

Politechnika Świętokrzyska w Kielcach

Wydział Zarządzania i Modelowania Komputerowego

Sieci Komputerowe

Laboratorium

Obliczanie podsieci IPv4

Praktyka projektowania i wdrażania VLSM

Konfiguracja adresacji IPv6

Stosowanie komendy ping oraz traceroute do testowania połączeń w sieci



Politechnika Świętokrzyska
Kielce University of Technology

Przygotowali:

Imię i Nazwisko	Nr albumu
Radosław Kulig	093795
Katarzyna Nowakowska	096946

Kierunek: Inżynieria Danych

Studia: stacjonarne

Data wykonania ćwiczenia: 27.01.2026

Oświadczam, że:

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

Radosław Kulig

Katarzyna Nowakowska

Lab 11.6.6 Obliczanie podsieci IPv4

Wstęp teoretyczny

Protokół IPv4 (Internet Protocol version 4) stanowi fundament komunikacji w większości współczesnych sieci komputerowych. Jest on odpowiedzialny za adresowanie urządzeń w taki sposób, aby dane mogły bezbłędnie trafić od nadawcy do odbiorcy. Adres IPv4 jest unikalnym identyfikatorem składającym się z 32 bitów. Dla ułatwienia zapisu bity te dzieli się na cztery części, zwane oktetami (po 8 bitów każdy), oddzielone kropkami. Każdy oktet może przyjmować wartość od 0 do 255 w systemie dziesiętnym. Adresowanie w systemie IPv4 opiera się na strukturze hierarchicznej, co oznacza, że każdy adres składa się z dwóch części:

- Części sieciowej (prefiks sieciowy): Identyfikuje konkretną sieć lub podsieć.
- Części hosta: Identyfikuje konkretne urządzenie (interfejs) w tej sieci.

O tym, gdzie kończy się część sieciowa, a zaczyna część hosta, decyduje maska podsieci. Składa się ona z ciągu jedynek (część sieciowa) i zer (część hosta).

Problem1:

Założenia:	
Adres IP hosta:	192.168.200.139
Oryginalna maska podsieci	255.255.255.0
Nowa maska podsieci:	255.255.255.224

Znajdź:	
Liczba bitów reprezentujących podsieci	3
Liczba stworzonych podsieci	8
Liczba bitów hostów w każdej podsieci	5
Liczba hostów w danej podsieci	30
Adres sieci dla tej podsieci	192.168.200.128
Adres IPv4 pierwszego hosta w podsieci	192.168.200.129
Adres IPv4 ostatniego hosta w tej podsieci	192.168.200.158
Adres rozgłoszeniowy dla tej podsieci	192.168.200.159

Problem2:

Założenia:	
Adres IP hosta:	10.101.99.228
Oryginalna maska podsieci	255.0.0.0
Nowa maska podsieci:	255.255.128.0

Znajdź:	
Liczba bitów reprezentujących podsieci	9
Liczba stworzonych podsieci	512
Liczba bitów hostów w każdej podsieci	15
Liczba hostów w danej podsieci	32766
Adres sieci dla tej podsieci	10.101.0.0
Adres IPv4 pierwszego hosta w podsieci	10.101.0.1
Adres IPv4 ostatniego hosta w tej podsieci	10.101.127.254
Adres rozgłoszeniowy dla tej podsieci	10.101.127.255

Problem3:

Założenia:	
Adres IP hosta:	172.22.32.12
Oryginalna maska podsieci	255.255.0.0
Nowa maska podsieci:	255.255.224.0

Znajdź:	
Liczba bitów reprezentujących podsieci	3
Liczba stworzonych podsieci	8
Liczba bitów hostów w każdej podsieci	13
Liczba hostów w danej podsieci	8190
Adres sieci dla tej podsieci	172.22.32.0
Adres IPv4 pierwszego hosta w podsieci	172.22.32.1
Adres IPv4 ostatniego hosta w tej podsieci	172.22.63.254
Adres rozgłoszeniowy dla tej podsieci	172.22.63.255

Problem4:

Założenia:	
Adres IP hosta:	192.168.1.245
Oryginalna maska podsieci	255.255.255.0
Nowa maska podsieci:	255.255.255.252

Znajdź:	
Liczba bitów reprezentujących podsieci	6
Liczba stworzonych podsieci	64
Liczba bitów hostów w każdej podsieci	2
Liczba hostów w danej podsieci	2
Adres sieci dla tej podsieci	192.168.1.244
Adres IPv4 pierwszego hosta w podsieci	192.168.1.245
Adres IPv4 ostatniego hosta w tej podsieci	192.168.1.246
Adres rozgłoszeniowy dla tej podsieci	192.168.1.247

Problem5:

Założenia:	
Adres IP hosta:	128.107.0.55
Oryginalna maska podsieci	255.255.0.0
Nowa maska podsieci:	255.255.255.0

Znajdź:	
Liczba bitów reprezentujących podsieci	8
Liczba stworzonych podsieci	256
Liczba bitów hostów w każdej podsieci	8
Liczba hostów w danej podsieci	254
Adres sieci dla tej podsieci	128.107.0.0
Adres IPv4 pierwszego hosta w podsieci	128.107.0.1
Adres IPv4 ostatniego hosta w tej podsieci	128.107.0.254
Adres rozgłoszeniowy dla tej podsieci	128.107.0.255

Problem6:

Założenia:	
Adres IP hosta:	192.135.250.180
Oryginalna maska podsieci	255.255.255.0
Nowa maska podsieci:	255.255.255.248

Znajdź:	
Liczba bitów reprezentujących podsieci	5
Liczba stworzonych podsieci	32
Liczba bitów hostów w każdej podsieci	3
Liczba hostów w danej podsieci	6
Adres sieci dla tej podsieci	192.135.250.176
Adres IPv4 pierwszego hosta w podsieci	192.135.250.177
Adres IPv4 ostatniego hosta w tej podsieci	192.135.250.182
Adres rozgłoszeniowy dla tej podsieci	192.135.250.183

-Dlaczego tak istotne jest analizowanie masek podsieci adresów IPv4?

