

**KURS**

**Wydanie II**

**Witold Wrotek**



# SIECI KOMPUTEROWE

**Zbuduj swoją własną sieć  
— to naprawdę proste!**

Jak utworzyć i skonfigurować własną sieć komputerową?  
Jak udostępniać zasoby i kontrolować dostęp do sieci?  
Jak zabezpieczyć sieć przed zagrożeniami  
i blokować niewłaściwe treści?

**Helion**

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Redaktor prowadzący: Michał Mrowiec

Wydawnictwo HELION

ul. Kościuszki 1c, 44-100 GLIWICE

tel. 32 231 22 19, 32 230 98 63

e-mail: [helion@helion.pl](mailto:helion@helion.pl)

WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<http://helion.pl/user/opinie/sieku2>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Kody źródłowe wybranych przykładów dostępne są pod adresem:

<ftp://ftp.helion.pl/przyklady/sieku2.zip>

ISBN: 978-83-283-2627-9

Copyright © Helion 2016

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

# Spis treści

Wstęp .....	9
Dla kogo jest przeznaczona książka? .....	10
Komputer, smartfon, tablet .....	11
Jaką strukturę ma książka? .....	12
Po co poznawać zasady działania sieci komputerowych? .....	13
<b>Rozdział 1. Jak zaprojektować sieć komputerową? .....</b>	<b>15</b>
Co to jest sieć komputerowa? .....	16
Jaki zasięg ma sieć? .....	17
Co to jest topologia sieci? .....	18
<i>Magistrala</i> .....	18
<i>Pierścień</i> .....	19
<i>Pierścień podwójny</i> .....	20
<i>Gwiazda</i> .....	21
<i>Gwiazda rozszerzona</i> .....	22
<i>Hierarchiczna</i> .....	23
<i>Siatka</i> .....	24
Jakie są media transmisji? .....	25
<i>Kable miedziane</i> .....	25
<i>Kable światłowodowe</i> .....	26
<i>Sieci bezprzewodowe</i> .....	26
Podsumowanie .....	29
Pytania kontrolne .....	30
Zadania do samodzielnego wykonania .....	31
<b>Rozdział 2. Jak wykonać okablowanie? .....</b>	<b>33</b>
Co to są skrętki? .....	34
<i>STP</i> .....	34
<i>FTP</i> .....	35
<i>UTP</i> .....	35
Czym charakteryzują się kable koncentryczne? .....	36
<i>10BASE2</i> .....	37
<i>10BASE5</i> .....	38
Jak wygląda wtyk RJ-45? .....	38
Czym się różnią kable: prosty i skrzyżowany? .....	39
<i>Kabel prosty</i> .....	40
<i>Kabel skrzyżowany</i> .....	43

	<i>Oznaczenie kabli</i> .....	44
	<i>Kontrola kabli</i> .....	45
	Do czego służą gniazdka i korytka? .....	49
	<i>Jakie są rodzaje gniazdek?</i> .....	49
	Podsumowanie .....	50
	Pytania kontrolne .....	51
	Zadania do samodzielnego wykonania .....	52
Rozdział 3.	<i>Jak wybrać, zainstalować i sprawdzić kartę sieciową?</i> .....	53
	Do czego służy karta sieciowa? .....	53
	Jakie są rodzaje kart sieciowych? .....	54
	Jak zainstalować kartę sieciową? .....	55
	Jak sprawdzić poprawność zainstalowania karty? .....	57
	Jak wyłączyć kartę sieciową? .....	60
	Jak sprawdzić, z jaką prędkością pracuje karta sieciowa? .....	63
	Jak zaktualizować sterownik karty sieciowej? .....	72
	Co to jest MAC? .....	74
	Podsumowanie .....	78
	Pytania kontrolne .....	79
	Zadania do samodzielnego wykonania .....	79
Rozdział 4.	<i>Jak połączyć urządzenia sieciowe?</i> .....	81
	Koncentratory, przełączniki i routery? .....	82
	Jak połączyć dwa komputery? .....	83
	Jak podłączyć komputer do gniazda RJ-45? .....	86
	Co to jest koncentrator? .....	88
	Co to jest przełącznik? .....	91
	Router .....	92
	Jak podłączyć urządzenie mobilne do komputera? .....	96
	Podsumowanie .....	98
	Pytania kontrolne .....	99
	Zadania do samodzielnego wykonania .....	99
Rozdział 5.	<i>Jak uruchomić router?</i> .....	101
	Do czego można użyć routera? .....	101
	Jak szybko rozpoznać stan routera? .....	102
	Jak uzyskać dostęp do programu konfiguracyjnego routera? .....	102
	Jak najprościej skonfigurować router? .....	104
	Jak przywrócić domyślne hasło logowania routera? .....	113
	Jak za pośrednictwem urządzenia mobilnego podłączyć komputer do internetu? .....	114

Podsumowanie .....	123
Pytania kontrolne .....	124
Zadania do samodzielnego wykonania .....	124
<b>Rozdział 6. Jak zabezpieczyć router? .....</b>	<b>125</b>
Jaką rolę odgrywa router? .....	125
Czy router ma wpływ na bezpieczeństwo? .....	126
Co daje klonowanie adresów fizycznych? .....	126
Po co zmieniać SSID? .....	128
Czy można ukryć SSID? .....	129
Jak zaszyfrować transmisję? .....	130
Jak zezwolić na dostęp do sieci urządzeniom o określonych adresach fizycznych? .....	131
Czy router może kontrolować milusińskich? .....	133
Jak włączyć zaporę sieciową? .....	135
Jak zmienić hasło dostępu do routera? .....	137
Jak uniemożliwić logowanie spoza LAN? .....	139
Jak wykonać kopię ustawień routera? .....	140
Jak odtworzyć ustawienia routera? .....	141
Jak przywrócić ustawienia fabryczne routera? .....	143
Jak poznać historię operacji wykonywanych przez router? .....	145
Jak odczytać tabelę routingu komputera? .....	146
Podsumowanie .....	147
Pytania kontrolne .....	148
Zadania do samodzielnego wykonania .....	149
<b>Rozdział 7. Jak skonfigurować protokół sieciowy? .....</b>	<b>151</b>
Klasy adresów IP .....	153
Maska podsieci .....	154
Brama domyślna .....	155
Jak włączyć i wyłączyć połączenie sieciowe? .....	155
Jak zmienić nazwę połączenia sieciowego? .....	160
Jak zainstalować protokół IP w wersji 6? .....	162
Czy można skonfigurować protokół IPv6 z wiersza poleceń? .....	165
Jak włączyć i wyłączyć protokół TCP/IP? .....	168
Jak skonfigurować protokół TCP/IP? .....	173
Jak przetestować konfigurację protokołu TCP/IP? .....	183
Podsumowanie .....	188
Pytania kontrolne .....	188
Zadania do samodzielnego wykonania .....	189

Rozdział 8.	Jak wykrywać i usuwać uszkodzenia sieci? .....	191
	Czy zabezpieczenia systemu mogą utrudniać pracę w sieci? .....	192
	Jakie niespodzianki sprawiają kable i połączenia? .....	199
	Jak wykryć połączenie? .....	200
	Jak przetestować stabilność połączenia? .....	201
	Dlaczego strony WWW nie są wyświetlane? .....	202
	Jak wykryć drogę pakietów? .....	205
	Jak zmierzyć przepustowość łącza? .....	206
	Pasmo sieci Wi-Fi urządzenia mobilnego .....	206
	Pasmo sieci GSM urządzenia mobilnego .....	209
	Jak odczytać adres IP i MAC urządzenia mobilnego? .....	212
	Parametry transmisji urządzenia mobilnego .....	214
	Podsumowanie .....	220
	Pytania kontrolne .....	220
	Zadania do samodzielnego wykonania .....	221
Rozdział 9.	Jak zarządzać użytkownikami i grupami? .....	223
	Co to jest konto użytkownika? .....	223
	Co to jest konto gościa? .....	224
	Co to jest grupa użytkowników? .....	224
	Co to jest grupa robocza? .....	225
	Co jest lepsze: grupa robocza czy domena? .....	226
	Czy jest możliwe korzystanie z wielu kont w urządzeniach z systemem Android? .....	239
	Podsumowanie .....	240
	Pytania kontrolne .....	241
	Zadania do samodzielnego wykonania .....	241
Rozdział 10.	Jak udostępniać pliki i foldery? .....	243
	Czemu służy ograniczanie uprawnień? .....	243
	Jakie można mieć uprawnienia? .....	244
	Jak nadać uprawnienia do zasobu? .....	245
	Jak zmienić uprawnienia do zasobu? .....	247
	Jak można udostępniać pliki i foldery? .....	249
	Jak udostępniać folder Publiczny? .....	249
	<i>Gdzie jest folder Publiczny?</i> .....	250
	<i>Co znajduje się w folderze Publiczny?</i> .....	250
	<i>Co umieszczać w folderze Publiczny?</i> .....	251
	Czy udostępnianie folderu Publiczny jest jedynym sposobem na współdzielenie plików w systemie Windows? .....	252
	<i>Jak udostępniać pliki znajdujące się w dowolnym folderze?</i> .....	252

