Ćwiczenie – Rozwiązywanie problemów związanych z DHCPv6 (wersja dla instruktora)

Uwaga dla instruktora: Czerwona czcionka lub szare wyróżnienie tekstu oznacza, że pojawia się on tylko w wersji dokumentu przeznaczonej dla instruktora.

Topologia

Tabela adresacji

Urządzenie	Interfejs	Adres IPv6	Długość prefiksu	Brama domyślna
R1	G0/1	2001:DB8:ACAD:A::1	64	Nie dotyczy
S1	VLAN 1	Przydzielony przez SLAAC	64	Przydzielona przez SLAAC
PC-A	Karta sieciowa	Przydzielony przez SLAAC i DHCPv6	64	Przydzielona przez SLAAC

Cele

Część 1: Budowa sieci i konfiguracja podstawowych ustawień urządzeń

Część 2: Rozwiązywanie problemów związanych z łącznością przy IPv6

Część 3: Rozwiązywanie problemów związanych z bezstanowym DHCPv6

Wprowadzenie / Scenariusz

Bardzo przydatną umiejętnością administratorów sieci jest zdolność rozwiązywania problemów z siecią. Podczas rozwiązywania problemów z siecią, ważnym jest zrozumienie adresów grupowych IPv6 i tego jak są one wykorzystywane. Do skutecznego rozwiązywania problemów niezbędna jest wiedza o komendach używanych do uzyskiwania informacji sieciowych IPv6 z różnych urządzeń.

W tym ćwiczeniu załadujesz konfiguracje do R1 i S1. Konfiguracje te zawierają błędy, które uniemożliwiają funkcjonowanie bezstanowego DHCPv6 w tej sieci. Twoim zadaniem jest usunięcie znalezionych błędów na R1 i S1 w celu rozwiązania problemów.

Uwaga: Do realizacji ćwiczenia preferowane są routery Cisco 1941 Integrated Services Routers (ISR) z systemem Cisco IOS Release 15.2(4)M3 (universalk9 image) oraz przełączniki Cisco Catalyst 2960 z systemem Cisco IOS Release 15.0(2) (lanbasek9 image). W przypadku ich braku mogą zostać użyte inne routery i przełączniki z inną wersją systemu operacyjnego. W zależności od modelu i wersji IOS dostępne komendy mogą się różnić od prezentowanych w instrukcji. Na końcu instrukcji zamieszczono tabelę zestawiającą identyfikatory interfejsów routera.

Uwaga: Upewnij się, że routery i przełączniki zostały wyczyszczone i nie posiadają konfiguracji startowej. Jeśli nie jesteś pewny jak to zrobić, poproś o pomoc instruktora.

Uwaga dla instruktorów: Procedury inicjalizacji i ponownego uruchomienia urządzeń znajdują się w instrukcji dla instruktorów.

Uwaga: Menedżer bazy danych przełącznika (Switch Database Manager - SDM) może używać szablonu ustawień domyślnych **lanbase-routing** lub **dual-ipv4-and-ipv6**. Tylko szablon **dual-ipv4-and-ipv6** zapewnia możliwość adresowania IPv6. Sprawdź czy SDM używa szablonu **dual-ipv4-and-ipv6**.

```
S1# show sdm prefer
```