Analizowanie masek podsieci jest kluczowe dla prawidłowego funkcjonowania i projektowania sieci komputerowych, ponieważ to właśnie maska pozwala urządzeniom sieciowym zinterpretować strukturę adresu IP.

Wnioski

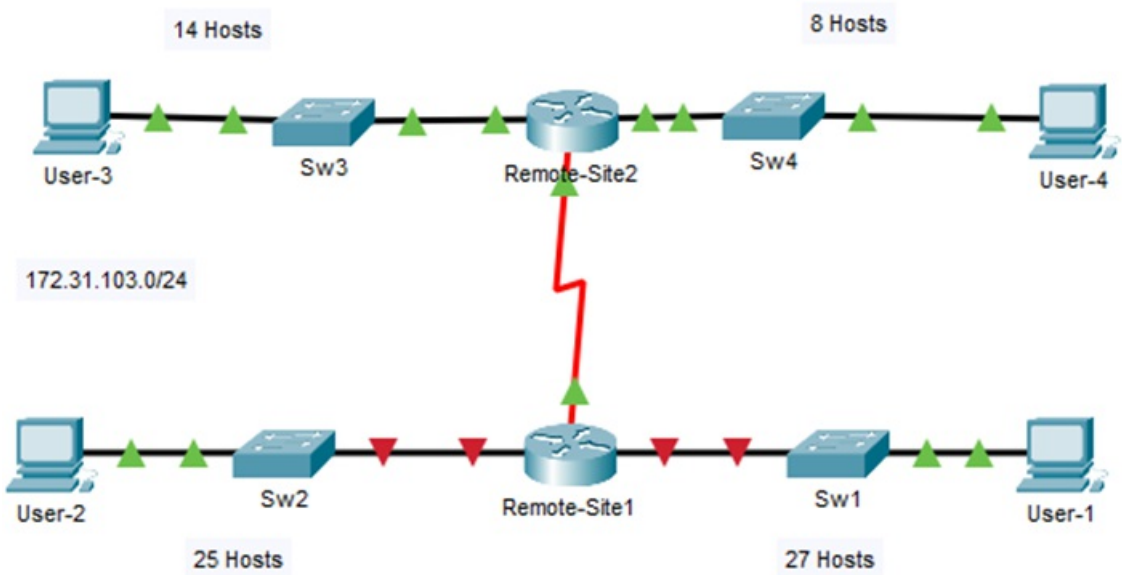
Ćwiczenie potwierdziło, że umiejętność określania adresów hostów oraz sieci na podstawie adresu IP i maski jest kluczem do zrozumienia działania sieci IPv4. Sama znajomość adresu IP bez maski nie pozwala na określenie przynależności urządzenia do konkretnego segmentu sieci.

PT 11.9.3 Praktyka projektowania i wdrażania VLSM

Wstęp teoretyczny

VLSM (Variable Length Subnet Mask), czyli maski podsieci o zmiennej długości, to technika pozwalająca na bardziej efektywne zarządzanie przestrzenią adresową. W tradycyjnym podejściu do adresowania sieciowego (tzw. adresowanie klasowe lub stałe podsieci FLSM), każda wydzielona część sieci otrzymuje taką samą liczbę adresów, niezależnie od tego, czy faktycznie ich potrzebuje. W praktyce prowadzi to do sytuacji, w której małe biuro (np. 5 komputerów) i duże piętro (np. 100 komputerów) otrzymują identyczną pulę adresów, co drastycznie marnuje dostępne zasoby. VLSM to technika, która pozwala "ciąć" sieć na kawałki o różnych rozmiarach. Zamiast jednej sztywnej maski dla całej topologii, stosujemy maski o zmiennej długości, precyzyjnie dopasowane do liczby hostów w danej sieci LAN lub na łączu WAN.

Zapoznajemy się z udostępnioną topologią oraz tabelą adresowania.



Dobieramy odpowiednie maski podsieci dla poszczególnych segmentów sieci tak, aby zapewnić wystarczającą liczbę użytecznych adresów IP.

-Jaka maska podsieci spełni wymagania ilości adresów IP w sieciach oraz ile używalnych adresów zapewnia ta podsieć?

- ASW-1: maska 255.255.255.224 (/27), 30 użytecznych adresów
- ASW-2: maska 255.255.255.224 (/27), 30 użytecznych adresów
- ASW-3: maska 255.255.255.240 (/28), 14 użytecznych adresów
- ASW-4: maska 255.255.255.240 (/28), 14 użytecznych adresów
- Building1–Building2: maska 255.255.255.252 (/30), 2 użyteczne adresy

W następnym kroku wykonujemy podział sieci bazowej 172.31.103.0/24 na mniejsze podsieci. Podział został wykonany techniką VLSM, rozpoczęto go od podsieci o największej liczbie hostów, a kolejne podsieci przydzielano w następnych dostępnych zakresach adresów. Następnie uzupełniamy tabelę podsieci.

Tabela podsieci

Opis podsieci	Ilość wymaganych hostów	Adres sieci/CIDR	Pierwszy użyteczny adres hosta	Adres rozgłoszeniowy
Asw1	27	172.31.103.0/27	172.31.103.1	172.31.103.31
Asw2	25	172.31.103.32/27	172.31.103.33	172.31.103.63
Asw3	14	172.31.103.64/28	172.31.103.65	172.31.103.79
Asw4	8	172.31.103.80/28	172.31.103.81	172.31.103.95
R	2	172.31.103.96/30	172.31.103.97	172.31.103.99

W celu udokumentowanie schematu adresowania przypisujemy adresy IP do urządzeń w każdej podsieci zgodnie z wytycznymi instrukcji.