Udostępnianie plików w urządzeniach mobilnych .....	256
Podsumowanie .....	262
Pytania kontrolne .....	263
Zadania do samodzielnego wykonania .....	263
<b>Rozdział 11. Jak udostępnić drukarkę? .....</b>	<b>265</b>
Na co wpływają uprawnienia do drukarek? .....	265
Jak dodać i usunąć drukarkę? .....	266
Jak udostępnić drukarkę? .....	274
Jak uzyskać dostęp do drukarek? .....	275
Jakie ma zadania bufor wydruku? .....	277
Drukowanie z Chrome przez Google Cloud Print .....	281
Podsumowanie .....	284
Pytania kontrolne .....	285
Zadania do samodzielnego wykonania .....	286
<b>Rozdział 12. Jak skonfigurować zabezpieczenia systemowe? .....</b>	<b>287</b>
Co to jest Centrum zabezpieczeń systemu Windows? .....	288
<i>Do czego służy zaporę sieciowa?</i> .....	290
<i>Dlaczego aktualizacje są ważne?</i> .....	296
Jak można chronić komputer przed programami szpiegowskimi? .....	300
Jak zabezpieczyć komputer przed włamaniem podczas przeglądania stron internetowych? .....	305
Do czego można wykorzystać serwer proxy? .....	308
Bezpieczeństwo urządzeń mobilnych .....	311
Podsumowanie .....	320
Pytania kontrolne .....	320
Zadania do samodzielnego wykonania .....	321
<b>Rozdział 13. Jak chronić komputery przed wirusami? .....</b>	<b>323</b>
Czym różnią się wirusy, robaki, trojany i szpiegzy? .....	324
Skąd program antywirusowy czerpie wiedzę o wirusach? .....	325
Co jest największym problemem w walce z wirusami? .....	325
Jaki program antywirusowy zainstalować? .....	326
Skąd wziąć program Norton AntiVirus? .....	326
Jak uaktualnić program antywirusowy? .....	336
Jak wykonać skanowanie? .....	338
Jak Norton Security reaguje na wirusa? .....	340
Antywirus dla urządzeń mobilnych .....	342
Podsumowanie .....	348

Pytania kontrolne .....	349
Zadania do samodzielnego wykonania .....	350
Rozdział 14. Jak blokować wyświetlanie reklam? .....	351
Jak włączyć funkcję blokowania wyskakujących okien? .....	352
Jak sprawdzić skuteczność blokowania wyskakujących okien? .....	353
Jak sprawdzić, co próbowało wyświetlić wyskakujące okno? .....	354
Urządzenia mobilne .....	355
Podsumowanie .....	361
Pytania kontrolne .....	361
Zadania do samodzielnego wykonania .....	362
Rozdział 15. Jak wykorzystać zaporę sieciową? .....	363
Jak sprawdzić ustawienia zapory sieciowej? .....	364
Jak stworzyć wyjątek dla programu? .....	369
Jak utworzyć wyjątek dla portu? .....	372
Zapora sieciowa w urządzeniach mobilnych .....	378
Podsumowanie .....	387
Pytania kontrolne .....	388
Zadania do samodzielnego wykonania .....	388
Dodatek A Odpowiedzi na pytania .....	389
Dodatek B Lista serwerów proxy .....	FTP
Dodatek C Wybrane polecenia ułatwiające pracę w sieci .....	FTP



W tym rozdziale poznasz odpowiedzi na następujące pytania:

- Jak spowodować, aby zapora sieciowa nie blokowała użytecznych programów?
- Jak wykryć połączenie i sprawdzić jego stabilność?
- Jak wyznaczyć drogę pakietów?
- Jak zmierzyć przepustowość łącza?

# 8

## Jak wykrywać i usuwać uszkodzenia sieci?

Aby sieć działała poprawnie, konieczne jest:

- wykonanie okablowania,
- poprawne zmontowanie i podłączenie sprzętu,
- zainstalowanie i skonfigurowanie oprogramowania.

Dopiero gdy wszystkie elementy są sprawne i mają odpowiednio dobrane parametry, sieć działa stabilnie i z zakładaną przepustowością.

Co jednak robić, gdy brak jest połączenia lub sieć działa niestabilnie?

Najłatwiej jest znaleźć przyczynę całkowitej niesprawności. Może to być wtyk wysunięty z gniazdka lub ustawienie zapory sieciowej, które powoduje blokowanie ruchu.

Większym wyzwaniem są niesprawności, które pojawiają się i znikają. Ich przyczyną może być brak kontaktu, przegrzewanie się urządzenia, uszkodzony lub zbyt długi kabel itp.

Usunięcie uszkodzenia w sieci wymaga cierpliwości i systematyczności. Nie wolno po prostu zakładać, że coś jest sprawne, lecz wszystko trzeba sprawdzić

eksperymentalnie. Zwykle nasze założenie okazuje się błędne, a to przysparza to wiele dodatkowej pracy i powoduje stratę czasu.

Jeżeli mamy podejrzenia co do sprawności elementu, trzeba zastąpić go innym, sprawnym. Po wymianie należy sprawdzić działanie sieci. Problem pojawia się, gdy podejrzewamy nieprawidłowe działanie np. routera, a nie dysponujemy innym. W takim przypadku trzeba poszukać ratunku u znajomych lub poprosić o pomoc fachowca.

## Czy zabezpieczenia systemu mogą utrudniać pracę w sieci?

System Windows 7 jest wyposażony w wiele systemów zabezpieczeń: *Kontrola rodzicielska*, *Opcje internetowe*, *Zapora systemu Windows*.

Zadaniem zapory sieciowej jest między innymi blokowanie połączeń, które mogą być niebezpieczne. Gdy zapora wykrywa nowe połączenie, prosi użytkownika o podjęcie decyzji, czy jest ono bezpieczne, czy też nie. Jeżeli omyłkowo zostanie ono zakwalifikowane do połączeń niechcianych, wówczas będzie blokowane. Aby sprawdzić, czy zapora sieciowa blokuje połączenie, trzeba ją wyłączyć, a następnie ponownie spróbować uruchomić usługę, z którą wystąpił kłopot.

Podobnie sprawa przedstawia się z pozostałymi systemami zabezpieczeń. Mają za zadanie chronić komputer, jednak omyłkowo wprowadzona reguła spowoduje blokowanie usług pożądanых.

Zasada postępowania sprowadza się do:

- wyłączenia zabezpieczenia,
- sprawdzenia, czy problem ustąpił.

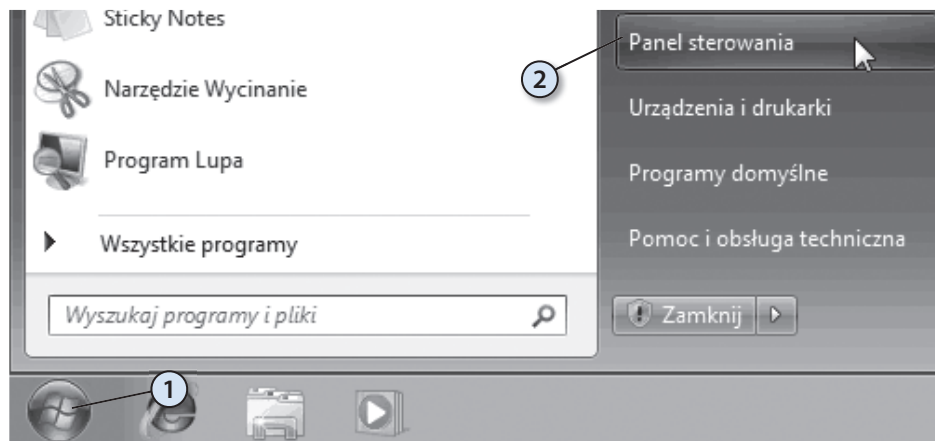
Gdy znajdziemy zabezpieczenie, które było zbyt restrykcyjne, należy z niego zrezygnować lub spowodować, aby nie blokowało potrzebnej usługi.



Za każdym razem trzeba zwalniać tylko jedno zabezpieczenie i sprawdzać jego wpływ na system. Gdy zwolnimy więcej niż jedno zabezpieczenie, nie będziemy mogli ustalić, które blokowało usługę.

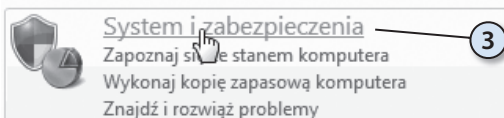
Aby wyłączyć zaporę sieciową:

1. Kliknij przycisk *Start*.
2. Po rozwinięciu menu kliknij przycisk *Panel sterowania*.

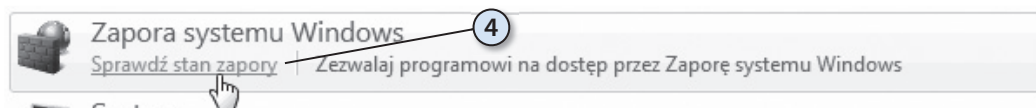


3. W Panelu sterowania odszukaj pozycję *System i zabezpieczenia*. Kliknij odsyłacz.

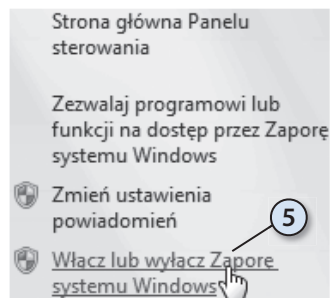
Dostosuj ustawienia komputera

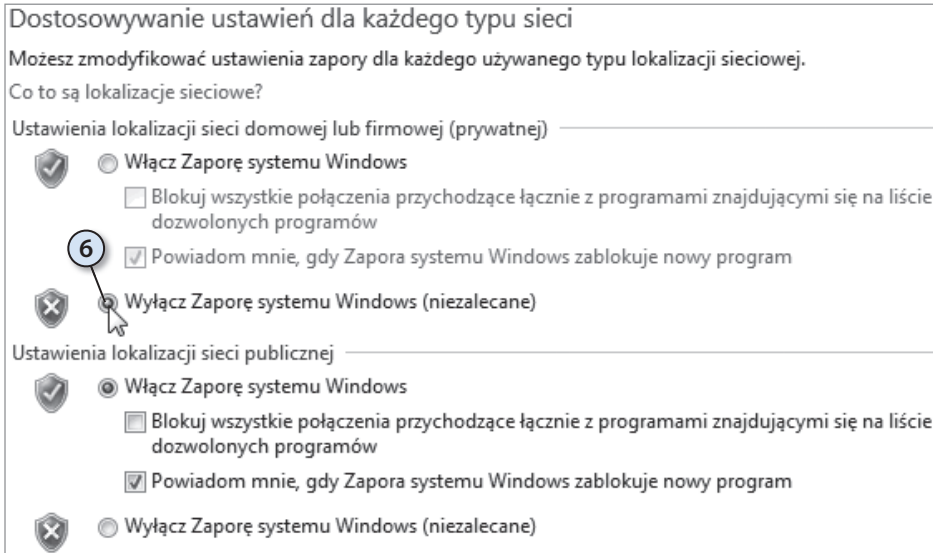


4. W oknie *System i zabezpieczenia* kliknij odsyłacz *Sprawdź stan zapory*.

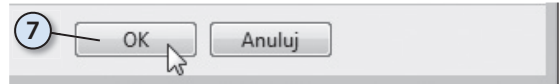


5. Po lewej stronie okna kliknij odsyłacz *Włącz lub wyłącz Zaporę systemu Windows*.



6. W wybranej lokalizacji kliknij opcję *Wyłącz*.

## 7. Kliknij przycisk OK.



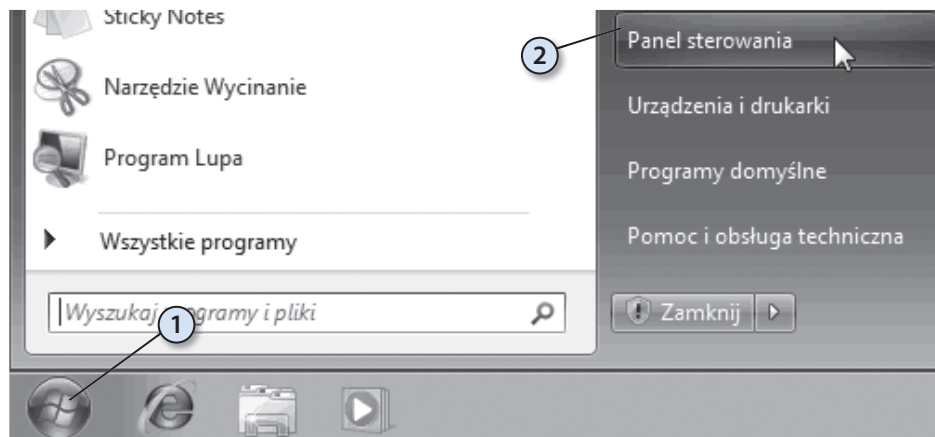
Po wyłączeniu zapory sieciowej sprawdź, czy blokowany program zaczął działać. Dodaj go do listy wyjątków, a następnie włącz zaporę sieciową.



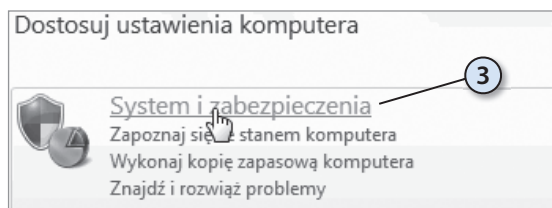
Aby zmienić ustawienia zapory sieciowej w systemie Windows 10, dotknij ikony *Start* widocznej w lewym dolnym rogu ekranu. Wybierz kolejno: *Panel sterowania*, *System i bezpieczeństwo*, *Zapora sieciowa*. Zmień ustawienia zapory i zapisz je, klikając przycisk *OK*.

Aby dodać program do listy wyjątków:

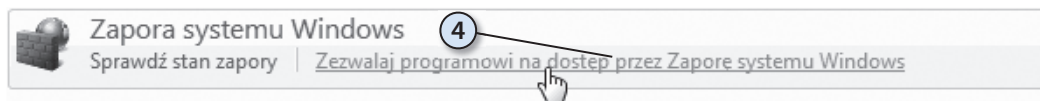
1. Kliknij przycisk *Start*.
2. Po rozwinięciu menu kliknij przycisk *Panel sterowania*.



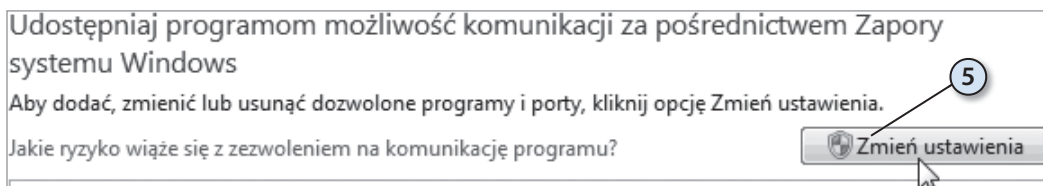
3. W Panelu sterowania odszukaj pozycję *System i zabezpieczenia*. Kliknij odsyłacz.



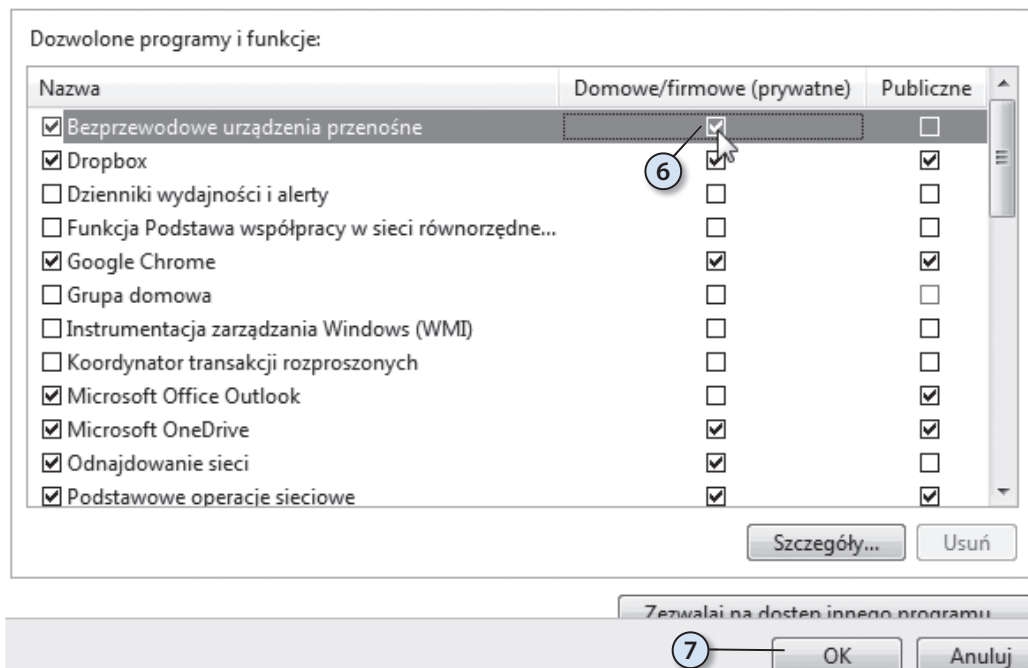
4. Kliknij odsyłacz *Zezwalaj programowi na dostęp przez Zaporę systemu Windows*.



5. W oknie *Udostępniaj programom możliwość komunikacji za pośrednictwem Zapory systemu Windows* kliknij przycisk *Zmień ustawienia*.



6. W oknie *Udostępniaj programom możliwość komunikacji za pośrednictwem Zapory systemu Windows* zaznacz pole przy nazwie programu.
7. Kliknij przycisk *OK*.



**i** Dodanie programu do listy wyjątków, czyli otwarcie portu, umożliwia działanie aplikacji. Takie działanie powinno być jednak podejmowane tylko w niezbędnych przypadkach, ponieważ każdy wyjątek stanowi furtkę, przez którą można się włamać do komputera.

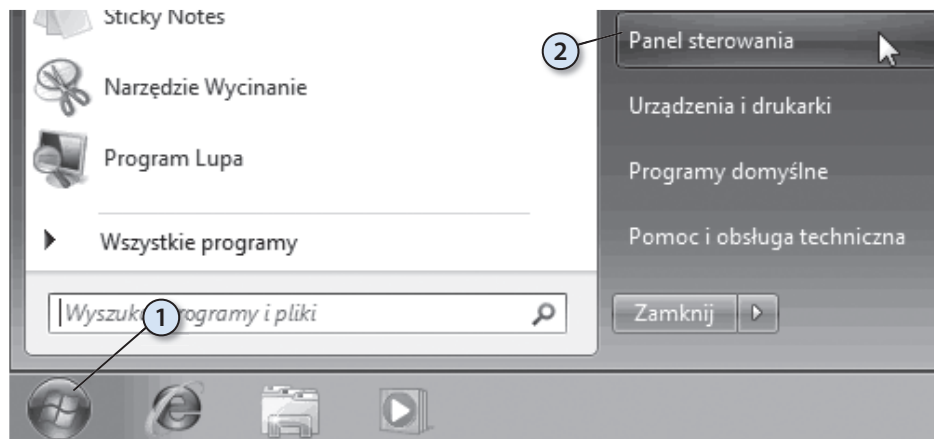
**i** Informację, jakiego portu i protokołu używa program, znajdziesz w dokumentacji programu.

Jeśli program nie jest wymieniony na liście, może być konieczne otwarcie portu. Może to mieć miejsce np. w przypadku zamiaru korzystania z sieciowej gry wieloosobowej. Dzięki otwarciu portu zapora będzie zezwalała na przekazywanie do komputera informacji dotyczących gry.

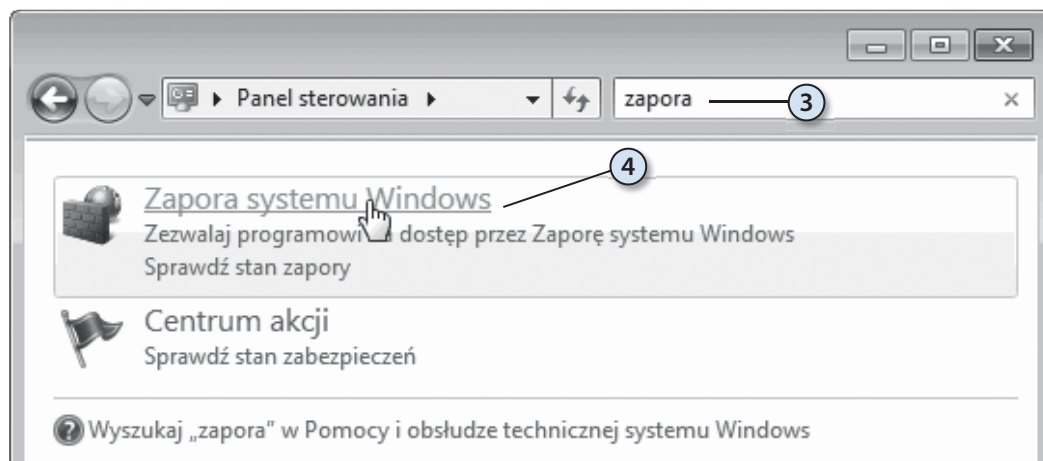
**i** Porty pozostają otwarte przez cały czas. Może to zostać wykorzystane przez włamywacza. Z tego względu należy zamykać te porty, które nie są już potrzebne.