W celu zmiany szablonu ustawień domyślnych SDM na **dual-ipv4-and-ipv6** należy wykonać poniższe kroki. Zmieniony szablon zostanie użyty po przeładowaniu przełącznika, nie ma potrzeby zapisywania konfiguracji.

```
S1# config t
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Wymagane zasoby

- 1 router (Cisco 1941 z Cisco IOS Release 15.2(4)M3 universalk9 image lub podobny)
- 1 przełącznik (Cisco 2960 z Cisco IOS Release 15.0(2) lanbasek9 image lub podobny)
- 1 komputer (Windows 7, Vista lub XP z programem Putty lub innym programem terminalowym)
- Kable konsolowe do konfiguracji urządzeń Cisco IOS poprzez porty konsolowe
- Kable sieciowe zgodne z topologią

Część 1: Budowa sieci i konfiguracja podstawowych ustawień urządzeń

W Części 1. należy zestawić sieć zgodnie z diagramem topologii i wyczyścić konfiguracje, o ile jest to konieczne. Następnie dokonasz podstawowej konfiguracji routera i przełącznika. Potem wczytasz załączone konfiguracje IPv6 i rozpoczniesz rozwiązywanie problemów.

Krok 1: Okabluj sieć zgodnie z diagramem topologii.

Krok 2: Wyczyść konfiguracje routera i przełącznika oraz przeładuj urządzenia.

Krok 3: Wykonaj podstawową konfigurację routera i przełącznika.

a. Wyłącz opcję DNS lookup.

b. Przypisz urządzeniom nazwy zgodnie z diagramem topologii.

c. Zaszyfruj hasła wpisywane tekstem jawnym.

d. Utwórz komunikat powitalny (banner) ostrzegający każdą osobę pragnącą uzyskać dostęp do urządzenia, że nieautoryzowany dostęp jest zabroniony.

e. Ustaw **class** jako hasło szyfrowane do trybu uprzywilejowanego EXEC.

f. Ustaw **cisco** jako hasło do trybu konsoli i trybu VTY i włącz możliwość logowania.

g. Włącz logowanie synchroniczne (**logging synchronous**) aby zapobiec przerywaniu wprowadzania komend przez komunikaty pojawiające się na konsoli.

Krok 4: Wczytaj do routera R1 konfigurację IPv6.

```
ip domain name ccna-lab.com
! ipv6 unicast-routing
ipv6 dhcp pool IPV6POOL-A
 dns-server 2001:DB8:ACAD:CAFE::A
 domain-name ccna-lab.com
interface g0/0
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
interface g0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::11/64
! no ipv6 address 2001:db8:acad:a::11/64
! ipv6 address 2001:db8:acad:a::1/64
! ipv6 nd other-config-flag
! ipv6 dhcp server IPV6POOL-A
! no shutdown
end
```

Krok 5: Wczytaj do S1 konfigurację IPv6.

```
interface range f0/1-24
 shutdown
!interface range f0/5-6
! no shutdown
interface range g0/1-2
 shutdown
interface Vlan1
 shutdown
! ipv6 address autoconfig
! no shutdown
end
```

Krok 6: Zapisz bieżące konfiguracje na R1 i S1.

Krok 7: Sprawdź czy protokół IPv6 jest aktywny na PC-A.

Sprawdź w polu Właściwości połączenia lokalnego czy protokół IPv6 jest aktywny na PC-A.

Część 2: Rozwiązywanie problemów związanych z łącznością przy IPv6

W Części 2. będziesz przeprowadzał testy i sprawdzał połączenia IPv6 w 3 warstwie sieciowej. Kontynuuj rozwiązywanie problemów z siecią, aż łączność w warstwie 3 zostanie ustanowiona na wszystkich urządzeniach. Nie należy przechodzić do Części 3. dopóki pełnym sukcesem nie zakończysz Części 2.

Krok 1: Rozwiąż problemy związane z interfejsami IPv6 na R1.

a. Który interfejs na R1 musi być aktywny, według topologii, do ustanowienia połączeń sieciowych? Zapisz wszystkie polecenia używane do określenia, które interfejsy są aktywne.

_____

_____

G0/1

R1# **show ip interface brief**

b. W razie potrzeby, podejmij czynności wymagane aby podnieść interfejs. Zapisz polecenia używane do skorygowania błędów w konfiguracji i sprawdź, czy interfejs jest aktywny.

_____

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

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

c. Określ adresy IPv6 skonfigurowane na R1. Zapisz te adresy i polecenia używane w celu ich wyświetlenia.

_____

_____

2001:DB8:ACAD:A::11/64

show ipv6 interface lub **show ipv6 interface g0/1**. **Show run interface g0/1** również może być użyte.

d. Ustal czy wystąpił błąd w konfiguracji. Jeśli zidentyfikujesz błędy, zapisz wszystkie polecenia użyte do skorygowania konfiguracji

_____

_____

_____