Tabela adresowania

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
Building 1	G0/0	172.31.103.1	27	nd
	G0/1	172.31.103.33	27	nd
	S0/0/0	172.31.103.97	30	nd
Building 2	G0/0	172.31.103.65	28	nd
	G0/1	172.31.103.81	28	nd
	S0/0/0	172.31.103.98	30	nd
ASW-1	VLAN 1	172.31.103.2	27	172.31.103.1
ASW-2	VLAN 1	172.31.103.34	27	172.31.103.33
ASW-3	VLAN 1	172.31.103.66	28	172.31.103.65
ASW-4	VLAN 1	172.31.103.82	28	172.31.103.81
Host-A	karta sieciowa	172.31.103.30	27	172.31.103.1
Host-B	karta sieciowa	172.31.103.62	27	172.31.103.33
Host-C	karta sieciowa	172.31.103.78	28	172.31.103.65
Host-D	karta sieciowa	172.31.103.94	28	172.31.103.81

Wnioski

Projektowanie sieci z wykorzystaniem techniki VLSM uczy, jak przestać marnować adresy IP poprzez porzucenie sztywnego podziału na równe podsieci na rzecz elastycznego dopasowania maski do faktycznej liczby hostów. Głównym wnioskiem z zadania jest to, że kluczem do sukcesu jest zachowanie hierarchii – planowanie adresacji należy zawsze zaczynać od największych segmentów sieci, stopniowo przechodząc do najmniejszych, w tym dwuadresowych łącz WAN. Poprawnie wykonane ćwiczenie dowodzi, że systematyczne dokumentowanie pierwszych i ostatnich użytecznych adresów w tabeli adresowania jest niezbędne do sprawnego skonfigurowania urządzeń i uzyskania pełnej łączności w całej topologii.

PT 12.6.6 Konfiguracja adresacji IPv6

Wstęp teoretyczny

Przejsie z protokołu IPv4 na IPv6 to nie tylko zmiana długości adresu, ale przede wszystkim ewolucja sposobu, w jaki urządzenia komunikują się w sieci. Ćwiczenie to kupia się na praktycznym wdrożeniu tej adresacji w topologii typu gwiazda, łączącej sieć lokalną z Internetem (ISP). W protokole IPv6 standardem dla sieci lokalnych (LAN) jest prefiks /64. Oznacza to, że pierwsze 64 bity adresu definiują sieć, a pozostałe 64 bity są zarezerwowane dla identyfikatora interfejsu urządzenia. Urządzenia Cisco domyślnie mają włączony protokół IPv4, ale obsługa IPv6 wymaga ręcznej aktywacji. Kluczowym krokiem jest wydanie komendy ipv6 unicast-routing. Bez niej router zachowuje się jak zwykły komputer – nie będzie przekazywał pakietów między swoimi interfejsami GigabitEthernet i Serial.

Na początku klikamy na R1, a następnie zakładkę CLI. Przechodzimy do trybu uprzywilejowanego. Wprowadzamy komendę, która musi być skonfigurowana, aby router mógł przysyłać pakiety IPv6.

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

Teraz będziemy konfigurować adresację IPv6 na GigabitEthernet0/0. Wprowadzamy polecenia niezbędne do przejścia do trybu konfiguracji interfejsu dla GigabitEthernet0/0. Konfigurujemy adres IPv6 korzystając z poniższego polecenia: R1(config-if)# ipv6 address 2001:db8:1:1::1/64. Następnie konfigurujemy adres lokalnego łącza IPv6 (ang. link-local address) korzystając z polecenia: R1(config-if)# ipv6 address fe80::1 link-local. Na końcu uaktywniamy interfejs.

```
R1(config)#interface GigabitEthernet 0/0
R1(config-if)#ipv6 address 2001:db8:1:1::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
|
```

Konfigurujemy adresację IPv6 na GigabitEthernet0/1. Wprowadzamy polecenia niezbędne do przejścia do trybu konfiguracji interfejsu dla GigabitEthernet0/1. Konfigurujemy adres IPv6, adres lokalnego łącza i uaktywniamy interfejs.

```

R1(config-if)#exit
R1(config)#interface GigabitEthernet 0/1
R1(config-if)#ipv6 address 2001:db8:1:2::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
|

```

Konfigurujemy adresację IPv6 na Serial0/0/0. Wprowadzamy polecenia niezbędne do przejścia do trybu konfiguracji interfejsu dla Serial0/0/0. Konfigurujemy adres IPv6, adres lokalnego łącza i uaktywnij interfejs.

```

R1(config-if)#exit
R1(config)#interface Serial0/0/0
R1(config-if)#ipv6 address 2001:db8:1:a001::2/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
|

```

Weryfikujemy adresowanie IPv6 na R1. Wychodzimy z trybu konfiguracji na R1. Musimy zweryfikować adresowanie skonfigurowane. Jeśli jakiegokolwiek adresy są niepoprawne, powtarzamy powyższe kroki w razie potrzeby, aby wprowadzić poprawki. Zapisujemy konfigurację routera w pamięci NVRAM.

```

R1#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::1
    2001:DB8:1:1::1
GigabitEthernet0/1      [up/up]
    FE80::1
    2001:DB8:1:2::1
GigabitEthernet0/2      [administratively down/down]
    unassigned
Serial0/0/0              [up/up]
    FE80::1
    2001:DB8:1:A001::2
Serial0/0/1              [administratively down/down]
    unassigned
Vlan1                    [administratively down/down]
    unassigned
R1#cp running-config startup-config
^
% Invalid input detected at '^' marker.

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

```

Teraz skonfigurujemy adresację IPv6 na serwerze Accounting. Klikamy Accounting następnie zakładka Desktop > IP Configuration. W polu IPv6 Address wprowadzamy adres postaci 2001:DB8:1:1::4 z prefiksem /64. W polu IPv6 Gateway wprowadzamy adres lokalnego łącza postaci, FE80::1.

IPv6 Configuration

☐ Automatic
 ☒ Static

IPv6 Address: 2001:DB8:1:1::4 / 64

Link Local Address: FE80::201:C7FF:FE83:3CED

Default Gateway: FE80::1

DNS Server:

Konfigurujemy serwer CAD z adresami, jak to zostało zrobione w poprzednim kroku.