Aby dodać port do listy wyjątków:

1. Kliknij przycisku *Start*.
2. Kliknij *Panel sterowania*.



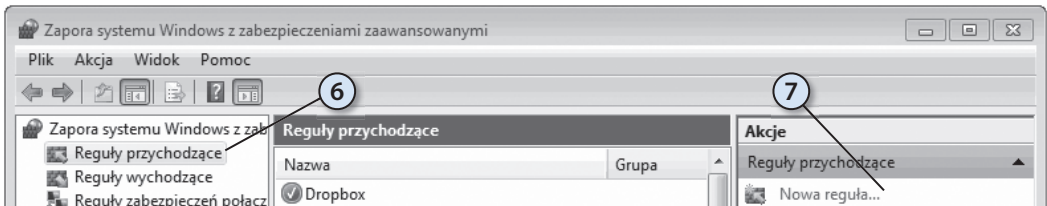
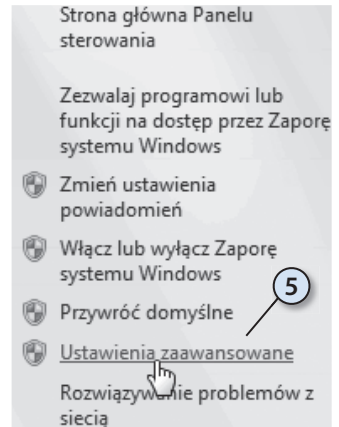
3. W polu wyszukiwania wpisz *zapora*.
4. Kliknij pozycję *Zapora systemu Windows*.



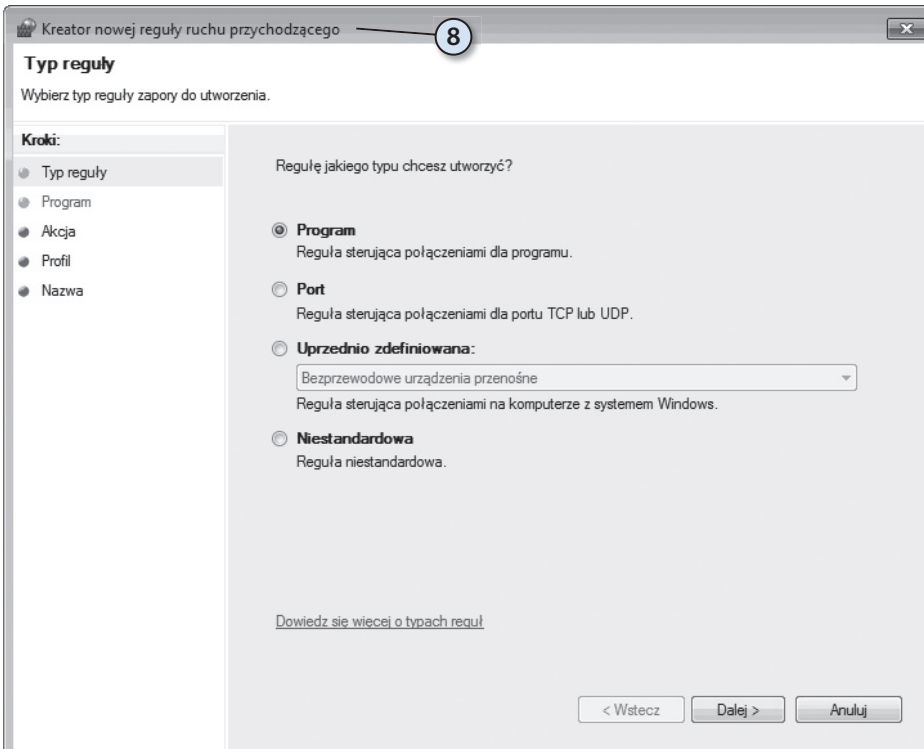
5. W lewym okienku kliknij łącze *Ustawienia zaawansowane*.

6. W oknie dialogowym *Zapora systemu Windows z zabezpieczeniami zaawansowanymi* w lewym okienku kliknij pozycję *Reguły przychodzące*.

7. Następnie w prawym okienku kliknij opcję *Nowa reguła*.



8. Postępuj zgodnie z instrukcjami wyświetlanymi w *Kreatorze nowej reguły ruchu przychodzącego*.



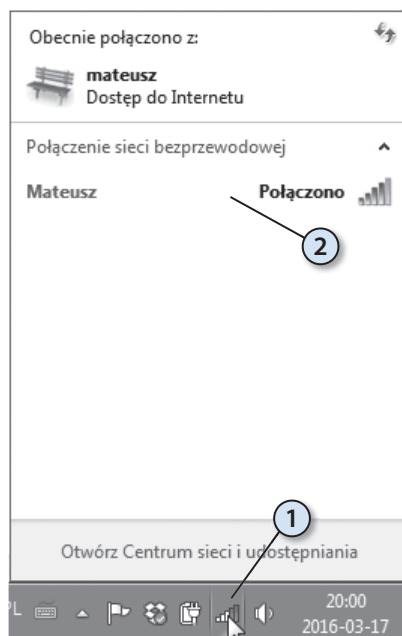


# Jakie niespodzianki sprawiają kable i połączenia?

Kable są narażone na wiele uszkodzeń. Okablowanie łączące budynki jest często umieszczane w studzienkach telekomunikacyjnych, może więc ono zostać uszkodzone przez gryzonie, zalane itp. Kable prowadzone wewnątrz budynku w rynienkach mogą zostać uszkodzone podczas wiercenia otworów w ścianach, przesuwania mebli, odnawiania pomieszczeń. Kable, którymi urządzenia sieciowe są podłączone do gniazdek umieszczonych w ścianach, mogą zostać przecięte lub wyrwane z gniazdek. Usterka jest trudna do wykrycia gołym okiem, ponieważ często uszkodzeniu ulega krucha miedziana żyła, natomiast plastikowa izolacja zachowuje ciągłość.

Aby sprawdzić, czy połączenie jest aktywne:

1. Kliknij ikonę połączenia sieciowego widoczną w prawym dolnym rogu ekranu.
2. Po chwili zostanie wyświetlona lista aktywnych połączeń sieciowych — zapoznaj się z ich opisem.





- Z informacji o ograniczonej łączności nie możesz wywnioskować, który element jest niesprawny. Sprawdź, czy wtyki są pewnie zamocowane w gniazdach. Jeżeli masz wątpliwości — wyjmij każdy z nich i wsadź ponownie.
- Jeżeli urządzenie jest chłodzone wymuszonym obiegiem powietrza, wraz z nim mogą być wciągane zanieczyszczenia, które mogą spowodować brak kontaktu. Jeżeli zauważysz w gnieździe sporo kurzu, przetrzyj wtyk i gniazdo szmatką zamoczoną w spirytusie. Odczekaj chwilę, aby alkohol wyparował, a następnie włóż wtyk do gniazda.
- Sprawdź, czy kontrolki na kartach i urządzeniach sieciowych są zapalone i nie sygnalizują błędów.
- Sprawdź, czy zamiast kabli prostych nie zostały użyte skrzyżowane i na odwrót.
- Sprawdź, czy kable nie mają przerw.
- Wyłącz i włącz ponownie przełącznik lub router, do którego jest podłączony komputer.

## Jak wykryć połączenie?

Urządzenia podłączone do sieci mają unikatowe adresy logiczne. Wykorzystując ten fakt, można sprawdzić, czy z urządzeniem jest poprawne połączenie.

Załóżmy, że w sieci są trzy komputery: K1, K2 i K3. Aby sprawdzić, czy komputer K1 jest podłączony, trzeba sprawdzić, czy istnieje połączenie pomiędzy komputerami K1 i K2 oraz K1 i K3.

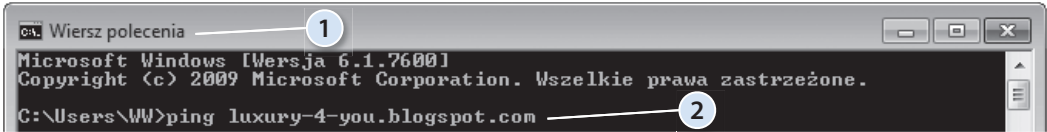
Jeżeli nie ma połączenia z komputerami K2 i K3, jest bardzo prawdopodobne, że zostało uszkodzone połączenie komputera K1.

Jeżeli nie ma połączenia z komputerem K2, a jest z komputerem K3, jest bardzo prawdopodobne, że zostało uszkodzone połączenie komputera K2.

Komputery nie muszą znajdować się w sieci LAN. Równie dobrze możesz sprawdzić połączenie pomiędzy stacją roboczą a odległym serwerem, z którym masz połączenie przez internet.

