



## Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego
- 3 Protokoły i modele
- 4 Warstwa fizyczna
- 5 Systemy liczbowe
- 6 Warstwa łącza danych
- 7 Przełączanie w sieciach Ethernet
- 8 Warstwa sieci
- 9 Odzworowanie adresów

[🏠](#) / [Budowanie małej sieci](#) / [Przykłady rozwiązywania problemów](#)

# Przykłady rozwiązywania problemów

17.7.1

## Problemy z działaniem duplexu i kwestie niezgodności

Wiele typowych problemów sieciowych można zidentyfikować i rozwiązać przy niewielkim wysiłku. Teraz, gdy znasz narzędzia i proces rozwiązywania problemów z siecią, w tym temacie omówiono niektóre typowe problemy z siecią, które prawdopodobnie napotkasz jako administrator sieci.

W komunikacji danych, *dupleks* odnosi się do kierunku transmisji danych między dwoma urządzeniami.

Istnieją dwa tryby komunikacji duplex:

- **Półdupleks** - Komunikacja jest ograniczona do wymiany danych w jednym kierunku na raz.
- **Pełny duplex** - Komunikacja może być wysyłana i odbierana jednocześnie.

Rysunek ilustruje, jak działa każda metoda duplexu.

## Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ☐
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego ☐
- 3 Protokoły i modele ☐
- 4 Warstwa fizyczna ☐
- 5 Systemy liczbowe ☐
- 6 Warstwa łącza danych ☐
- 7 Przełączanie w sieciach Ethernet ☐
- 8 Warstwa sieci ☐
- 9 Odzworowanie adresów ☐

## Techniki negocjacji trybu pełnego duplexu

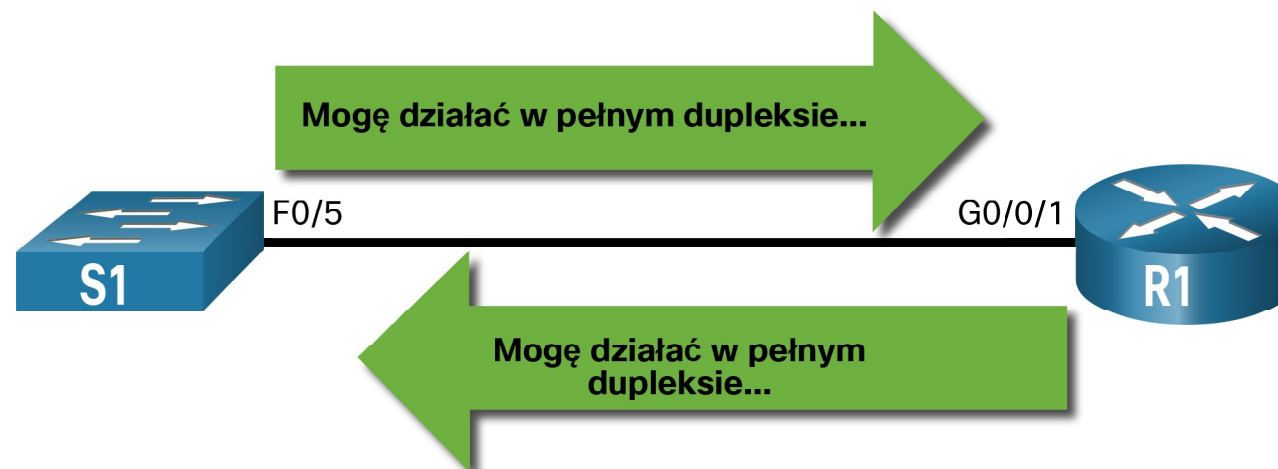


Interfejsy łączące Ethernet muszą działać w tym samym trybie duplexu, aby zapewnić najlepszą wydajność komunikacji oraz uniknąć nieefektywności i opóźnień łącza.

Funkcja automatycznej negocjacji Ethernet ułatwia konfigurację, minimalizuje problemy i maksymalizuje wydajność łącza między dwoma połączonymi łączami Ethernet. Podłączone urządzenia najpierw ogłaszają obsługiwane tryby, a następnie wybierają tryb najwyższej wydajności obsługiwany przez oba końce. Na przykład przełącznik i router na rysunku pomyślnie negocjuje tryb pełnego duplexu.

## Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś ▼
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego ▼
- 3 Protokoły i modele ▼
- 4 Warstwa fizyczna ▼
- 5 Systemy liczbowe ▼
- 6 Warstwa łącza danych ▼
- 7 Przełączanie w sieciach Ethernet ▼
- 8 Warstwa sieci ▼
- 9 Odzworowanie adresów ▼



Jeśli jedno z dwóch podłączonych urządzeń działa w pełnym duplexie, a drugie działa w półduplexie, występuje niezgodność duplexu. Podczas gdy komunikacja danych nastąpi za pośrednictwem łącza z niedopasowaniem duplexu, wydajność łącza będzie bardzo słaba.

Niedopasowanie duplexu jest zwykle spowodowane błędnie skonfigurowanym interfejsem lub w rzadkich przypadkach nieudaną auto-negocjacją. Rozbieżności duplexu mogą być trudne do rozwiązania, ponieważ komunikacja między urządzeniami nadal występuje.

17.7.2

## Kwestie adresacji IP na urządzeniach IOS



Problemy związane z adresami IP prawdopodobnie powstrzymają komunikację zdalnych urządzeń sieciowych. Ponieważ adresy IP są hierarchiczne, każdy adres IP przypisany do urządzenia sieciowego musi być zgodny z zakresem adresów dla danej sieci. Nieprawidłowo przypisane adresy IP tworzą różne problemy, w tym konflikty adresów IP i problemy z routingiem.

Dwie najczęstsze przyczyny nieprawidłowego przypisania IPv4 to błędy przypisania ręcznego lub problemy związane z DHCP.

Administratorzy sieci często muszą ręcznie przypisywać adresy IP urządzeniom takim jak serwery i routery. Jeśli podczas

## Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 3 Protokoły i modele 
- 4 Warstwa fizyczna 
- 5 Systemy liczbowe 
- 6 Warstwa łącza danych 
- 7 Przełączanie w sieciach Ethernet 
- 8 Warstwa sieci 
- 9 Odzworowanie adresów 

przypisania zostanie popełniony błąd, najprawdopodobniej wystąpią problemy z komunikacją z urządzeniem.

Na urządzeniu z systemem IOS użyj polecenia **show ip interface** lub **show ip interface brief**, aby sprawdzić, jakie adresy IPv4 są przypisane do interfejsów sieciowych. Na przykład, wydawanie polecenia **show ip interface brief**, jak pokazano, pozwoli sprawdzić stan interfejsu na R1.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	209.165.200.225	YES	manual	up	up
GigabitEthernet0/0/1	192.168.10.1	YES	manual	up	up
Serial0/1/0	unassigned	NO	unset	down	down
Serial0/1/1	unassigned	NO	unset	down	down
GigabitEthernet0	unassigned	YES	unset	administratively down	down

```
R1#
```

17.7.3

## Kwestie adresacji IP na urządzeniach końcowych



Na komputerach z systemem Windows, gdy urządzenie nie może skontaktować się z serwerem DHCP, system Windows automatycznie przypisze adres należący do zakresu 169.254.0.0/16. Ta funkcja nazywa się automatycznym prywatnym adresowaniem IP (APIPA) i ma na celu ułatwienie komunikacji w sieci lokalnej. Pomyśl o tym, jakby Windows mówił: „Użyję tego adresu z zakresu 169.254.0.0/16, ponieważ nie mogłem uzyskać żadnego innego adresu”.

Często komputer z adresem APIPA nie będzie w stanie komunikować się z innymi urządzeniami w sieci, ponieważ najprawdopodobniej te urządzenia nie będą należeć do sieci 169.254.0.0/16. Ta sytuacja wskazuje na problem z automatycznym przypisaniem adresu IPv4, który powinien zostać naprawiony.

**Uwaga:** Inne systemy operacyjne, takie jak Linux i OS X, nie przypisują adresu IPv4 do interfejsu sieciowego, jeśli komunikacja z serwerem DHCP nie powiedzie się.

Większość urządzeń końcowych jest skonfigurowana tak, aby polegała na serwerze DHCP do automatycznego przypisywania adresów IPv4. Jeśli urządzenie nie może komunikować się z serwerem DHCP, serwer nie może przypisać adresu IPv4 dla określonej sieci, a urządzenie nie będzie w stanie komunikować się.

## Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 3 Protokoły i modele 
- 4 Warstwa fizyczna 
- 5 Systemy liczbowe 
- 6 Warstwa łącza danych 
- 7 Przełączanie w sieciach Ethernet 
- 8 Warstwa sieci 
- 9 Odzworowanie adresów 

Aby zweryfikować adresy IP przypisane do komputera z systemem Windows, użyj polecenia **ipconfig**, jak pokazuje wyjście.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
    IPv4 Address. . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
(Output omitted)
```

17.7.4

## Kwestie bramy domyślnej



Domyślną bramą urządzenia końcowego jest najbliższe urządzenie sieciowe, które może przesyłać ruch do innych sieci. Jeśli urządzenie ma nieprawidłowy lub nieistniejący adres bramy domyślnej, nie będzie w stanie komunikować się z urządzeniami w sieciach zdalnych. Ponieważ brama domyślna jest ścieżką do sieci zdalnych, jej adres musi należeć do tej samej sieci co urządzenie końcowe.

Adres bramy domyślnej można ustawić ręcznie lub uzyskać z serwera DHCP. Podobnie jak w przypadku problemów związanych z protokołem IPv4, problemy z bramą domyślną mogą być związane z błędną konfiguracją (w przypadku przypisania ręcznego) lub problemami DHCP (jeśli automatyczne przypisanie jest używane).

Aby rozwiązać problemy ze źle skonfigurowanymi bramami domyślnymi, upewnij się, że w urządzeniu skonfigurowano poprawną bramę domyślną. Jeśli adres bramy został ustawiony ręcznie, ale jest niepoprawny, po prostu zastąp go odpowiednim adresem. Jeśli adres bramy domyślnej został ustawiony automatycznie, upewnij się, że urządzenie może komunikować się z serwerem DHCP. Ważne jest również sprawdzenie, czy właściwy adres IPv4 i maska podsieci zostały skonfigurowane na interfejsie routera i czy interfejs jest aktywny.

Aby zweryfikować bramę domyślną na komputerach z systemem Windows, użyj polecenia **ipconfig** w pokazany sposób.

## Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 3 Protokoły i modele 
- 4 Warstwa fizyczna 
- 5 Systemy liczbowe 
- 6 Warstwa łącza danych 
- 7 Przełączanie w sieciach Ethernet 
- 8 Warstwa sieci 
- 9 Odwzorowanie adresów 

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
    IPv4 Address. . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
(Output omitted)
```

Na routerze użyj polecenia **show ip route**, aby wyświetlić tablicę routingu i sprawdzić, czy ustawiono bramę domyślną, znaną jako trasa domyślna. Ta trasa jest używana, gdy adres docelowy pakietu nie pasuje do żadnej innej trasy w tablicy routingu.

Na przykład dane wyjściowe weryfikują, czy R1 ma skonfigurowaną bramę domyślną (tj. Bramę ostatniej szansy) wskazującą adres IP 209.168.200.226.



Pierwsza podświetlona linia zasadniczo mówi, że brama do dowolnej sieci (tj. 0.0.0.0) biegnie przez adres IP 209.165.200.226. Drugi podświetlony pokazuje, jak R1 dowiedział się o bramie domyślnej. W tym przypadku R1 otrzymał informacje od innego routera obsługującego OSPF.

17.7.5

## Rozwiązywanie problemów z DNS



Usługa nazw domen (DNS) definiuje zautomatyzowaną usługę, która dopasowuje nazwy, takie jak [www.cisco.com](http://www.cisco.com), do adresu IP. Chociaż odwzorowanie DNS nie jest kluczowe dla komunikacji z urządzeniami, jest bardzo ważne dla użytkownika końcowego.

Często zdarza się, że użytkownicy błędnie odnoszą działanie łącza internetowego do dostępności DNS. Skargi użytkowników, takie jak „sieć jest wyłączona” lub „Internet jest wyłączony”, są często powodowane przez nieosiągalny serwer DNS. Podczas

## Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 3 Protokoły i modele 
- 4 Warstwa fizyczna 
- 5 Systemy liczbowe 
- 6 Warstwa łącza danych 
- 7 Przełączanie w sieciach Ethernet 
- 8 Warstwa sieci 
- 9 Odzworowanie adresów 

gdy routing pakietów i wszystkie inne usługi sieciowe nadal działają, awarie DNS często prowadzą użytkownika do błędnego wniosku. Jeśli użytkownik wpisze nazwę domeny, taką jak [www.cisco.com](http://www.cisco.com) w przeglądarce internetowej, a serwer DNS jest nieosiągalny, nazwa nie zostanie przetłumaczona na adres IP, a witryna nie zostanie wyświetlona.

Adresy serwerów DNS można przypisać ręcznie lub automatycznie. Administratorzy sieci często odpowiadają za ręczne przypisywanie adresów serwerów DNS na serwerach i innych urządzeniach, natomiast DHCP służy do automatycznego przypisywania adresów serwerów DNS klientom.