IPv6 Configuration

☐ Automatic
 ☒ Static

IPv6 Address: 2001:db8:1:2::4 / 64

Link Local Address: FE80::20B:BEFF:FE8E:73E2

Default Gateway: fe80::1

DNS Server:

Klikamy komputer Billing, następnie wybieramy zakładkę Desktop a potem IP Configuration. W polu IPv6 Address wprowadzamy adres postaci 2001:DB8:1:1::3 z prefiksem /64. W polu IPv6 Gateway wprowadzamy adres link-local FE80::1. Powtarzamy poprzednie kroki dla komputera Sales.

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: 2001:DB8:1:1::3 / 64

Link Local Address:

Default Gateway: FE80::1

DNS Server:

Klikamy komputer Engineering, następnie wybierz zakładkę Desktop a potem IP Configuration. W polu IPv6 Address wprowadzamy adres postaci 2001:DB8:1:2::3 z prefiksem /64, a polu IPv6 Gateway adres link-local FE80::1. Powtarzamy kroki dla komputera Design.

IPv6 Configuration

☐ Automatic ☒ Static

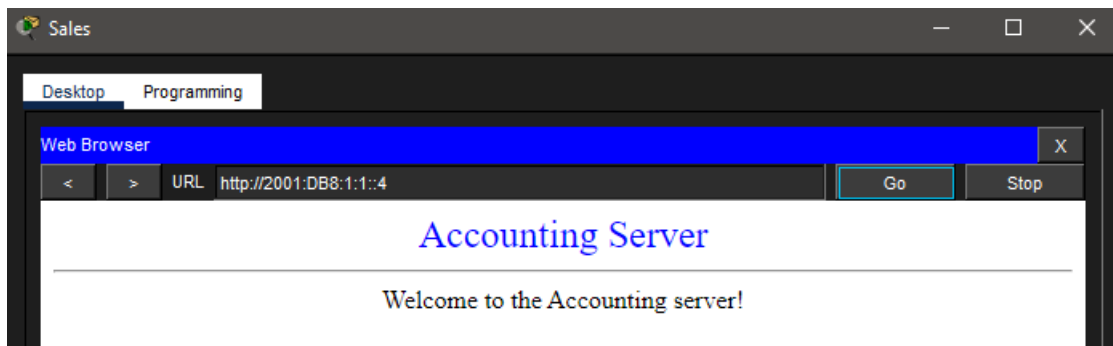
IPv6 Address: 2001:db8:1:1::2 / 64

Link Local Address:

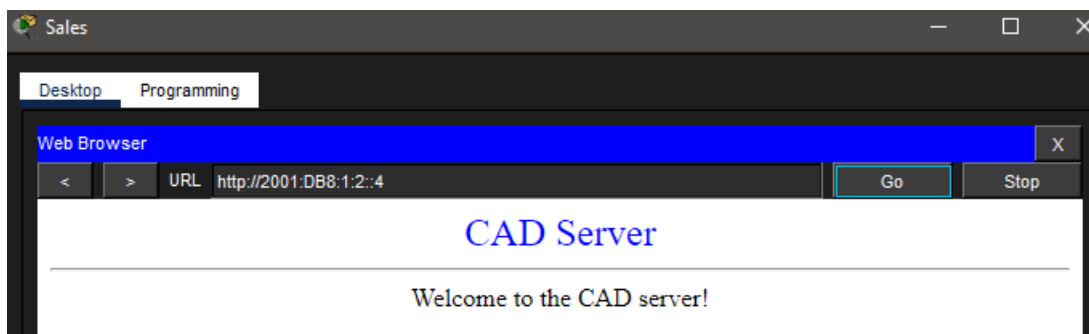
Default Gateway: fe80::1

DNS Server:

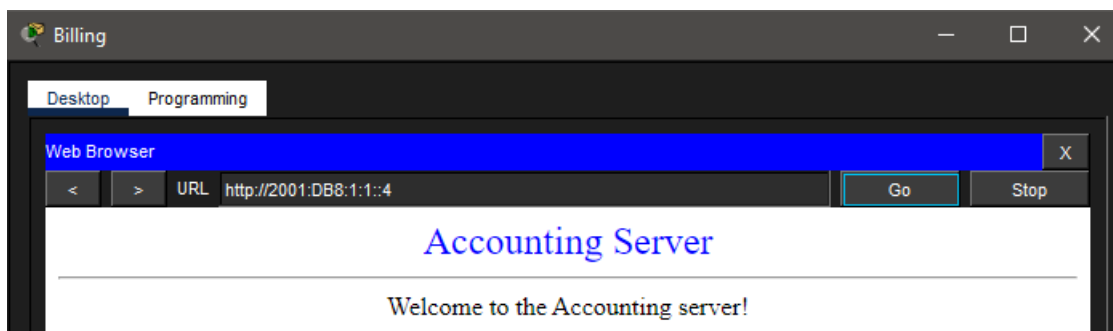
Klikamy Sales a następnie kliknij zakładkę Desktop . Klikamy Web Browser. W polu URL wprowadzamy 2001:DB8:1:1::4 i klikamy przycisk Go. Powinna się pojawić strona WWW serwera Accounting.