```
R1(config)# interface g0/1
R1(config-if)# no ipv6 address 2001:db8:acad:a::11/64
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
```

e. Jaka multicastowa grupa adresów jest potrzebna na R1 aby funkcjonował SLAAC?

_____

All-routers multicast (FF02::2)

f. Jakie polecenie służy do sprawdzenia, czy R1 jest członkiem tej grupy?

_____

show ipv6 interface lub **show ipv6 interface g0/1**

```
R1# show ipv6 interface
GigabitEthernet0/1 is down, line protocol is down
  IPv6 is tentative, link-local address is FE80::1 [TEN]
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64 [TEN]
  Joined group address(es):
    FF02::1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

g. Jeśli R1 nie należy do grupy multicastowej, co jest niezbędne do tego aby SLAAC działała poprawnie. Wprowadź niezbędne zmiany w konfiguracji tak, aby R1 przyłączył się do grupy. Zapisz wszystkie polecenia konieczne do skorygowania błędów konfiguracyjnych.

_____

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

h. Ponownie wydaj polecenie, aby sprawdzić czy interfejs G0/1 dołączył do grupy multicastowej wszystkich routerów (FF02 :: 2).

Uwaga: Jeśli nie byłeś w stanie dołączyć R1 do grupy multicastowej wszystkich routerów, to konieczne będzie zapisanie aktualnej konfiguracji routera i przeładowanie go.

Krok 2: Rozwiązywanie problemów na S1.

a. Czy na S1 są aktywne interfejsy niezbędne do ustanowienia połączeń sieciowych? _____Nie

Zapisz wszystkie polecenia używane do włączenia potrzebnych interfejsów na S1.

_____

_____

_____

_____

```
S1(config)# interface range f0/5-6
S1(config-if)# no shutdown
S1(config-if)# interface vlan 1
S1(config-if)# no shutdown
```

b. Jakiego polecenia można użyć do określenia, czy adres unicastowy IPv6 został przypisany do S1?

_____

Wydaj polecenie **show ipv6 interface** lub **show ipv6 interface vlan1**.

c. Czy S1 ma skonfigurowany adres unicastowy IPv6? Jeśli tak, to jaki?

_____

Brak przypisanych adresów IPv6

d. Jeśli S1 nie otrzymuje adresu SLAAC, dokonaj niezbędnych zmian w konfiguracji aby mu to umożliwić. Zapisz użyte polecenia.

_____

_____

```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address autoconfig
```

e. Ponownie wydaj polecenie, sprawdzające czy interfejs otrzymuje adres SLAAC.

f. Czy S1 może wykonać ping na adres unicastowy IPv6 przypisany do interfejsu G0/1 na R1?

_____

Tak, Ping z S1 na adres IPv6 2001:db8:acad:a::1 powinien się powieść

Krok 3: Rozwiąż problemy na PC-A.

a. Wydaj polecenie używane na PC-A do weryfikacji przydzielonego adresu IPv6. Zapisz to polecenie.

_____

ipconfig /all

b. Jaki adres unicastowy IPv6 przydziela SLAAC do PC-A?

_____

Jeśli wszystkie zmiany zostały dokonane na R1 I S1, PC-A powinien odebrać adres IPv6 z prefiksem 2001:db8:acad:a::/64.

c. Czy z PC-A można wykonać ping na adres bramy domyślnej, przydzielony przez SLAAC?

_____

Tak, Ping z PC-A na adres FE80::1 powinien się powieść.

d. Czy PC-A może wykonać ping do interfejsu zarządzania na S1?

_____

_____

_____

Tak, Ping z PC-A na adres IPv6 przypisany do VLAN1 powinien się powieść. Ten adres można znaleźć wydając polecenie **show ipv6 interface vlan1** na S1 a następnie poszukując adres IPv6 a prefiksem 2001:db8:acad:a::/64.

