Ćwiczenie – Podstawy konfiguracji i zabezpieczania przełączników.

Topologia

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

Cele nauczania

Część 1: Budowa sieci oraz inicjalizacja urządzeń

Część 2: Konfiguracja urządzeń i sprawdzenie łączności

- Konfiguracja adresacji IP komputerów.
- Konfiguracja podstawowych ustawień routera i przełącznika.
- Weryfikacja łączności w sieci

Część 3: Konfiguracja urządzeń do obsługi SSH

- Konfiguracja i weryfikacja dostępu przy użyciu SSH.
- Modyfikacja parametrów protokołu SSH.

Część 4: Zarządzanie tabelą adresów MAC

- Odczytanie adresu MAC komputera.
- Ustalenie adresu MAC, którego uczy się przełącznik.
- Sprawdzenie opcji komendy **show mac address-table**.
- Statyczne ustawienie adresu MAC.

Część 5: Konfiguracja i weryfikacja aspektów bezpieczeństwa na przełączniku

- Konfiguracja i weryfikacja ogólnych aspektów bezpieczeństwa.
- Konfiguracja i weryfikacja bezpieczeństwa portów przełącznika.

Wprowadzenie

Jest to kompleksowe ćwiczenie służące do powtórki wcześniej poznanych poleceń IOS routera i przełącznika. W tym ćwiczeniu zbudujesz prostą sieć i uzyskasz dostęp do przełącznika przy użyciu połączenia konsolowego oraz zdalnego. Przełączniki Cisco mogą być konfigurowane przy użyciu specjalnego adresu IP zwanego wirtualnym adresem przełącznika SVI (switch virtual interface). SVI lub adres zarządzania mogą zostać użyte do zdalnego dostępu do przełącznika w celu wyświetlenia lub konfiguracji ustawień. Jeżeli adres IP SVI jest przypisany do VLAN1 to domyślnie wszystkie porty przełącznika mają dostęp do adresu zarzadzania SVI. 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.

W części 1 i 2 będziesz okablowywać urządzenia i uzupełniać podstawową konfigurację oraz ustawienia interfejsów z protokołem IPv4 na routerze. Na potrzeby powtórki niniejsza instrukcja zawiera polecenia niezbędne do konkretnej konfiguracji routera

W części 3 będziesz używać SSH do połączenia zdalnego z routerem i przełącznikiem. Wprowadzisz modyfikacje ustawień SSH i zweryfikujesz łączność z urządzeniem

W części 4 określisz adres MAC, którego uczy się przełącznik, ustawisz statycznie adres MAC na interfejsie przełącznika a następnie usuniesz statyczny wpis.

W części 5 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.

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 PC (Windows 7, Vista, lub XP z zainstalowanymi programami emulatora terminala, takim jak PuTTy oraz Wireshark)
- 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.

Uwaga: W dodatku A opisano szczegółowo kroki prowadzące do inicjacji i przeładowania urządzeń.

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.

a. Skonfiguruj adres IP, maskę podsieci i bramę domyślną na PC-A.

Krok 2: Konfiguracja podstawowych ustawień routera R1.

a. Skonfiguruj nazwę urządzenia: R1_<Twoje nazwisko>.

b. Wyłącz niepożądane zapytania DNS (DNS lookup).

c. Skonfiguruj adres IP zgodnie tabelą adresacji.

d. Ustaw **cisco12345** jako hasło do trybu uprzywilejowanego EXEC

e. Ustaw odpowiednio **ciscoconpass i ciscovtypass** jako hasła do połączeń konsolowych i wirtualnych (console i vty).

f. Ustaw szyfrowanie haseł.

g. 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.

a. Skonfiguruj nazwę urządzenia: **S1_<Twoje nazwisko>**

b. Wyłącz niepożądane zapytania DNS (DNS lookup).