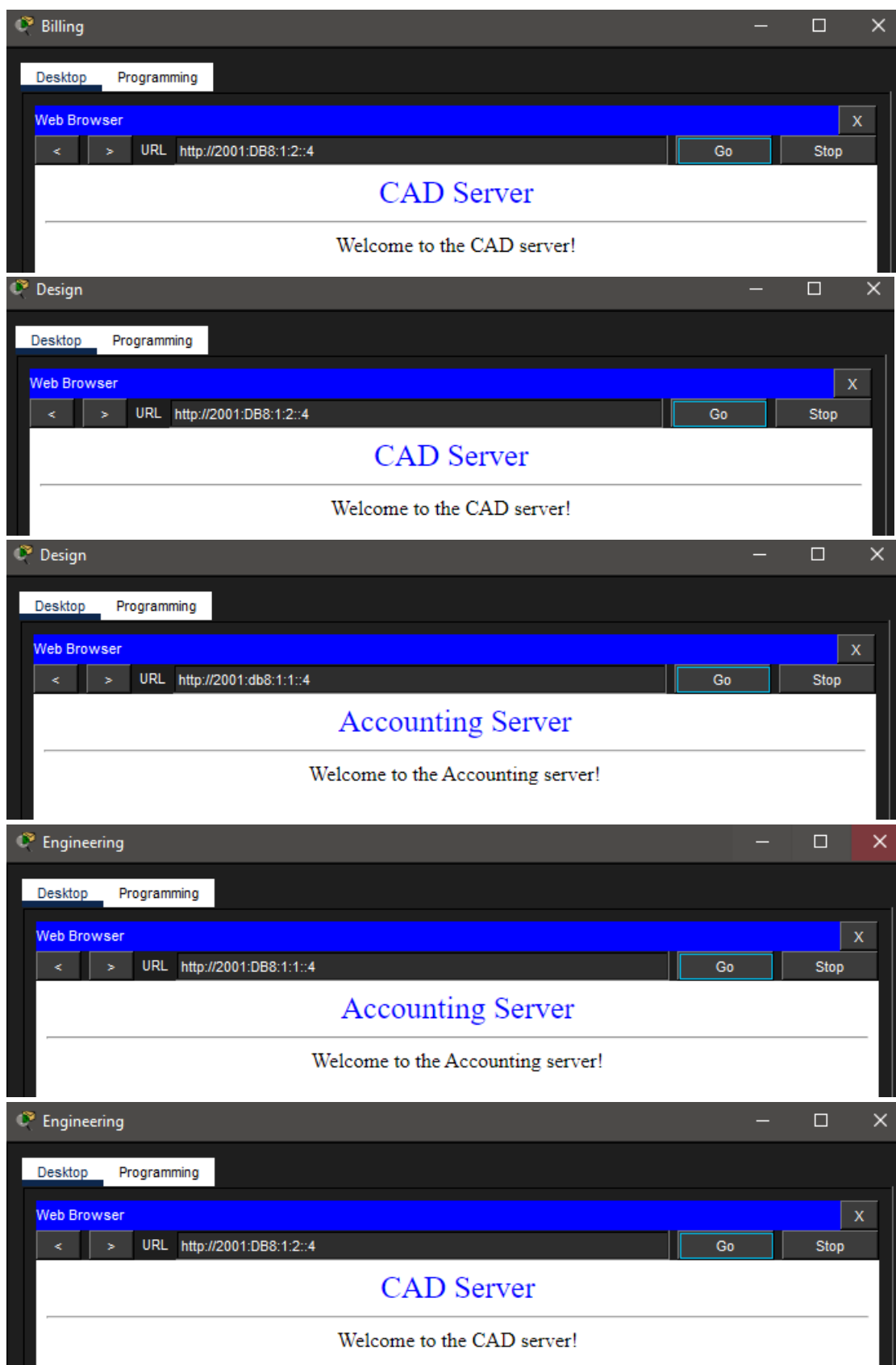


W polu URL wprowadzamy 2001:DB8:1:2::4 i klikamy przycisk Go. Powinna się pojawić strona WWW serwera CAD.



Powtarzamy kroki dla pozostałych klientów.





Klikamy na dowolnego Klienta. Wybieramy zakładkę Desktop > Command Prompt. Testujemy połączenie z ISP, wpisując komendę: K PC> ping 2001:db8:1:a001::1

```
Sales
Desktop Programming
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:1:a001::1

Pinging 2001:db8:1:a001::1 with 32 bytes of data:

Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=14ms TTL=254

Ping statistics for 2001:DB8:1:A001::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 14ms, Average = 4ms

C:\>|
```

```
Billing
Desktop Programming
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:1:a001::1

Pinging 2001:db8:1:a001::1 with 32 bytes of data:

Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254

Ping statistics for 2001:DB8:1:A001::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>|
```

```
Design
Desktop Programming
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:1:a001::1

Pinging 2001:db8:1:a001::1 with 32 bytes of data:

Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=2ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=2ms TTL=254

Ping statistics for 2001:DB8:1:A001::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>|
```

```
Engineering
Desktop Programming
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:1:a001::1

Pinging 2001:db8:1:a001::1 with 32 bytes of data:

Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=5ms TTL=254
Reply from 2001:DB8:1:A001::1: bytes=32 time=1ms TTL=254

Ping statistics for 2001:DB8:1:A001::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>
```

Powtarzamy komendę ping dla pozostałych klientów by w pełni zweryfikować łączność.