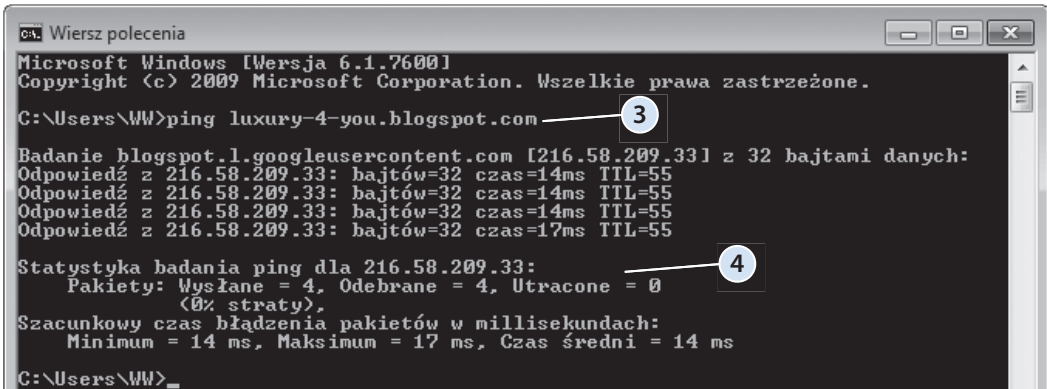
Aby sprawdzić, czy jest połączenie pomiędzy komputerami K1 i K2:

1. Wyświetl okno *Wiersz polecenia*.
2. Wpisz w nim ping IP\_K2 (gdzie IP\_K2 oznacza adres komputera, z którym chcesz przetestować połączenie).



```
ca. Wiersz polecenia
Microsoft Windows [Wersja 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\Users\WW>ping luxury-4-you.blogspot.com
```

3. Naciśnij klawisz *Enter*.
4. Zaczekaj na wyświetlenie wyniku.



```
ca. Wiersz polecenia
Microsoft Windows [Wersja 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\Users\WW>ping luxury-4-you.blogspot.com
Badanie blogspot.l.googleusercontent.com [216.58.209.33] z 32 bajtami danych:
Odpowiedź z 216.58.209.33: bajtów=32 czas=14ms TTL=55
Odpowiedź z 216.58.209.33: bajtów=32 czas=14ms TTL=55
Odpowiedź z 216.58.209.33: bajtów=32 czas=14ms TTL=55
Odpowiedź z 216.58.209.33: bajtów=32 czas=17ms TTL=55

Statystyka badania ping dla 216.58.209.33:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
            (<0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 14 ms, Maksimum = 17 ms, Czas średni = 14 ms
C:\Users\WW>
```



- Różnice w czasach odpowiedzi wynikają z obciążenia sieci — są one dopuszczalne.
- Niedopuszczalna jest utrata pakietów (% straty większy od zera).

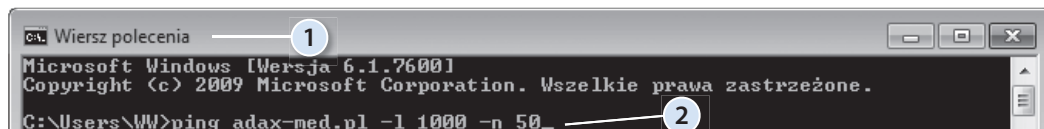
## Jak przetestować stabilność połączenia?

Sprawdzenie połączenia może dać wynik pozytywny, a tymczasem łączność może być niestabilna. Połączenie może raz być, a raz zanikać.

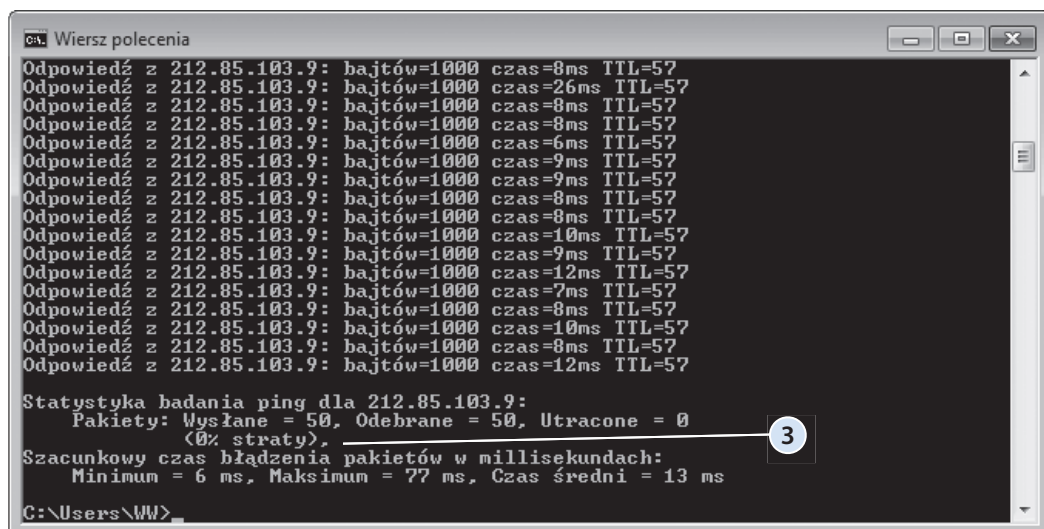
Polecenie ping standardowo wysyła cztery pakiety. W tym czasie może nie pojawić się zakłócenie. Jest jednak możliwe wysłanie określonej liczby pakietów o zadanej wielkości — wydłużenie czasu testowania i zwiększenie liczby przesyłanych danych sprzyjają wykryciu niesprawności.

Aby sprawdzić stabilność połączenia:

1. Wyświetl okno *Wiersz polecenia*.
2. Wpisz w nim polecenie `ping IP_K2 -l 1000 -n 50` (gdzie `IP_K2` oznacza adres komputera, z którym połączenie chcesz przetestować). Polecenie spowoduje wysłanie 50 pakietów po 1000 bajtów każdy.



3. Naciśnij klawisz *Enter*. Zaczekaj na wyświetlenie wyniku.

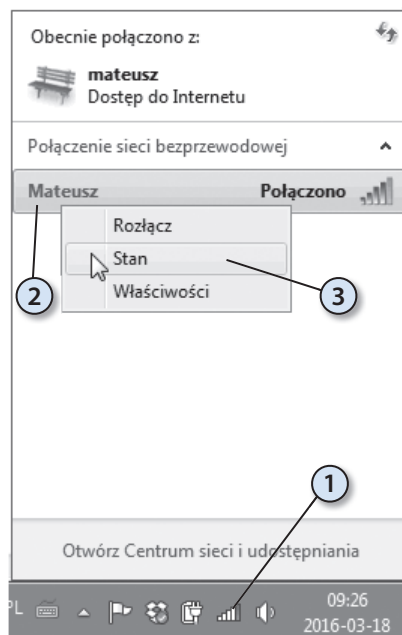


## Dlaczego strony WWW nie są wyświetlane?

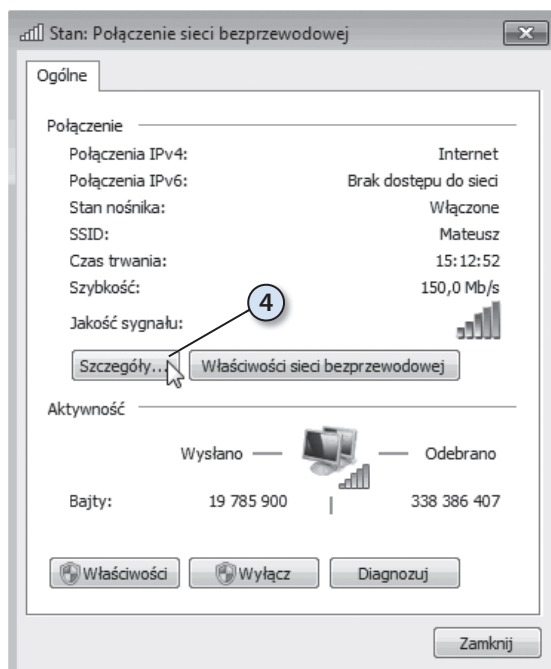
Jeżeli połączenie z internetem jest sprawne, a mimo to strony WWW nie ładują się, winę za to może ponosić serwer *DNS*. Jego zadaniem jest zamiana adresów domenyowych na liczbowe. Jeżeli serwer *DNS* jest niedostępny, strony WWW nie będą ładowane.

Aby sprawdzić, czy serwer DNS jest dostępny:

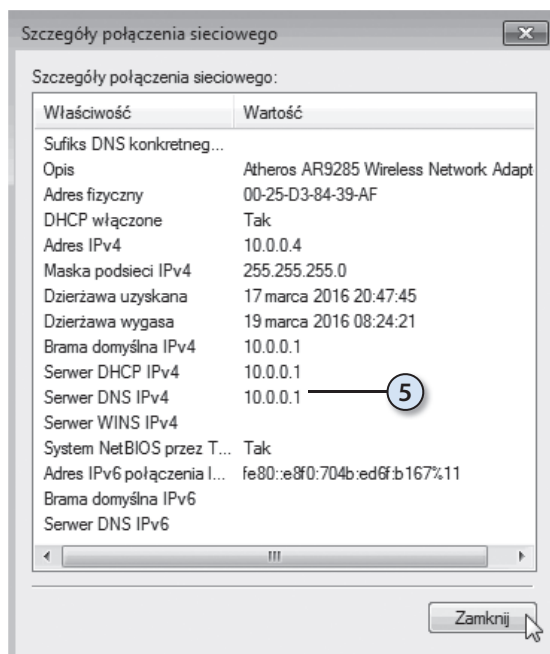
1. Kliknij symbol połączenia sieciowego widoczny w prawym dolnym rogu ekranu.
2. Po rozwinięciu menu odszukaj nazwę połączenia i kliknij go prawym przyciskiem myszy.
3. Z menu podręcznego wybierz *Stan*.



4. W oknie *Stan* kliknij przycisk *Szczegóły...*



## 5. Sprawdź, czy serwer DNS jest dostępny.



- Jeżeli adres *IP* serwera *DNS* nie będzie widoczny, oznacza to, że komputer nie może skorzystać z serwera *DNS*.
- Jeżeli adres *IP* serwera *DNS* będzie widoczny, należy sprawdzić jego dostępność przy użyciu polecenia **ping**.
- Jeżeli serwery *DNS* dostawcy usług internetowych nie są dostępne, skorzystaj z ogólnodostępnych serwerów *DNS*, np. *TPSA* (*194.204.152.34* oraz *194.204.159.1*).
- W systemie Windows znajduje się plik *hosts* (domyślna lokalizacja *C:\WINDOWS\system32\drivers\etc\hosts*). Można w nim wpisać adresy *IP* komputerów i serwerów oraz odpowiadające im nazwy komputerów w sieci lokalnej i nazwy domenowe. Zamiast wpisywania adresu *IP* wystarczy wpisać **Komputer Zuzi** (jeżeli nazwa została przypisana adresowi *IP*) i połączenie zostanie zrealizowane.