c. Ustaw **cisco12345** jako hasło do trybu uprzywilejowanego EXEC

d. Ustaw odpowiednio **ciscoconpass i ciscovtypass** jako hasła do połączeń konsolowych i wirtualnych (console i vty).

e. Skonfiguruj bramę domyślną dla S1 używając adresu IP odpowiedniego interfejsu routera R1.

f. Ustaw szyfrowanie haseł.

g. Zapisz bieżącą konfigurację jako startową.

h. Stwórz VLAN 99 nazwij go jako **Management**.

```
S1_TwojeNazwisko(config)# vlan 99
S1_TwojeNazwisko(config-vlan)# name Management
S1_TwojeNazwisko(config-vlan)# exit
S1_TwojeNazwisko(config)#
```

i. Ustaw adres IP zarzadzania dla VLAN 99 zgodnie z tabelą adresacji oraz włącz interfejs.

```
S1_TwojeNazwisko(config)# interface vlan 99
S1_TwojeNazwisko(config-if)# ip address 172.16.99.11 255.255.255.0
S1_TwojeNazwisko(config-if)# no shutdown
S1_TwojeNazwisko(config-if)# end
S1_TwojeNazwisko#
```

j. Wydaj komendę **show vlan** na S1. Jaki jest status VLAN 99? _____

k. 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**?

_____

l. Przypisz porty F0/5 i F0/6 do VLAN 99.

```
S1_TwojeNazwisko# config t
S1_TwojeNazwisko(config)# interface f0/5
S1_TwojeNazwisko(config-if)# switchport mode access
S1_TwojeNazwisko(config-if)# switchport access vlan 99
S1_TwojeNazwisko(config-if)# interface f0/6
S1_TwojeNazwisko(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

m. 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.

a. Użyj polecenia ping na PC-A w celu sprawdzenia łączności do R1. Czy wynik polecenia ping był pozytywny? _____

b. Użyj polecenia ping na PC-A w celu sprawdzenia łączności do S1. Czy wynik polecenia ping był pozytywny? _____

c. Użyj polecenia ping na S1 w celu sprawdzenia łączności do R1. Czy wynik polecenia ping był pozytywny? _____

d. 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 **cisco12345**. Jeżeli pojawi się komunikat z zapytanie o zabezpieczone połączenie wybierz Nie. Czy uzyskałeś dostęp do interfejsu www przełącznika S1? _____

e. Zamknij przeglądarkę na PC-A.

Uwaga: Niezabezpieczony interfejs www na przełączniku jest domyślnie włączony. Powszechną praktyką jest wyłączenie tej usługi jak opisano w części 5.

Część 3: Konfiguracja urządzeń do obsługi SSH

Krok 1: Konfiguracja dostępu przez SSH na przełączniku.

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

```
S1_TwojeNazwisko(config)# ip domain-name CCNA-Lab.com
```

b. Utwórz lokalnego użytkownika dla połączeń SSH. Użytkownik powinien mieć uprawnienia administratora.

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

```
S1_TwojeNazwisko(config)# username admin privilege 15 secret sshadmin
```

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

```
S1_TwojeNazwisko(config)# line vty 0 15
S1_TwojeNazwisko(config-line)# transport input ssh
S1_TwojeNazwisko(config-line)# login local
S1_TwojeNazwisko(config-line)# exit
```

d. Wygeneruj klucz RSA o długości 1024 btów.

```
S1_TwojeNazwisko(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_TwojeNazwisko(config)#
S1_TwojeNazwisko(config)# end
```

e. Zweryfikuj konfigurację SSH i odpowiedz na pytania.

```
S1_TwojeNazwisko# 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 konfiguracji SSH na przełączniku.

Zmodyfikuj domyślną konfigurację SSH.

```
S1_TwojeNazwisko# config t
S1_TwojeNazwisko(config)# ip ssh time-out 75
S1_TwojeNazwisko(config)# ip ssh authentication-retries 2
```

Ile jest dozwolonych prób logowania? _____

Jaki jest czas nieaktywności (timeout) dla SSH? _____

Krok 3: Weryfikacja konfiguracji SSH na przełączniku.

a. 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?