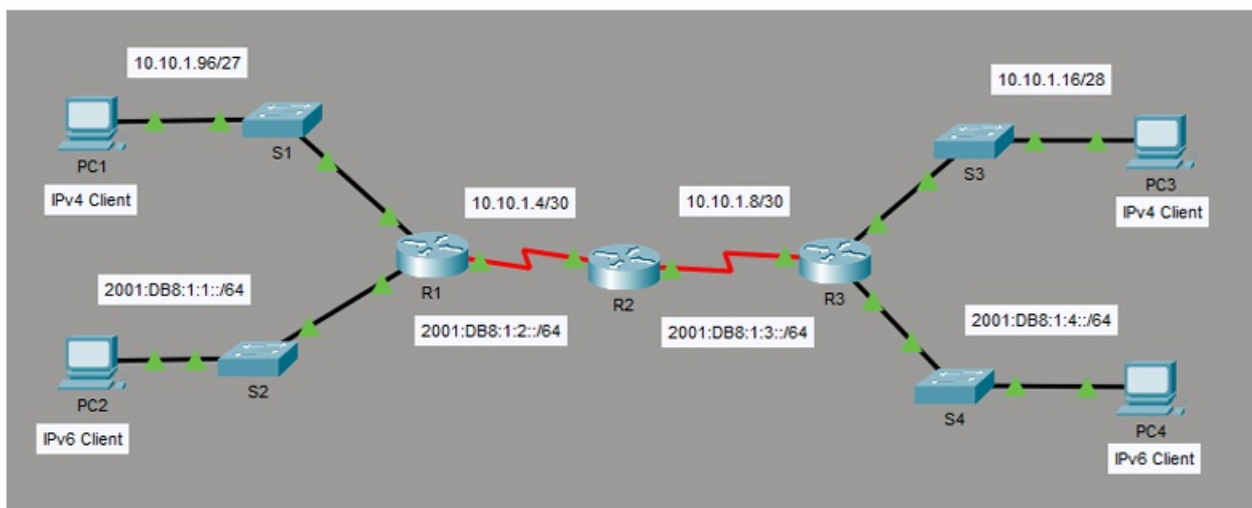
Wnioski

Ćwiczenie to koncentruje się na praktycznym wdrożeniu protokołu IPv6, co wymaga przede wszystkim aktywacji routingu na routerze poleceniem `ipv6 unicast-routing`. Konfiguracja opiera się na przypisaniu interfejsom routera R1 oraz urządzeniom końcowym adresów Global Unicast do komunikacji zewnętrznej oraz adresów Link-Local (`fe80::1`) do komunikacji wewnątrz lokalnych segmentów sieci. Głównym wnioskiem z zadania jest efektywność wykorzystania adresu Link-Local jako bramy domyślnej dla wszystkich hostów, co ujednoliciła konfigurację w różnych podsieciach. Testy końcowe, obejmujące dostęp do stron WWW serwerów Accounting i CAD oraz komunikację z adresem ISP, potwierdzają, że poprawnie zdefiniowana adresacja i routing umożliwiają pełną łączność w nowym standardzie protokołu IP. Istotnym aspektem technicznym jest również fakt, że w IPv6 błędne adresy nie są automatycznie nadpisywane, co wymusza na administratorze ich ręczne usuwanie w celu uniknięcia konfliktów.

PT 13.2.7 Stosowanie komendy ping oraz traceroute do testowania połączeń w sieci

Wstęp teoretyczny

Głównym celem scenariusza jest przywrócenie pełnej łączności w środowiskach IPv4 oraz IPv6 poprzez identyfikację błędów w konfiguracji urządzeń końcowych i pośredniczących. Proces ten rozpoczyna się od zbierania informacji o bieżącym stanie sieci za pomocą narzędzi weryfikacyjnych, takich jak polecenia `ipconfig` i `ipv6config`, które pozwalają na odczytanie przypisanych adresów IP, masek podsieci oraz bram domyślnych. Kluczowym elementem diagnostyki jest wykorzystanie protokołu ICMP poprzez polecenie `ping`, służące do sprawdzania podstawowej drożności kanału komunikacyjnego między hostami. W przypadku wystąpienia awarii, narzędzie `tracert` umożliwia precyzyjne śledzenie trasy pakietu i wskazanie konkretnego urządzenia, na którym następuje przerwanie transmisji. Analiza ta, uzupełniona o wgląd w tablice routingu routerów (polecenie `show ip route`) oraz status ich interfejsów (polecenie `show ip interface brief`), pozwala na wykrycie rozbieżności między stanem faktycznym a dokumentacją techniczną zawartą w tabeli adresowania. Ostatecznym etapem jest wdrożenie odpowiednich poprawek konfiguracyjnych i ponowna weryfikacja stabilności połączeń, co gwarantuje poprawność działania całej infrastruktury sieciowej.



Adresy i prefiksy oraz bramy domyślne dla PC1, PC2, PC3 i PC4 w tabeli zostały uzupełnione ręcznie zgodnie z poleceniami.

Tabela adresowania

Urządzenie	Interfejs	Adres IP/Prefiks		Brama domyślna
R1	G0/0	2001:db8:1:1::1/64		nd
	G0/1	10.10.1.97	255.255.255.224	nd
	S0/0/1	10.10.1.6	255.255.255.252	nd
		2001:db8:1:2::2/64		✓
		fe80::1		
R2	S0/0/0	10.10.1.5	255.255.255.252	nd
		2001:db8:1:2::1/64		✓
	S0/0/1	10.10.1.9	255.255.255.252	nd
		2001:db8:1:3::1/64		✓
		fe80::2		✓
R3	G0/0	2001:db8:1:4::1/64		nd
	G0/1	10.10.1.17	255.255.255.240	nd
	S0/0/1	10.10.1.10	255.255.255.252	nd
		2001:db8:1:3::2/64		✓
		fe80::3		✓
PC1	karta sieciowa	10.10.1.98	255.255.255.224	10.10.1.97
PC2	karta sieciowa	2001:db8:1:1::2		FE80::1
PC3	karta sieciowa	10.10.1.18	255.255.255.240	10.10.1.17
PC4	karta sieciowa	2001:db8:1:4::2		FE80::2

Klikamy PC1 i otwieramy Command Prompt. WPisujemy polecenie ipconfig /all, aby zebrać informacje IPv4.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 0060.47CA.4DEE
    Link-local IPv6 Address.....: FE80::260:47FF:FECA:4DEE
    IPv6 Address.....: ::
    IPv4 Address.....: 10.10.1.98
    Subnet Mask.....: 255.255.255.224
    Default Gateway.....: ::
                                10.10.1.97

    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-B2-33-AD-8B-00-60-47-CA-4D-EE
    DNS Servers.....: ::
                                0.0.0.0
```

Powtarzamy dla PC3.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 0060.7034.6930
    Link-local IPv6 Address.....: FE80::260:70FF:FE34:6930
    IPv6 Address.....: ::
    IPv4 Address.....: 10.10.1.18
    Subnet Mask.....: 255.255.255.240
    Default Gateway.....: ::
                        10.10.1.17
    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-82-76-04-5A-00-60-70-34-69-30
    DNS Servers.....: ::
                        0.0.0.0

```

Używamy polecenia ping, aby przetestować łączność między PC1 i PC3. Test ping powinien zakończyć się niepowodzeniem.

```

C:\>ping 10.10.1.18

Pinging 10.10.1.18 with 32 bytes of data:

Reply from 10.10.1.97: Destination host unreachable.
Reply from 10.10.1.97: Destination host unreachable.
Reply from 10.10.1.97: Destination host unreachable.
Reply from 10.10.1.97: Destination host unreachable.

Ping statistics for 10.10.1.18:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

W celu zlokalizowania problemu, wykonujemy polecenia tracert z jednego komputera na drugi i z powrotem. PC1 do PC3:

```

C:\>tracert 10.10.1.18

Tracing route to 10.10.1.18 over a maximum of 30 hops:

  1  0 ms      0 ms      0 ms      10.10.1.97
  2  0 ms      *          0 ms      10.10.1.97
  3  *          0 ms      *          Request timed out.
  4  0 ms      *          0 ms      10.10.1.97
  5  *          0 ms      *          Request timed out.
  6  0 ms      *          0 ms      10.10.1.97
  7  *          0 ms      *          Request timed out.
  8  0 ms      *          0 ms      10.10.1.97
  9  *          0 ms      *          Request timed out.
 10  0 ms      *          0 ms      10.10.1.97
 11  *          0 ms      *          Request timed out.
 12  0 ms      *          0 ms      10.10.1.97
 13  *          0 ms      *          Request timed out.
 14  0 ms      *          0 ms      10.10.1.97
 15  *          0 ms      *          Request timed out.
 16  0 ms      *          0 ms      10.10.1.97
 17  *          0 ms      *          Request timed out.
 18  0 ms      *          0 ms      10.10.1.97
 19  *          0 ms      *          Request timed out.
 20  0 ms      *          0 ms      10.10.1.97
 21
Control-C

```

PC3 do PC1:

```

C:\>tracert 10.10.1.98

Tracing route to 10.10.1.98 over a maximum of 30 hops:

  1  0 ms      0 ms      0 ms      10.10.1.17
  2  0 ms      *          0 ms      10.10.1.17
  3  *          0 ms      *          Request timed out.
  4  0 ms      *          0 ms      10.10.1.17
  5  *          0 ms      *          Request timed out.
  6  0 ms      *          0 ms      10.10.1.17
  7
Control-C

```

W dalszym poszukiwaniu problemu, logujemy się do Routera 1 oraz Routera 2 za pomocą haseł podanych na początku instrukcji. Po zalogowaniu się używamy komend show ip interface brief, aby zobaczyć informacje odnośnie interfejsów oraz show ip route do wyświetlenia sieci podłączonych pod router.

Router 1:

```

User Access Verification

Password:

R1>enable
Password:
R1#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/1	10.10.1.97	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	10.10.1.6	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

```

R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.10.1.4/30 is directly connected, Serial0/0/1
L       10.10.1.6/32 is directly connected, Serial0/0/1
C       10.10.1.96/27 is directly connected, GigabitEthernet0/1
L       10.10.1.97/32 is directly connected, GigabitEthernet0/1

```

Router 2:

```

User Access Verification

Password:

R2>enable
Password:
R2#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	10.10.1.2	YES	manual	up	up
Serial0/0/1	10.10.1.9	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 6 subnets, 4 masks
C      10.10.1.4/30 is directly connected, Serial0/0/0
L      10.10.1.5/32 is directly connected, Serial0/0/0
C      10.10.1.8/30 is directly connected, Serial0/0/1
L      10.10.1.9/32 is directly connected, Serial0/0/1
D      10.10.1.16/28 [90/2170112] via 10.10.1.10, 00:00:15, Serial0/0/1
D      10.10.1.96/27 [90/2170112] via 10.10.1.6, 00:00:12, Serial0/0/0
```

-(2a) Jaki jest ostatni osiągnięty adres IPv4?

10.10.1.97 -(2c) Jaki jest ostatni osiągnięty adres IPv4? 10.10.1.17 -(2f) Jaki jest drugi? 10.10.1.6 -(2g) Jakie to pozycje? 10.10.1.4/30 typu C oraz 10.10.1.6/32 typu L -(2h) Jakie to pozycje? 10.10.1.8/30 typu C oraz 10.10.1.10/32 typu L

Porównujemy odpowiedzi z kroku 2 do danych z dokumentacji, którą mamy dostępną dla tej sieci. - Jaki jest błąd?

Adres IPv4 dla Routera R2 w interfejsie S0/0/0 jest inny niż w dokumentacji. - Jakie rozwiązanie proponujesz, aby rozwiązać problem? Zmiana adresu.

Teraz wykonujemy nasz plan.

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Serial0/0/0
R2(config-if)#no ipv4 address 10.10.1.2
^
% Invalid input detected at '^' marker.

R2(config-if)#no ip address 10.10.1.2
R2(config-if)#ip address 10.10.1.5
% Incomplete command.
R2(config-if)#ip address 10.10.1.5 255.255.255.252
R2(config-if)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.1.6 (Serial0/0/0) is up: new adjacency

R2(config-if)#no shutdown
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Upewniamy że łączność została przywrócona. Testujemy łączność z PC1 do PC3, a następnie z PC3 do PC1.

```
C:\>ping 10.10.1.18

Pinging 10.10.1.18 with 32 bytes of data:

Reply from 10.10.1.18: bytes=32 time=2ms TTL=125
Reply from 10.10.1.18: bytes=32 time=2ms TTL=125
Reply from 10.10.1.18: bytes=32 time=2ms TTL=125
Reply from 10.10.1.18: bytes=32 time=2ms TTL=125

Ping statistics for 10.10.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

```
C:\>ping 10.10.1.98

Pinging 10.10.1.98 with 32 bytes of data:

Reply from 10.10.1.98: bytes=32 time=2ms TTL=125
Reply from 10.10.1.98: bytes=32 time=2ms TTL=125
Reply from 10.10.1.98: bytes=32 time=2ms TTL=125
Reply from 10.10.1.98: bytes=32 time=2ms TTL=125

Ping statistics for 10.10.1.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

-Czy problem został rozwiązany?

Problem został rozwiązany, co potwierdzają pingi.