Uwaga: Kontynuuj rozwiązywanie problemów, aż będzie można wykonać ping z PC-A do R1 i S1.

Część 3: Rozwiązywanie problemów związanych z bezstanowym DHCPv6

W Części 3 będziesz przeprowadzał testy i sprawdzał czy w twojej sieci działa poprawnie bezstanowy DHCPv6. Musisz używać odpowiednich komend IPv6 dla CLI na routerze, żeby sprawdzić, czy działa bezstanowy DHCPv6. Możesz używać debugowania, aby określić czy serwer DHCP jest poszukiwany wiadomością solicit.

Krok 1: Sprawdzenie, czy bezstanowy DHCPv6 działa poprawnie.

a. Jaka jest nazwa puli DHCPv6? Jak to ustalić?

_____

_____

IPV6POOL-A. Wydaj polecenie **show ipv6 dhcp pool** w celu określenia nazwy puli serwera DHCPv6. Możesz również wydać polecenie **show run | section ipv6 dhcp** aby zobaczyć te informacje.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  DNS server: 2001:DB8:ACAD:CAFE::A
  Domain name: ccna-lab.com
  Active clients: 0
```

b. Jakie informacje sieciowe są wymienione w puli DHCPv6?

_____

Wyświetlony jest adres serwera DNS: 2001:DB8:ACAD:CAFE::A oraz nazwa domeny: ccna-lab.com.

c. Czy informacje DHCPv6 zostały przydzielone do PC-A? Jak to ustalić?

_____

Nie, te informacje można ustalić wydając polecenie **ipconfig /all** w linii komend komputera PC-A.

Krok 2: Rozwiąż problemy na R1.

a. Jakie polecenie może być użyte, żeby określić czy R1 jest skonfigurowany do bezstanowego DHCPv6?

_____

_____

Polecenie **show ipv6 interface** może być użyte do określenia czy interfejs ma ustawioną flagę konfiguracji bezstanowej DHCPv6. Polecenie **show run** również może być użyte do podglądnięcia konfiguracji na tym interfejsie.

```
R1# show ipv6 interface
GigabitEthernet0/1 is up, line protocol is up
```

```
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

b. Czy interfejs G0/1 na R1 jest w trybie bezstanowego DHCPv6?

_____

_____

Nie. Interfejs nie jest częścią grupy all- DHCPv6 Servers ponieważ adres grupy FF02::1:2 nie został wyświetlony. Ponadto, nie informuje o stanie serwera DHCP w dolnej części wyników z routera.

c. Jakie polecenie może być użyte, żeby dołączyć R1 do grupy wszystkich serwerów DHCPv6?

_____

_____

Wydaj polecenie **ipv6 dhcp server IPV6POOL-A** na interfejsie G0/1.

R1(config)# **interface g0/1**
R1(config-if)# **ipv6 dhcp server IPV6POOL-A**

d. Sprawdź, czy grupa wszystkie serwery DHCPv6 jest skonfigurowana dla interfejsu G0/1.

```
R1# show ipv6 interface
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:2
    FF02::1:FF00:1
    FF05::1:3
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
```

```
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

e. Czy PC-A otrzyma teraz informacje DHCP? Wyjaśnij.

_____

_____

Nie, polecenie **show ipv6 interface** nadal nie pokazuje, że host zamierza używać DHCP do pozyskiwania pozostałych informacji konfiguracyjnych. Może być to zweryfikowane wydając polecenie **ipconfig /all** na PC-A.

f. Czego brakuje w konfiguracji G0/1, sprawiającego że hosty korzystające z serwera DCHP pobierają inne informacje sieciowe?

_____

_____

Potrzebne jest polecenie **ipv6 nd other-config-flag** do poinformowania hostów aby używały serwera DHCP do pozyskiwania pozostałych informacji sieciowych.

