err-disabled)

 Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)

 MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,

 reliability 255/255, txload 1/255, rxload 1/255

<output omitted>

S1# **show port-security address**

 Secure Mac Address Table

------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

 (mins)

---- ----------- ---- ----- -------------

 99 30f7.0da3.1821 SecureConfigured Fa0/5 -

-----------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) :0

Max Addresses limit in System (excluding one mac per port) :8192

* + 1. Wyłącz interfejs G0/1 na routerze R1, usuń wpisany adres MAC i ponownie włącz interfejs.

R1(config-if)# **shutdown**

R1(config-if)# **no mac-address aaaa.bbbb.cccc**

R1(config-if)# **no shutdown**

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

* + 1. Na routerze R1 użyj polecenia ping na adres komputera PC-A. Czy wynik był pozytywny?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Na przełączniku użyj komendy **show interface f0/5** w celu wykrycia przyczyny braku odpowiedzi polecenia ping. Zapisz znalezioną przyczynę.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Wyczyść błąd statusu portu F0/5 na przełączniku S1.

S1# **config t**

S1(config)# **interface f0/5**

S1(config-if)# **shutdown**

S1(config-if)# **no shutdown**

**Uwaga**: Może wystąpić opóźnienie przy zmianie statusu portu.

* + 1. Wydaj komendę **show interface f0/5** na S1 w celu weryfikacji czy port F0/5 nie jest dłużej w błędnym trybie wyłączenia.

S1# **show interface f0/5**

FastEthernet0/5 is up, line protocol is up (connected)

 Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)

 MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,

 reliability 255/255, txload 1/255, rxload 1/255

* + 1. Na routerze R1 użyj polecenia ping na adres komputera PC-A. Wynik powinien być pozytywny.
1. Do przemyślenia
	1. Dlaczego włącza się bezpieczeństwo portów na przełączniku?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Dlaczego nieużywane porty przełącznika powinny być wyłączone?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Tabela interfejsów routera

|  |
| --- |
| Interfejsy routera |
| Model routera | Interfejs Ethernet #1 | Interfejs Ethernet #2 | Interfejs Serial #1 | Interfejs Serial #2 |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **Uwaga**: Aby dowiedzieć się jak router jest skonfigurowany należy spojrzeć na jego interfejsy i zidentyfikować typ urządzenia oraz liczbę jego interfejsów. Nie ma możliwości wypisania wszystkich kombinacji i konfiguracji dla wszystkich routerów. Powyższa tabela zawiera identyfikatory dla możliwych kombinacji interfejsów szeregowych i ethernetowych w urządzeniu. Tabela nie uwzględnia żadnych innych rodzajów interfejsów, pomimo że podane urządzenia mogą takie posiadać np. interfejs ISDN BRI. Opis w nawiasie (przy nazwie interfejsu) to dopuszczalny w systemie IOS akronim, który można użyć przy wpisywaniu komend. |