# Jak wykryć drogę pakietów?

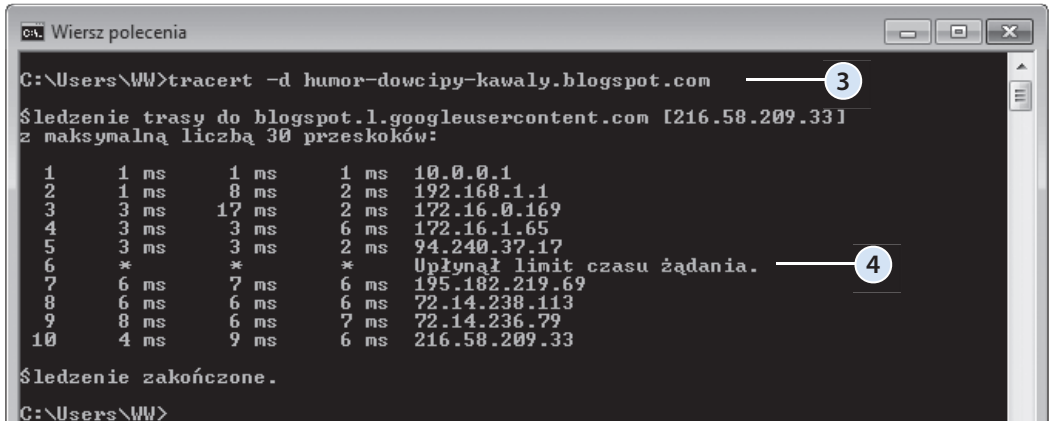
W sieciach komputerowych dane są dzielone na porcje — noszą one nazwę pakietów. Pakiety są przesyłane od nadawcy do adresata. Droga pakietów nie jest cały czas taka sama, lecz zmienia się ona w zależności od chwilowego obciążenia segmentów sieci. Węzły sieci analizują ruch i kierują pakiety tak, aby zoptymalizować ruch w sieci.

Aby stwierdzić, jaką drogą są przesyłane pakiety:

1. Wyświetl okno *Wiersz polecenia*.
2. Wpisz w nim polecenie `tracert -d komputer_docelowy`, gdzie `komputer_docelowy` oznacza adres komputera, do którego drogę pakietów chcesz prześledzić.



3. Naciśnij klawisz *Enter*.
4. Zapoznaj się z wynikiem działania polecenia.



- Polecenie `tracert` ustala ścieżkę do lokalizacji docelowej przez wysłanie komunikatów protokołu *ICMP* (*Internet Control Message Protocol*) typu *Echo Request* lub komunikatów *ICMPv6* do lokalizacji docelowej, stopniowo zwiększając wartości pola czasu wygaśnięcia (*TTL*, *Time to Live*).
- Wyświetlana ścieżka jest listą routerów znajdujących się na ścieżce między komputerem źródłowym a lokalizacją docelową.

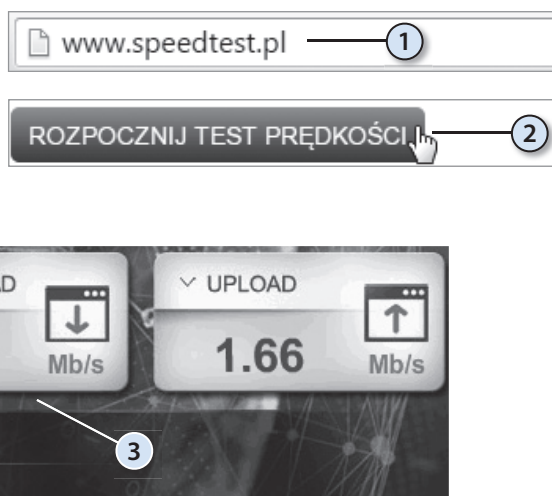
## Jak zmierzyć przepustowość łącza?

Szybkość ładowania stron WWW czy płynność wyświetlania filmów dostępnych w internecie nie są obiektywnymi miernikami przepustowości łącza. Zależą one bowiem od: chwilowego obciążenia serwera lub węzłów sieci, wydajności karty grafiki, mocy obliczeniowej procesora, zainstalowanej pamięci RAM, uruchomionych aplikacji itp.

Miarodajne jest odczytanie przepustowości łącza przy wykorzystaniu kilku specjalizowanych serwisów.

Aby zmierzyć przepustowość łącza:

1. Załaduj stronę o adresie *speedtest.pl*.
2. Kliknij przycisk *Rozpocznij test prędkości*.
3. Odczytaj wynik pomiaru.



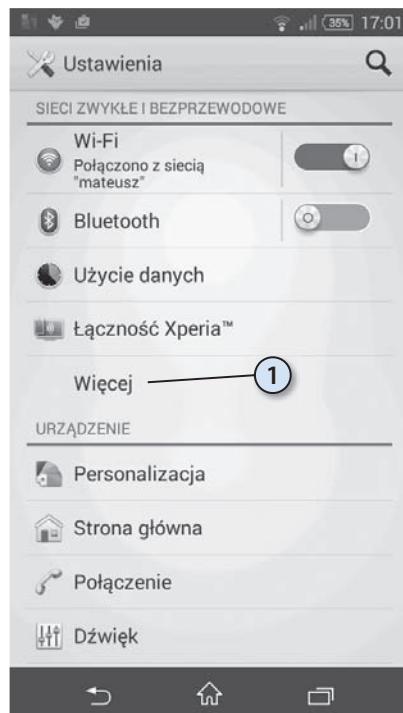
## Pasmo sieci Wi-Fi urządzenia mobilnego

Sieć Wi-Fi może pracować w dwóch pasmach: starszym — 2,4 GHz i nowszym — 5 GHz. Urządzenia mobilne mogą nawiązywać połączenia w zadanym paśmie częstotliwości lub znajdować pasmo automatycznie. Jeżeli jednak router Wi-Fi i urządzenie mobilne mają ustalone inne pasma — wówczas połączenie nie będzie możliwe.

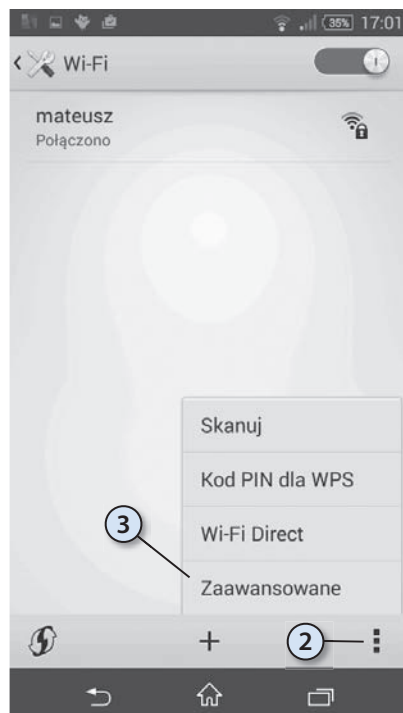


Aby zmienić pasmo pracy urządzenia mobilnego:

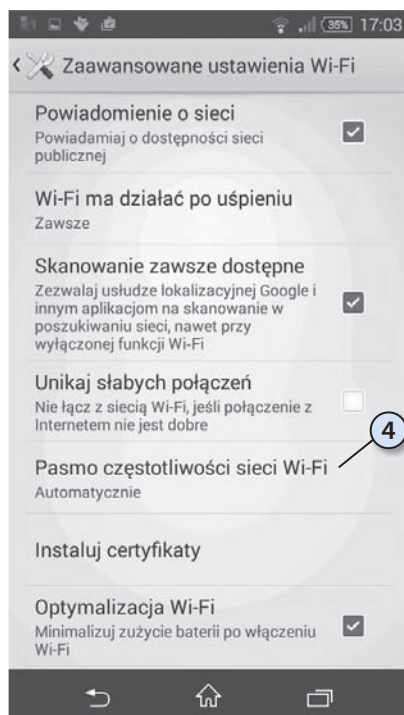
1. W oknie *Ustawienia* dotknij odсылacza *Więcej*.



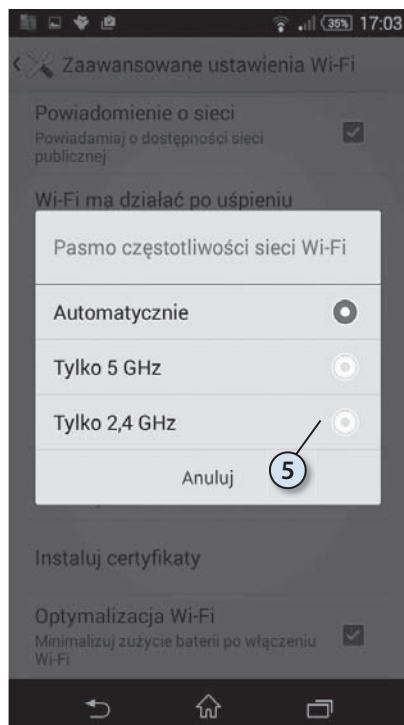
2. Dotknij widocznej w prawym dolnym rogu ikony oznaczonej trzema kwadratami.
3. Z menu wybierz polecenie *Zaawansowane*.



4. Dotknij odsyłacz *Pasmo częstotliwości sieci Wi-Fi*.



5. Z listy wybierz zakres częstotliwości.



## Pasma sieci GSM urządzenia mobilnego

Wraz z rozwojem sieci GSM były w niej implementowane różne standardy transmisji danych. Najłatwiej więc ustawić opcję automatycznego wyboru zakresu częstotliwości. Zapewnia to zgodność z stacjami bazowymi, w zasięgu których się znajdujemy. Rozwiązanie wygodne — ma ono jednak wadę: połączenie nastąpi przy użyciu najwyższej dostępnej prędkości. Jeżeli jednak zasięg się pogorszy, np. na skutek zmiany warunków atmosferycznych, wówczas urządzenie mobilne, chcąc utrzymać łączność, będzie przełączało się na niższe częstotliwości. Przełączanie spowoduje z kolei większy pobór energii z baterii.