```
R1(config)# interface g0/1
R1(config-if)# ipv6 nd other-config-flag
R1# show ipv6 interface
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:2
    FF02::1:FF00:1
    FF05::1:3
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
  Hosts use DHCP to obtain other configuration.
```

g. Zresetuj ustawienia IPv6 na PC-A.

1) Otwórz okno Właściwości połączenia LAN, usuń zaznaczenie pola wyboru **Internet Protocol Version 6 (TCP/IPv6)**, a następnie kliknij przycisk **OK**, aby zaakceptować zmiany.

2) Ponownie otwórz okno Właściwości połączenia LAN, kliknij, aby zaznaczyć pole wyboru **Internet Protocol Version 6 (TCP/IPv6)**, a następnie kliknij przycisk OK, aby zaakceptować zmiany.

h. Wydaj polecenie, aby sprawdzić czy zostały wprowadzone zmiany na PC-A.

Uwaga: Kontynuuj rozwiązywanie problemów, aż PC-A odbierze dodatkowe informacje DHCP od R1.

Do przemyślenia

1. Jaka komenda jest potrzebna w puli DHCPv6 dla stanowego DHCPv6, a nie jest potrzebna dla bezstanowego DHCPv6? Dlaczego?

   _____

   _____

   _____

   Dla stanowego DHCPv6 potrzebne jest polecenie **address prefix <*ipv6 prefix address*>.** Hosty otrzymują swoje adresy IPv6 unicast od serwera DHCP dlatego to polecenie jest potrzebne dostarczając prefiks IPv6 do użycia w sieci.

2. Jaka komenda jest potrzebne na interfejsie, aby sprawić żeby sieć korzystała ze stanowego DHCPv6 zamiast z bezstanowego DHCPv6?

   _____

   _____

   Polecenie **ipv6 nd managed-config-flag** jest używane w celu ustawienia flagi Stateful DHCPv6. Ta jest wysyłana przez R1 do wszystkich hostów w sieci w komunikatach router advertisement.

Tabela z zestawieniem interfejsów routera

Zestawienie interfejsów 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: Obejrzyj router, aby zidentyfikować typ routera oraz aby określić liczbę jego interfejsów. W ten sposób dowiesz się, jaka jest konfiguracja sprzętowa routera. Możesz to sprawdzić również z poziomu IOS poleceniem **show ip interface brief**. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla wszystkich rodzajów routerów. Powyższa tabela zawiera identyfikatory możliwych kombinacji interfejsów szeregowych i Ethernet w urządzeniach. Tabela nie zawiera żadnych innych rodzajów interfejsów, mimo iż dany router może mieć jakieś zainstalowane. Przykładem może być interfejs ISDN BRI. Łańcuch w nawiasie jest skrótem, który może być stosowany w systemie operacyjnym Cisco IOS przy odwoływaniu się do interfejsu.

Konfiguracja urządzań

Router R1 (końcowa)

```
R1#sh run
Building configuration...

Current configuration : 1829 bytes
!
```

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
memory-size iomem 10
!
ipv6 unicast-routing
ipv6 dhcp pool IPV6POOL-A
 dns-server 2001:DB8:ACAD:CAFE::A
 domain-name ccna-lab.com
!
ipv6 cef
!
no ip domain lookup
ip domain name ccna-lab.com
ip cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp server IPV6POOL-A
!
interface Serial0/0/0
```

```
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CC
  Unauthorized Access is Prohibited!
^C
!
line con 0
 exec-timeout 0 0
 password 7 0205085A1815
 logging synchronous
 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 vty 0 4
 password 7 104D05181604
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1 (końcowa)

```
S1#sh run
Building configuration...

Current configuration : 3365 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

```
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
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
 ipv6 address autoconfig
!
ip http server
ip http secure-server
!
control-plane
!
```

```
banner motd ^C
  Unauthorized Access is Prohibited!
^C
!
line con 0
 password 7 104D000A0618
 logging synchronous
 login
line vty 0 4
 password 7 104D000A0618
 login
line vty 5 15
 password 7 104D000A0618
 login
!
end
```