_____

_____

b. Wpisz **exit** i zamknij sesję SSH na S1.

Część 4: Zarządzanie tabelą adresów MAC przełącznika

W części 4 określisz adres MAC, którego uczy się przełącznik, ustawisz statycznie adres MAC na interfejsie przełącznika a następnie usuniesz statyczny wpis.

Krok 1: Odczyt adresu MAC komputera.

Wpisz w wierszu poleceń komputera PC-A komendę **ipconfig /all** w celu odczytania fizycznego adresu drugiej warstwy karty sieciowej.

_____

Krok 2: Określenie adresu MAC, którego uczy się przełącznik.

Wyświetl adresy MAC używając komendy **show mac address-table**.

```
S1_TwojeNazwisko# show mac address-table
```

Ile dynamicznych adresów MAC znajduje się w tablicy? _____

Ile wszystkich adresów MAC znajduje się w tablicy? _____

Czy dynamiczny adres MAC odpowiada adresowi komputera PC-A? _____

Krok 3: Poznanie opcji komendy show mac address-table.

a. Wyświetl opcje tabeli adresów MAC.

```
S1_TwojeNazwisko# show mac address-table ?
```

Ile opcji jest dostępnych dla komendy **show mac address-table**? _____

a. Użyj komendy **show mac address-table dynamic** w celu wyświetlenia adresów poznanych dynamicznie.

```
S1_TwojeNazwisko# show mac address-table dynamic
```

Ile dynamicznych adresów znajduje się w tablicy? _____

b. Wyświetl adres MAC komputera PC-A. Format adresu dla tej komendy to xxxx.xxxx.xxxx.

```
S1_TwojeNazwisko# show mac address-table address <tutaj MAC PC-A>
```

Krok 4: Ustawianie statycznych adresów MAC.

a. Wyczyść tablicę adresów MAC.

W celu usunięcia istniejących wpisów w tablicy użyj komendy **clear mac address-table dynamic**.

```
S1_TwojeNazwisko# clear mac address-table dynamic
```

b. Sprawdź czy tablica została wyczyszczona.

```
S1_TwojeNazwisko# show mac address-table
```

Ile statycznych adresów znajduje się w tablicy?_____

Ile dynamicznych adresów znajduje się w tablicy?_____

c. Wyświetl ponownie tablicę adresów MAC.

Bardzo prawdopodobne jest, że aplikacje uruchomione na PC-A wysłały już pakiety do przełącznika. Wyświetl ponownie tablicę adresów MAC na przełączniku, aby sprawdzić czy przełącznik nauczył się już adresu MAC komputera PC-A.

```
S1# show mac address-table
```

Ile dynamicznych adresów znajduje się w tablicy? _____

Dlaczego liczba się zmieniła się od ostatniego wyświetlenia tablicy? _____

Jeżeli przełącznik nie poznał jeszcze adresu MAC komputera PC-A, użyj polecenia ping z komputera na adres SVI przełącznika, a następnie powtórz komendę **show mac address-table**.

d. Ustaw statyczny adres MAC.

W celu ustawienia, które porty mogą połączyć się z komputerem tworzy się statyczne odwzorowanie adresu MAC komputera na danym porcie przełącznika.

Ustaw statyczny adres MAC komputera PC-A na porcie F0/6 przełącznika. Adres MAC 0050.56BE.6C89 pokazany poniżej stanowi tylko przykład użycia komendy. Zamiast niego użyj adresu komputera PC-A.

```
S1_TwojeNazwisko(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6
```

e. Sprawdź wpisy w tabeli adresów MAC.

```
S1_TwojeNazwisko# show mac address-table
```

Ile wszystkich adresów znajduje się w tablicy? _____

Ile statycznych adresów znajduje się w tablicy? _____

f. Usuń statyczny adres MAC z tablicy. Wejdź do trybu globalnej konfiguracji i użyj tej samej komendy co w punkcie g, tylko z przedrostkiem **no** na początku.