Czy można ustawić najniższą możliwą prędkość? Można, aczkolwiek GPRS to technika związana z pakietowym przesyłaniem danych w sieciach GSM. Maksymalna wartość prędkości pobierania danych wynosi do 115 kbit/s, w praktyce jednak prędkość ta wynosi około 30 – 80 kbit/s. GPRS umożliwia korzystanie z internetu lub z transmisji strumieniowej audio/wideo.

Nieco szybszym standardem jest EDGE - rozszerzenie dla GPRS . Oba standardy są często jedyną metodą dostępu do internetu na obszarach słabo zurbanizowanych.

UMTS umożliwia użytkownikom możliwość wykonywania połączeń głosowych, wideorozmów, wysyłania wiadomości tekstowych oraz przesyłania danych. Będące częścią standardu UMTS techniki HSDPA i HSUPA pozwalają uzyskać transfer z przepływnością 21,6 Mbit/s podczas odbierania informacji i 5,76 Mbit/s podczas ich wysyłania.

HSPA+ zapewnia mobilny dostęp do internetu z prędkością: download (do klienta) do 42 Mb/s oraz upload (od klienta) do 11 Mb/s.

LTE umożliwiającą osiągnięcie przepływności zbliżonych do uzyskiwanych w sieciach lokalnych dostawców internetowych.

W tabeli 8.1 znajdziesz zestawienie standardów transmisji danych GSM i maksymalne przepustowości

Tabela 8.1. Standardy transmisji danych GSM i maksymalne przepustowości

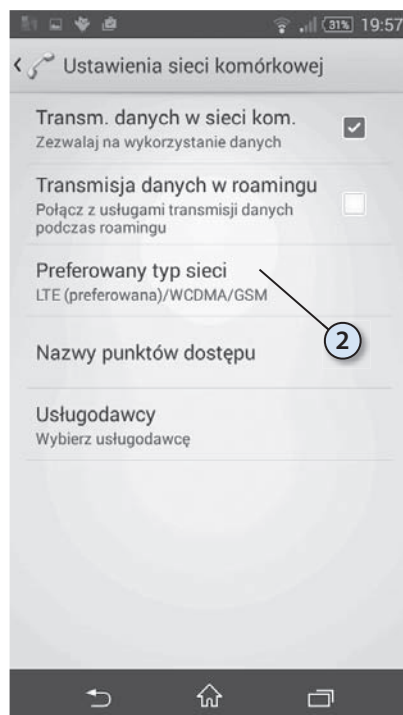
Sieć	Maksymalna przepustowość
LTE	150 Mbit/s
HSPA+	42 Mbit/s
HSDPA	21,6 Mbit/s
CDMA	9,3 Mbit/s
UMTS (3G)	384 kbit/s
EDGE	250 kbit/s
GPRS	115 kbit/s

Aby zmienić pasmo sieci GSM urządzenia mobilnego:

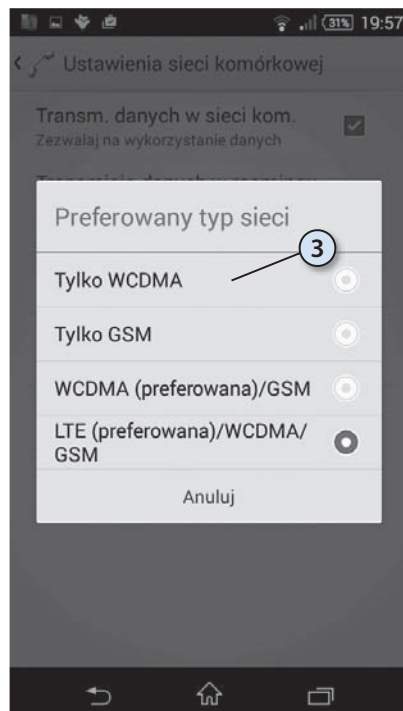
1. W oknie *Ustawienia* dotknij odsyłacza *Sieci komórkowe*.



2. Dotknij odsyłacza *Preferowany typ sieci*.



3. Wybierz typ sieci, którego chcesz używać.

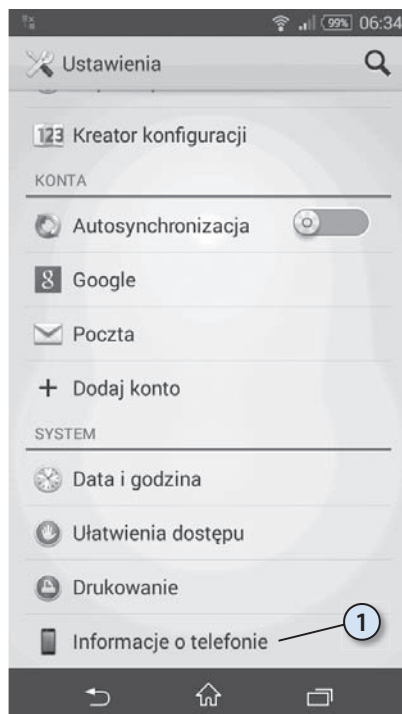


# Jak odczytać adres IP i MAC urządzenia mobilnego?

Urządzenie mobilne — choć wyglądem nie przypomina stacjonarnego komputera osobistego — współpracuje z siecią na tych samych zasadach co on. Ma więc kartę sieciową, a ona ma adresy IP i MAC.

Aby odczytać adresy IP i MAC urządzenia mobilnego:

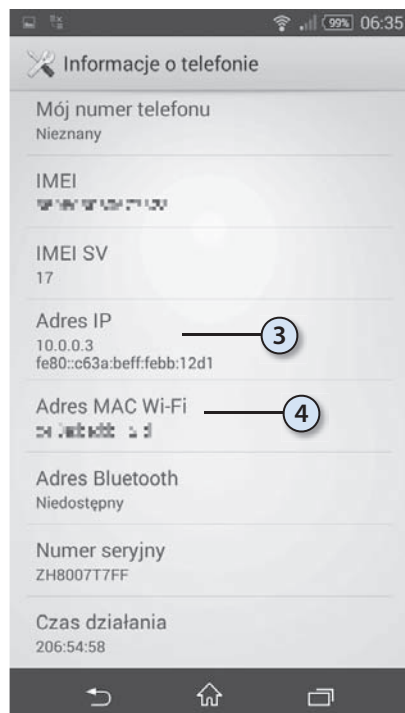
1. W oknie *Ustawienia* dotknij odsyłacza *Informacje o telefonie*.



2. W oknie *Informacje o telefonie* dotknij odsyłacza *Informacje o telefonie*.



3. Odczytaj adres IP.
4. Odczytaj adres MAC.

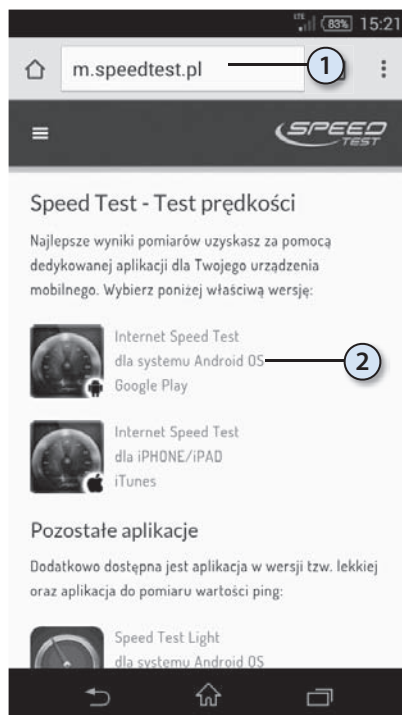


# Parametry transmisji urządzenia mobilnego

Jeżeli odnosimy wrażenie, że pliki są wolno przesyłane lub istnieją opóźnienia w sieci, wówczas należy dokonać obiektywnego pomiaru.

Aby zmierzyć parametry transmisji urządzenia mobilnego:

1. W pasku adresu przeglądarki wpisz *speedtest.pl*.
2. Po załadowaniu strony dotknij ikony aplikacji, która zostanie zainstalowana w urządzeniu mobilnym.

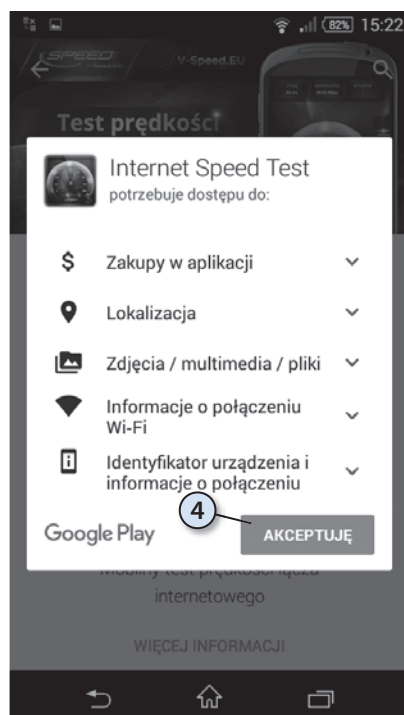




- Po załadowaniu strony z opisem aplikacji dotknij odsyłacz *Zainstaluj*.



- Zapoznaj się z listą zezwoleń, które musi mieć aplikacja, aby działała. Jeżeli zgadzasz się z nią, dotknij przycisku *Akceptuję*.

