Ćwiczenie – Konfiguracja aspektów bezpieczeństwa przełącznika

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 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.

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, ze 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 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.

a. Skonfiguruj nazwę urządzenia.
b. Wyłącz niepożądane zapytania DNS (DNS lookup).
c. Skonfiguruj adres IP zgodnie tabelą adresacji.
d. Ustaw **class** jako hasło do trybu uprzywilejowanego EXEC
e. Ustaw **cisco** jako hasło 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.
b. Wyłącz niepożądane zapytania DNS (DNS lookup).
c. Ustaw **class** jako hasło do trybu uprzywilejowanego EXEC
d. Ustaw **cisco** jako hasło do połączeń konsolowych i wirtualnych (console i vty).
e. Skonfiguruj bramę domyślną dla S1 używając adresu IP routera R1.
f. Ustaw szyfrowanie haseł.
g. Zapisz bieżącą konfigurację jako startową.
h. Stwórz VLAN 99 nazwij go jako **Management**.

```
S1(config)# vlan 99
```

```
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

i. 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#
```

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

k. Wydaj komendę **show ip interface brief** na S1. Jaki jest status i protokół interfejsu VLAN 99?

_____

Stan interfejsu jest up, a stan protokołu jest down.

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

_____

Żaden port na switchu nie jest przypisany do sieci VLAN 99.

l. 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
```

m. Wydaj komendę **show ip interface brief** na S1. Jaki jest status i protokół interfejsu VLAN 99? _____ Up i up

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? _____Tak

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

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

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

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 4.

Część 3: Konfiguracja i weryfikacja protokołu SSH na przełączniku S1

Krok 1: Konfiguracja dostępu SSH na S1.

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

```
S1(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 powinno być używane tylko do celów dydaktycznych.

```
S1(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(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

d. 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
```

e. Zweryfikuj konfigurację SSH i odpowiedz na pytania.

```
S1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCKWqCN0g4XLVdJJUOr+9qoJkFqC/g0OuAV1semrR5/
xy0bbUBPywvqhwSPJtucIKxKw/YfrRCeFwY+dc+/jGSeckAHahuv0jJfOdFcgqiKGeeluAu+iQ2drE+k
butnlLTGmtNhdEJMxri/ZeO3BsFcnHpO1hbB6Vsm4XRXGk7OfQ==
```

Jaka jest wersja SSH używana przez przełącznik? _____1.99

Ile jest dozwolonych prób logowania? _____3

Jaki jest domyślny czas nieaktywności (timeout) dla SSH? _____120 sekund

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
S1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 75 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
```

```
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCKWqCN0g4XLVdJJUOr+9qoJkFqC/g0OuAV1semrR5/
xy0bbUBPywvqhwSPJtucIKxKw/YfrRCeFwY+dc+/jGSeckAHahuv0jJfOdFcgqiKGeeluAu+iQ2drE+k
butnlLTGmtNhdEJMxri/ZeO3BsFcnHpO1hbB6Vsm4XRXGk7OfQ==
```

Ile jest dozwolonych prób logowania? _____2

Jaki jest czas nieaktywności (timeout) dla SSH? _____75 sekund

Krok 3: Weryfikacja konfiguracji SSH na S1.

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? _____Tak

Co zostało wyświetlone na przełączniku S1?

_____

_____

S1 wskazuje ścieżkę do dostępu uprzywilejowanego, ponieważ poziom 15 został użyty w czasie konfiguracji nazwy użytkownika I hasła

b. 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.

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)?

_____

Porty F0/5 i F0/6

c. 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#
```

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

_____

Wyłączone administracyjnie

e. Wydaj komendę **show ip http server status**.

```
S1# show ip http server status
HTTP server status: Enabled
```

```
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:html
HTTP server help root:
Maximum number of concurrent server connections allowed: 16
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 25
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-
sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

Jaki jest status serwera HTTP? _____ Enabled

Jaki port jest używany przez serwer? _____80

Jaki jest status serwera HTTPS? _____ Enabled

Jaki port jest używany przez serwer HTTPS? _____443

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

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

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

_____

.Strona internetowa nie może się otworzyć. Połaczenia HTTP są teraz odrzucane.

h. 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?

_____

Udana chroniona sesja webowa.

i. Zamknij przeglądarkę na PC-A.

Krok 2: Konfiguracja i weryfikacja bezpieczeństwa portu na S1.

a. 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? _____

W przykładzie powyżej jest to 30f7.0da3.1821

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: _____30f7.0da3.1821

F0/6 – adresy MAC: _____00e0.b857.1ccd

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(config)# interface f0/5
```

2 Wyłacz port.

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

3 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.