Uwaga: Adres MAC 0050.56BE.6C89 jest użyty jako przykład. Użyj adresu komputera PC-A.

```
S1_TwojeNazwisko(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6
```

g. Sprawdź czy statyczny adres MAC został usunięty.

```
S1_TwojeNazwisko# show mac address-table
```

Ile statycznych adresów znajduje się w tablicy? _____

Część 5: Konfiguracja i weryfikacja aspektów bezpieczeństwa na przełączniku

W części 5 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.

a. Skonfiguruj baner (MOTD) na S1 z odpowiednią wiadomością ostrzegającą.

b. Wydaj komendę **show ip interface brief** na S1. Które fizyczne porty są włączone (up)?

_____

c. Wyłącz wszystkie nieużywane porty, użyj komendy **interface range** .

```
S1_TwojeNazwisko(config)# interface range f0/1 – 4
S1_TwojeNazwisko(config-if-range)# shutdown
S1_TwojeNazwisko(config-if-range)# interface range f0/7 – 24
S1_TwojeNazwisko(config-if-range)# shutdown
S1_TwojeNazwisko(config-if-range)# interface range g0/1 – 2
S1_TwojeNazwisko(config-if-range)# shutdown
S1_TwojeNazwisko(config-if-range)# end
S1_TwojeNazwisko#
```

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

_____

e. 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? _____

f. Sesja HTTP wysyła wszystko jawnym tekstem. Wyłącz serwer HTTP na przełączniku.

```
S1_TwojeNazwisko(config)# no ip http server
```

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

_____

h. Na komputerze PC-A wpisz w przeglądarce adres https://172.16.99.11. Zaakceptuj certyfikat. Zaloguj się bez użytkownika i z hasłem **cisco12345**. Jaki jest rezultat?

_____

i. Zamknij przeglądarkę na PC-A.

Krok 2: Konfiguracja i weryfikacja bezpieczeństwa portu na przełączniku.

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

```
R1_TwojeNazwisko# 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? _____

b. 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: _____

c. 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_TwojeNazwisko(config)# interface f0/5
```

2 Wyłacz port.

```
S1_TwojeNazwisko(config-if)# shutdown
```

3 Włącz bezpieczeństwo portu F0/5.

```
S1_TwojeNazwisko(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.

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

```
S1_TwojeNazwisko(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.

5 Włącz port przełącznika.

```
S1_TwojeNazwisko(config-if)# no shutdown
S1_TwojeNazwisko(config-if)# end
```

d. 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? _____

e. Na routerze R1 użyj polecenia ping na adres komputera PC-A.

```
R1_TwojeNazwisko# ping 172.16.99.3
```

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

```
R1_TwojeNazwisko# config t
R1_TwojeNazwisko(config)# interface g0/1
R1_TwojeNazwisko(config-if)# shutdown
```

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

```
R1_TwojeNazwisko(config-if)# mac-address aaaa.bbbb.cccc
```

h. 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_TwojeNazwisko(config-if)# no shutdown
```

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

_____

j. Na przełączniku zweryfikuj bezpieczeństwo portu następującymi komendami.

```
S1_TwojeNazwisko# 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
```

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

```
R1_TwojeNazwisko(config-if)# shutdown
R1_TwojeNazwisko(config-if)# no mac-address aaaa.bbbb.cccc
```

```
R1_TwojeNazwisko(config-if)# no shutdown
R1_TwojeNazwisko(config-if)# end
```

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

_____

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

_____

n. Wyczyść błąd statusu portu F0/5 na przełączniku S1.