Klikamy PC2 i otwórz Command Prompt, wprowadzamy polecenie `ipv6config /all`, aby zebrać informacje o IPv6.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipv6config /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 00E0.B035.82B8
Link-local IPv6 Address.....: FE80::2E0:B0FF:FE35:82B8
IPv6 Address.....: 2001:DB8:1:1::2
Default Gateway.....: FE80::1
DNS Servers.....: ::
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-15-A9-3E-85-00-E0-B0-35-82-B8

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 0001.4391.C48B
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
Default Gateway.....: ::
DNS Servers.....: ::
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-15-A9-3E-85-00-E0-B0-35-82-B8
```

Powtarzamy na PC4:

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipv6config /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0006.2ABC.7CD4
Link-local IPv6 Address.....: FE80::206:2AFF:FEBC:7CD4
IPv6 Address.....: 2001:DB8:1:4::2
Default Gateway.....: FE80::2
DNS Servers.....: ::
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-54-60-98-B7-00-06-2A-BC-7C-D4

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address.....: 00D0.FF7D.AD44
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
Default Gateway.....: ::
DNS Servers.....: ::
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-54-60-98-B7-00-06-2A-BC-7C-D4

```

Testujemy łączność między PC2 i PC4. Ten test ping znowu zakończył się niepowodzeniem.

```

C:\>ping 2001:db8:1:4::2

Pinging 2001:db8:1:4::2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:1:4::2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Lokalizujemy źródło problemu. Tak jak w poprzedniej części zadania problem leży w komunikacji pomiędzy tymi dwoma urządzeniami. W celu weryfikacji problemu ponownie używamy polecenia tracert z jednego urządzenia na drugie. PC2 do PC4:

```

C:\>tracert 2001:db8:1:4::2

Tracing route to 2001:db8:1:4::2 over a maximum of 30 hops:

  1    1 ms    0 ms    0 ms    2001:DB8:1:1::1
  2    0 ms    0 ms    1 ms    2001:DB8:1:2::1
  3    0 ms    2 ms    0 ms    2001:DB8:1:3::2
  4    *        *        *        Request timed out.
  5    *        *        *        Request timed out.
  6

Control-C

```

PC4 do PC2:

```

Tracing route to 2001:DB8:1:1::2 over a maximum of 30 hops:

  1    *        *        *        Request timed out.
  2    *        *        *        Request timed out.
  3    *        *        *        Request timed out.
  4    *

Control-C

```

W kolejnych próbach rozpoznania problemu, nastąpiło zalogowanie do Routera 3 oraz Routera 1. Dla routera 1:

User Access Verification

Password:

R1>enable

Password:

R1#show ipv6 interface brief

```
GigabitEthernet0/0      [up/up]
    FE80::1
    2001:DB8:1:1::1
GigabitEthernet0/1      [up/up]
    unassigned
Serial0/0/0              [administratively down/down]
    unassigned
Serial0/0/1              [up/up]
    FE80::1
    2001:DB8:1:2::2
Vlan1                    [administratively down/down]
    unassigned
```

Dla router 3:

User Access Verification

Password:

R3>enable

Password:

R3#show ipv6 interface brief

```
GigabitEthernet0/0      [up/up]
    FE80::3
    2001:DB8:1:4::1
GigabitEthernet0/1      [up/up]
    unassigned
Serial0/0/0              [administratively down/down]
    unassigned
Serial0/0/1              [up/up]
    FE80::3
    2001:DB8:1:3::2
Vlan1                    [administratively down/down]
    unassigned
```

User Access Verification

Password:

R3>enable

Password:

R3#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/1	10.10.1.17	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	10.10.1.10	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

R3#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C 10.10.1.8/30 is directly connected, Serial0/0/1
L 10.10.1.10/32 is directly connected, Serial0/0/1
C 10.10.1.16/28 is directly connected, GigabitEthernet0/1
L 10.10.1.17/32 is directly connected, GigabitEthernet0/1

-(2a) Jaki jest ostatni osiągnięty adres IPv6?

2001:DB8:1:3::2 -(2c) Jaki jest ostatni osiągnięty adres IPv6? Nie został osiągnięty żaden adres. - Czy jest inaczej? Nie ma żadnego adresu zgodnego z bramą zapisaną we wcześniejszym poleceniu.

Brama domyślna adresu IPv6 na komputerze PC4 nie zgadza się. Propozycją rozwiązania problemu jest jej zmiana tak, aby była zgodna z bramą domyślną Routera R3.

IPv6 Configuration

☒ Automatic☒ Static

IPv6 Address

2001:DB8:1:4::2 / 64

Link Local Address

FE80::206:2AFF:FEBC:7CD4

Default Gateway

FE80::3

DNS Server

802.1X

Przed rozwiązaniem problemu adres był niezgodny z tym z tabeli adresowania, natomiast o zmianie pingi się udało. Oznacza to całkowite wyeliminowanie problemu PC2 do PC4:

```
C:\>ping 2001:db8:1:4::2

Pinging 2001:db8:1:4::2 with 32 bytes of data:

Reply from 2001:DB8:1:4::2: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:4::2: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:4::2: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:4::2: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:4::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

PC4 do PC2:

```
C:\>ping 2001:DB8:1:1::2

Pinging 2001:DB8:1:1::2 with 32 bytes of data:

Reply from 2001:DB8:1:1::2: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:1::2: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:1::2: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:1::2: bytes=32 time=3ms TTL=125

Ping statistics for 2001:DB8:1:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Wnioski

Na podstawie przeprowadzonych czynności diagnostycznych w ramach instrukcji można stwierdzić, że kluczem do sprawnego funkcjonowania sieci jest ścisła zgodność konfiguracji z dokumentacją techniczną. Ćwiczenie wykazało, że narzędzia takie jak ping i tracert są niezbędne do precyzyjnego lokalizowania punktów awarii. Pozwoliły one ustalić, że w przypadku IPv4 problemem był błędny adres IP na interfejsie szeregowym routera R2, natomiast w części dotyczącej IPv6 przyczyną braku łączności była nieprawidłowo skonfigurowana brama domyślna na komputerze PC4. Skuteczna naprawa wymagała systematycznej analizy statusu interfejsów oraz tablic routingu, co pozwoliło na wykrycie rozbieżności i wdrożenie poprawek przywracających pełną drożność kanałów komunikacyjnych. Ostateczne testy potwierdziły, że prawidłowe adresowanie, uwzględniające techniki takie jak VLSM oraz właściwe przypisanie bram domyślnych, stanowi fundament stabilnej i wydajnej infrastruktury sieciowej.