4 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.

5 Włącz port przełącznika.

```
S1(config-if)# no shutdown
S1(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? _____

Status jest secure-up co oznacza, że port jest chroniony a jego status I protokół są podniesione (up).

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

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

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

```
R1(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(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?

_____

Nie, port F0/5 na S1 jest wyłączony z powodu restrykcji bezpieczeństwa.

j. 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
```

k. 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
```

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

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

_____

Port F0/5 na S1 jest wciąż w stanie errdisable.

```
S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

n. 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.

o. 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
```

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

Do przemyślenia

1. Dlaczego włącza się bezpieczeństwo portów na przełączniku?

_____

Zabezpiecza to przed dostępem nieautoryzowanych urządzeń wpinanych do twojego switcha

2. Dlaczego nieużywane porty przełącznika powinny byc wyłączone?

_____

Doskonałym przykładem jest to, że użytkownik nie powinien się połączyć ze switchem przez nieużywany port I otrzymać połączenie do LAN.

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.

Konfiguracja urządzeń

Router R1

```
R1#sh run
Building configuration...
Current configuration : 1232 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain-lookup
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.99.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
```

```
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!line con 0
 password 7 030752180500
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line 67
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 password 7 13061E01080344
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
S1#sh run
Building configuration...
Current configuration : 3762 bytes
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
service password-encryption
!
hostname S1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
no ip domain-lookup
ip domain-name CCNA-Lab.com
!
crypto pki trustpoint TP-self-signed-2530358400
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2530358400
 revocation-check none
 rsakeypair TP-self-signed-2530358400
!
crypto pki certificate chain TP-self-signed-2530358400
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32353330 33353834 3030301E 170D3933 30333031 30303030
  35395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 35333033
  35383430 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100C0E3 1B8AF1E4 ADA4C4AD F82914AF BF8BCEC9 30CFBF54 D76B3940 38353E50
  A9AE0FCE 9CA05B91 24312B31 22D5F89D D249023E AEEC442D F55315F6 D456DA95
  16B758FB 8083B681 C1B3A3BF 99420EC7 A7E0AD11 CF031CD1 36A997C0 E72BE4DD
  1D745542 1DC958C1 443B6727 F7047747 D94B8CAD 0A99CBDC ADC914C8 D820DC30
  E6B70203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 1464D1A8 83DEE145 E35D68C1 D078ED7D 4F6F0B82 9D301D06
  03551D0E 04160414 64D1A883 DEE145E3 5D68C1D0 78ED7D4F 6F0B829D 300D0609
  2A864886 F70D0101 05050003 81810098 D65CFA1C 3942148D 8961D845 51D53202
  EA59B526 7DB308C9 F79859A0 D93D56D6 C584AB83 941A2B7F C44C0E2F DFAF6B8D
  A3272A5C 2363116E 1AA246DD 7E54B680 2ABB1F2D 26921529 E1EF4ACC A4FBD14A
  BAD41C98 E8D83DEC B85A330E D453510D 89F64023 7B9782E7 200F615A 6961827F
  8419A84F 56D71664 5123B591 A62C55
        quit
!
ip ssh time-out 75
ip ssh authentication-retries 2
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
```

```
interface FastEthernet0/5
 switchport access vlan 99
 switchport mode access
 switchport port-security
 switchport port-security mac-address 30f7.0da3.1821
!
interface FastEthernet0/6
 switchport access vlan 99
 switchport mode access
!
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
shutdown
!
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
 no ip address
 shutdown
!
interface Vlan99
 ip address 172.16.99.11 255.255.255.0
!
ip default-gateway 172.16.99.1
no ip http server
ip http secure-server
!
banner motd ^CWarning! Unauthorized Access is Prohibited.^C
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
end
```