Mimo że firmy i organizacje często zarządzają własnymi serwerami DNS, do rozpoznawania nazw można używać dowolnego dostępnego serwera DNS. Użytkownicy małych biurowych i domowych biur (SOHO) często polegają na serwerze DNS prowadzonym przez dostawcę usług internetowych w celu rozpoznawania nazw. Serwery DNS utrzymywane przez ISP są przypisywane do klientów SOHO za pośrednictwem DHCP. Ponadto Google utrzymuje publiczny serwer DNS, który może być używany przez każdego i jest bardzo przydatny do testowania. Adres IPv4 publicznego serwera DNS Google to 8.8.8.8 i 2001:4860:4860::8888 dla adresu IPv6 DNS.

Cisco oferuje OpenDNS, który zapewnia bezpieczną usługę DNS poprzez filtrowanie phishingu i niektórych witryn złośliwego oprogramowania. Adres DNS można zmienić na 208.67.222.222 i 208.67.220.220 w polach Preferowany serwer DNS i Alternatywny serwer DNS. Zaawansowane funkcje, takie jak filtrowanie treści internetowych i bezpieczeństwo, są dostępne dla rodzin i firm.

Użyj metody **ipconfig /all** pokazanej, aby sprawdzić, który serwer DNS jest używany przez komputer z systemem Windows.

```
C:\Users\PC-A> ipconfig /all
(Output omitted)
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix . . : 
    Description . . . . . : Intel(R) Dual Band Wireless-AC 8265
    Physical Address. . . . . : F8-94-C2-E4-C5-0A
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
    IPv4 Address. . . . . : 192.168.10.10(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : August 17, 2019 1:20:17 PM
    Lease Expires . . . . . : August 18, 2019 1:20:18 PM
    Default Gateway . . . . . : 192.168.10.1
    DHCP Server . . . . . : 192.168.10.1
    DHCPv6 IAID . . . . . : 100177090
    DHCPv6 Client DUID. . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
    DNS Servers . . . . . : 208.67.222.222
```

## Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 3 Protokoły i modele 
- 4 Warstwa fizyczna 
- 5 Systemy liczbowe 
- 6 Warstwa łącza danych 
- 7 Przełączanie w sieciach Ethernet 
- 8 Warstwa sieci 
- 9 Odwzorowanie adresów 

```
NetBIOS over Tcpi. . . . . : Enabled
(Output omitted)
```

Polecenie **nslookup** to kolejne przydatne narzędzie do rozwiązywania problemów z DNS dla komputerów. Użytkownik może ręcznie umieszczać zapytania DNS przy pomocy **nslookup** i analizować odpowiedź DNS. Polecenie **nslookup** pokazuje wyjście dla zapytania dla [www.cisco.com](https://www.cisco.com). Zauważ, że możesz również po prostu wprowadzić adres IP i **nslookup** odwzorować nazwę.

```
C:\Users\PC-A> nslookup
Default Server:  Home-Net
Address:  192.168.1.1
> cisco.com
Server:  Home-Net
Address:  192.168.1.1
Non-authoritative answer:
Name:    cisco.com
Addresses:  2001:420:1101:1::185
           72.163.4.185
> 8.8.8.8
Server:  Home-Net
Address:  192.168.1.1
Name:    dns.google
Address:  8.8.8.8
>
> 208.67.222.222
Server:  Home-Net
Address:  192.168.1.1
Name:    resolver1.opendns.com
Address:  208.67.222.222
>
```

17.7.6

## Laboratorium - Rozwiązywanie problemów z łącznością





## Wprowadzenie do sieci

- 1 Komunikacja sieciowa dziś 
- 2 Podstawy konfiguracji przełącznika i urządzenia końcowego 
- 3 Protokoły i modele 
- 4 Warstwa fizyczna 
- 5 Systemy liczbowe 
- 6 Warstwa łącza danych 
- 7 Przełączanie w sieciach Ethernet 
- 8 Warstwa sieci 
- 9 Odzworowanie adresów 

Celem tego ćwiczenia jest realizacja następujących zadań:

- Zidentyfikować problem
- Wprowadzić zmiany w sieci
- Sprawdzić pełną funkcjonalność
- Udokumentować ustalenia i zmiany konfiguracji

 Rozwiązywanie problemów z łącznością

17.7.7

## Packet Tracer - Rozwiązywanie problemów z łącznością

Celem tego ćwiczenia Packet Tracer jest rozwiązywanie problemów z łącznością, jeśli to możliwe. W przeciwnym razie kwestie powinny być jasno udokumentowane i tak można je eskalować.

 Rozwiązywanie problemów z łącznością

 Rozwiązywanie problemów z łącznością



17.6

Metodologie rozwiązywania problemów

17.8

Moduł ćwiczeń i quizów 