```
S1_TwojeNazwisko# config t
S1_TwojeNazwisko(config)# interface f0/5
S1_TwojeNazwisko(config-if)# shutdown
S1_TwojeNazwisko(config-if)# no shutdown
```

Uwaga: Może wystąpić opóźnienie przy zmianie statusu portu.

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

```
S1_TwojeNazwisko# 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
```

p. Na routerze R1 użyj polecenia ping na adres komputera PC-A. Wynik powinien być pozytywny.

Do przemyślenia

1. Dlaczego powinno konfigurować się linie vty na przełączniku?

   _____

2. Dlaczego zmienia się domyślny VLAN 1 na inny?

   _____

3. Jak można zapobiec wysyłaniu haseł jawnym tekstem?

   _____

4. Dlaczego konfiguruje się statyczny adres MAC na portach przełącznika?

   _____

5. Dlaczego włącza się bezpieczeństwo portów na przełączniku?

   _____

6. Dlaczego nieużywane porty przełącznika powinny być wyłączone?

   _____

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.

Dodatek A: Inicjacja i przeładowanie routera oraz przełącznika

1 Inicjacja i przeładowanie routera.

a. Podłącz konsolę w routerze i przejdź na poziom uprzywilejowany (enable privileged EXEC mode).

```
Router> enable
Router#
```

a. Wpisz polecenie **erase startup-config** aby usunąć plik startup configuration z NVRAM.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
Router#
```

b. Wykonaj polecenie **reload** aby usunąć starą konfigurację z pamięci (RAM). Gdy pojawi się monit o **Proceed with reload**, naciśnij Enter aby potwierdzić przeładowanie (reload). (Naciśnięcie innego klawisza przerwie proces przeładowania.)

```
Router# reload
Proceed with reload? [confirm]
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

a. **Uwaga**: Może pojawić się monit o zachowanie running configuration przed przeładowaniem routera. Wpisz **no** i naciśnij Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

c. Po przeładowaniu routera pojawi się monit o rozpoczęcie dialogu konfiguracji początkowej. Wpisz **no** i naciśnij Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

d. Gdy pojawi się monit o zakończenie autoinstalacji. Wpisz **yes** i naciśnij Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

Krok 1. Inicjacja i przeładowanie przełącznika.

a. Podłącz się do konsoli przełącznika i przejdź do trybu uprzywilejowanego (privileged EXEC mode).

```
Switch> enable
Switch#
```

b. Użyj polecenia **show flash** do sprawdzenia czy na przełączniku były utworzone sieci VLAN

```
Switch# show flash
Directory of flash:/

    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00  config.text
    4  -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

c. Jeżeli plik **vlan.dat** zostanie znaleziony w pamięci flash należy go skasować.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

b. Pojawi się monit o potwierdzenie nazwy pliku. W tym miejscu możesz zmienić nazwę pliku lub po prostu nacisnąć Enter jeżeli wprowadzona nazwa jest poprawna.

c. Pojawi monit o potwierdzenie skasowania tego pliku. Naciśnij Enter aby potwierdzić kasowanie. (Naciśnij inny klawisz aby przerwać kasowanie.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

d. Użyj polecenia **erase startup-config** do skasowania pliku startup configuration z pamięci NVRAM. Pojawi się monit o potwierdzenie skasowania pliku z konfiguracją. Naciśnij Enter aby potwierdzić kasowanie. (Naciśnij inny klawisz aby przerwać kasowanie.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
Switch#
```

e. Wykonaj polecenie **reload** aby usunąć starą konfigurację z pamięci (RAM) przełącznika. Gdy pojawi się monit o **Proceed with reload**, naciśnij Enter aby potwierdzić przeładowanie (reload). (Naciśnięcie innego klawisza przerwie proces przeładowania.)

```
Switch# reload
Proceed with reload? [confirm]
```

d. **Uwaga**: Może pojawić się monit o zachowanie running configuration przed przeładowaniem routera. Wpisz **no** i naciśnij Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

e. Po przeładowaniu przełacznika pojawi się monit o rozpoczęcie dialogu konfiguracji początkowej. Wpisz **no** i naciśnij Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```