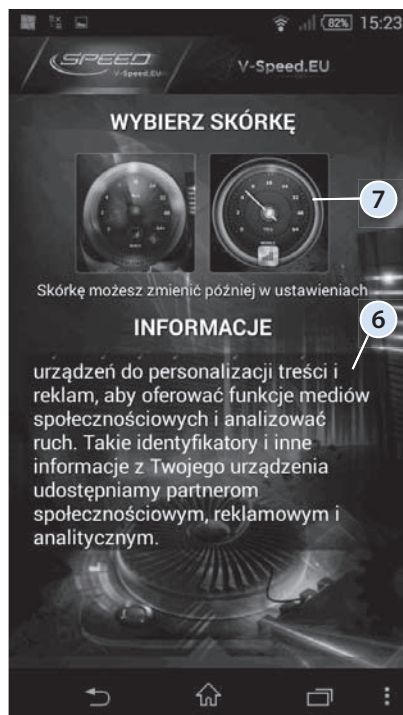


5. Dotknij przycisku *Otwórz*.



6. Zapoznaj się z warunkami użytkowania programu.

7. Wybierz wygląd interfejsu graficznego.



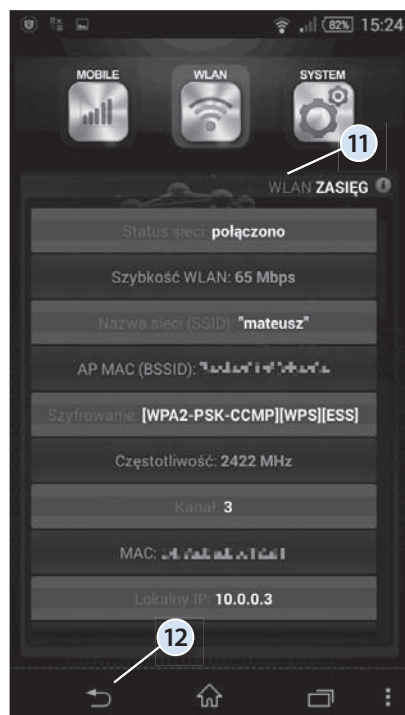
8. W górnej części okna są trzy ikony. Dotknięcie każdej z nich powoduje wyświetlenie informacji o parametrach: łącza mobilnego, łącza Wi-Fi, urządzenia mobilnego. Dotknij odsyłacz *WLAN*.



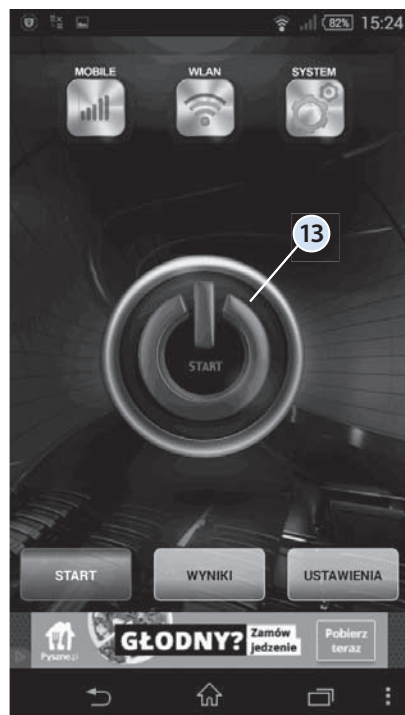
9. Odczytaj siłę sygnału.  
10. Dotknij przycisku *Więcej*.



11. Odczytaj parametry łącza.
12. Powrót do poprzedniego ekranu.



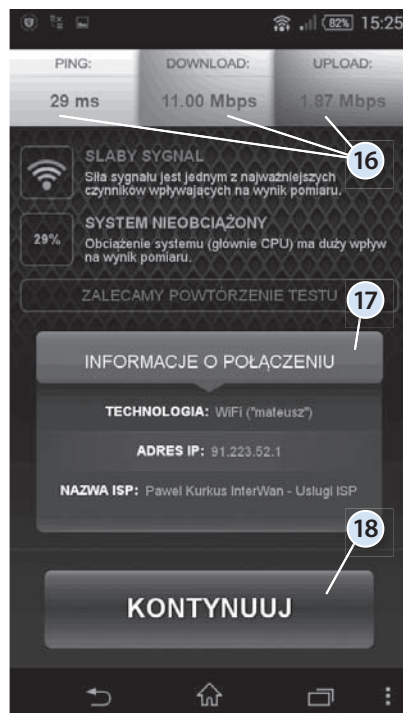
13. Dotknij przycisku *Start*.



14. Wartości wykonanych pomiarów są wyświetlane nad zegarem pomiarowym.
15. W czasie pomiaru zegar wskazuje wartości chwilowe.



16. Odczytaj wyniki pomiarów.
17. Zapoznaj się z dodatkowymi informacjami o sieci.
18. Dotknij przycisku *Kontynuuj*.



## Podsumowanie

- Zapora sieciowa nie dzieli programów na pożądane i niepożądane. Jeżeli chcesz korzystać z programu, musisz przy pierwszym jego uruchomieniu poinformować zaporę, że może on być uruchamiany.
- Polecenie ping umożliwia określenie, czy pakiety są przesyłane, jaki jest rozrzut czasowy ich transmisji oraz czy połączenie sieciowe jest stabilne.
- Polecenie tracert wyświetla drogę, jaką pakiety poruszają się od stacji roboczej do komputera docelowego. Droga pakietów jest zależna od stanu łączy, ich obciążenia i umów pomiędzy firmami internetowymi.
- Przepustowość łącza można sprawdzić, uruchamiając testy dostępne w internecie. Polegają one na ściąganiu i wysyłaniu pliku testowego. Powtórne uruchomienie testu może spowodować wzrost prędkości ściągania — jest on spowodowany pobieraniem większości danych z bufora na dysku lokalnym, a nie z internetu.

## Pytania kontrolne

### Pytanie 1.

Aby zapora sieciowa nie blokowała programu, należy:

- A. zainstalować program ponownie przy włączonej zaporze.
- B. dodać program do listy wyjątków.
- C. zaktualizować system operacyjny.

### Pytanie 2.

Do wyznaczania trasy pakietów należy użyć polecenia:

- A. tracert.
- B. ping.
- C. netsh.

**Pytanie 3.**

Podczas testowania szybkości łącza:

- A. nie należy używać komputera do innych zadań.
- B. należy komputer obciążyć maksymalnie.
- C. nie ma to wpływu na wynik pomiaru.

## Zadania do samodzielnego wykonania

1. Zmierz przepustowość łącza, korzystając z serwisu *speedtest.pl*.
2. Zmierz przepustowość łącza, korzystając z serwisu *dsl.cz*.
3. Zmierz przepustowość łącza, korzystając z serwisu *intel.com/ca/personal/digital-life/broadband*.
4. Wylicz średnią arytmetyczną z pomiarów wykonanych w punktach 1., 2. i 3.





# PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



- 1. ZAREJESTRUJ SIĘ**
- 2. PREZENTUJ KSIĄZKI**
- 3. ZBIERAJ PROWIZJĘ**

Zmień swoją stronę WWW  
w działający bankomat!

**Dowiedz się więcej i dołącz już dzisiaj!**

<http://program-partnerski.helion.pl>

GRUPA WYDAWNICZA

 **Helion SA**

# SIECI KOMPUTEROWE

KURS

## Zbuduj swoją własną sieć — to naprawdę proste!

W sieci jest wszystko, a sieć jest wszędzie, dlatego trudno obecnie wyobrazić sobie korzystanie z komputera bez dostępu do niej. O ile podpięcie pojedynczego urządzenia do internetu nie stanowi już problemu, o tyle w przypadku konieczności połączenia kilku urządzeń często stajemy przed sporym wyzwaniem, zwłaszcza jeśli nie dysponujemy specjalistyczną wiedzą i doświadczeniem. A któż nie ma w tej chwili komputera, tabletu, smartfona, odbiornika Smart TV i... rodziny lub współpracowników, z których każdy używa jednego lub nawet kilku takich sprzętów naraz i nie chce podjąć się zadania utworzenia i skonfigurowania sieci?

Jeśli należysz do tego grona, sięgnij po książkę *Sieci komputerowe. Kurs. Wydanie II*. Krok po kroku dowiesz się z niej, jak zaprojektować i zbudować własną sieć w domu lub biurze, podłączyć i skonfigurować odpowiednie urządzenia oraz oprogramowanie, reagować na błędy i uszkodzenia oraz zabezpieczyć swoją sieć przed włamaniami, a podłączone do niej komputery przed działaniem wirusów. Poznasz też sposoby udostępniania drukarek i danych, metody kontroli dostępu do zasobów i zarządzania użytkownikami oraz ich grupami, a także narzędzia umożliwiające blokowanie niechcianych treści i reklam. Co najważniejsze, przyswojenie całej tej wiedzy nie będzie wymagało doktoratu z nauk ścisłych, ponieważ książka jest napisana przystępnym i zrozumiałym językiem, który przemówi nawet do osób pozbawionych szczególnych zdolności technicznych. Do dzieła!

- Projektowanie sieci komputerowej
- Wykonanie okablowania sieciowego
- Wybór, instalacja i sprawdzanie karty sieciowej
- Łączenie urządzeń sieciowych
- Uruchamianie, konfigurowanie i zabezpieczanie routera
- Konfiguracja protokołu sieciowego
- Wykrywanie i usuwanie uszkodzeń sieci
- Zarządzanie użytkownikami i grupami
- Udostępnianie plików, folderów i urządzeń
- Zabezpieczenia systemowe i ochrona przeciwwirusowa
- Blokowanie wyświetlania reklam i niewłaściwych treści

## Nie takie sieci straszne, jak je malują!



księgarnia internetowa



<http://helion.pl>

zamówienia telefoniczne



0 801 339900



0 601 339900

Helion SA  
ul. Kościuszki 1c, 44-100 Gliwice  
tel.: 32 230 98 63  
e-mail: [helion@helion.pl](mailto:helion@helion.pl)  
<http://helion.pl>

Sprawdź najnowsze promocje:  
• <http://helion.pl/promocje>  
Książki najchętniej czytane:  
• <http://helion.pl/bestsellery>  
Zamów informacje o nowościach:  
• <http://helion.pl/nowosci>

sięgnij po WIĘCEJ



KOD KORZYŚCI

ISBN 978-83-283-2627-9



9 788328 326279

Informatyka w najlepszym wydaniu

cena: 44,90 zł