

# abc

Odkryj na nowo przyjemność korzystania  
z komputera – z Windows 8 PL!

- Jak się odnaleźć, czyli gdzie podziały się stary dobry ekran i menu Start?
- Integracja z usługami online, czyli jak efektywnie używać nowych kont użytkownika?
- Podręczna kopia na USB, czyli jak zmieścić w kieszeni Windows z własnymi ustawieniami?

## systemu

# Windows 8 PL

Danuta Mendrala  
Marcin Szeliga



Hellon

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

Projekt okładki: Maciek Pasek

Fotografia na okładce została wykorzystana za zgodą Shutterstock.com

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?abcwi8>  
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-246-5666-0

Copyright © Helion 2013

Printed in Poland.

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

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



abc

# SPIS TREŚCI

<b>Wstęp .....</b>	<b>9</b>
<b>1 Instalacja i aktualizacja systemu .....</b>	<b>13</b>
Przygotowanie do instalacji .....	14
Wymagania sprzętowe .....	14
Wybór architektury i edycji systemu .....	16
Kompatybilność sprzętu i oprogramowania .....	20
Instalacja .....	21
Instalacja Windows 8 jako nowego systemu operacyjnego ....	21
Instalacja Windows 8 jako dodatkowego systemu operacyjnego .....	27
Instalacja Windows 8 na dysku USB .....	31
Aktualizacja .....	33
Migracja .....	36
Kopiowanie sterowników urządzeń .....	37
Migracja ustawień systemowych i plików użytkowników ....	38
Weryfikacja instalacji .....	40
Aktywacja systemu .....	43
Wydłużenie 30-dniowego okresu prolongaty .....	44
Usługa Windows Anytime Upgrade .....	45
<b>2 Praca z systemem .....</b>	<b>47</b>
Uruchamianie i zamykanie systemu .....	48
Logowanie .....	48
Kończenie pracy z systemem Windows 8 .....	50

Nowy interfejs Windows 8 .....	55
Ekran startowy .....	55
Paski zadań .....	61
Aplikacje Windows 8 .....	65
Klasyczny interfejs Windows 8 .....	70
Wspólne elementy okien .....	70
Standardowe operacje .....	73
Nawigacja Aero .....	74
Eksplorator plików .....	75
Usługa wyszukiwania .....	90
Konfiguracja usługi wyszukiwania .....	91
Przeszukiwanie zasobów zdalnych komputerów .....	93
Centrum pomocy .....	95
<b>3 Konfiguracja systemu .....</b>	<b>99</b>
Konfiguracja środowiska użytkownika .....	99
Ekran blokowania i ekran startowy .....	100
Pulpit .....	101
Pasek zadań .....	104
Nowe ustawienia Zasad grupy .....	108
Konfiguracja środowiska systemowego .....	109
Okno ustawień komputera .....	109
Ekran .....	112
Właściwości komputera .....	113
Panel sterowania .....	119
Składniki systemu .....	122
Domyślne ustawienia programów i urządzeń .....	123
Usługi systemowe .....	124
Zasady grupy .....	126
<b>4 Konfiguracja urządzeń .....</b>	<b>131</b>
Sterowniki .....	132
Urządzenia i drukarki .....	133
Przywracanie poprzednich wersji sterowników .....	135
Konfiguracja automatycznego pobierania sterowników urządzeń .....	136
Starsze lub nietypowe urządzenia .....	137
Dyski .....	137
Inicjalizacja dysku .....	139
Zmiana wielkości woluminu .....	140
Dyski dynamiczne i woluminy .....	141
Dyski wirtualne .....	143
Dysk SkyDrive .....	144
Drukarki .....	146
Instalacja .....	146
Konfiguracja .....	148
Drukowanie .....	151
Konsola administracyjna Zarządzanie drukowaniem .....	153

Skanery .....	156
Koncentratory i urządzenia USB .....	157
Urządzenia audio .....	157
Urządzenia Bluetooth .....	159
Urządzenia biometryczne .....	160
Karty inteligentne .....	160
<b>5</b>	<b>Administrowanie kontami użytkowników ..... 163</b>
Uwierzytelnianie i autoryzacja .....	164
Konta i grupy użytkowników .....	167
Zarządzanie kontami .....	169
Automatyczne logowanie na konto standardowego użytkownika .....	179
Zarządzanie grupami lokalnymi .....	180
Hasła .....	184
Dysk resetowania hasła .....	185
Zmiana hasła własnego konta a resetowanie hasła innego użytkownika .....	187
Resetowanie zapomnianego hasła administratora systemu .....	188
Łamanie haseł .....	190
Prawa i uprawnienia .....	192
Uprawnienia NTFS .....	192
Prawa .....	194
Profile użytkowników .....	195
Kontrola rodzicielska .....	196
<b>6</b>	<b>Sieci lokalne ..... 199</b>
Centrum sieci i udostępniania .....	200
Połączenia sieciowe .....	201
Sieci bezprzewodowe .....	201
Protokół TCP/IP .....	208
Automatyczne konfigurowanie protokołu TCP/IP .....	209
Statyczne konfigurowanie protokołu TCP/IP .....	210
Stos nowej generacji protokołów TCP/IP .....	211
Druga wersja protokołu SMB .....	213
Grupa domowa .....	216
Praca w sieci .....	217
Korzystanie z zasobów udostępnionych w sieci .....	217
Udostępnianie zasobów komputera .....	220
DirectAccess .....	224
Mechanizm działania .....	224
Konfiguracja .....	225
BranchCache .....	226
Mechanizm działania .....	226
Konfiguracja .....	227

<b>7</b>	<b>Internet i multimedia .....</b>	<b>229</b>
	Usługi internetowe .....	230
	World Wide Web (WWW) .....	230
	Domain Name Services (DNS) .....	232
	Poczta elektroniczna .....	234
	File Transfer Protocol (FTP) .....	235
	Internet Relay Chat (IRC) .....	236
	Połączenie internetowe .....	236
	Połączenie modemowe lub za pośrednictwem wirtualnej sieci prywatnej .....	237
	Połączenie za pośrednictwem routera i serwera pośredniczącego .....	238
	Przeglądarka Internet Explorer 10 .....	240
	Internet Explorer w stylu Windows 8 .....	240
	Funkcjonalność .....	242
	Bezpieczeństwo .....	248
	Prywatność .....	256
	Konfiguracja .....	257
	Klient poczty elektronicznej .....	259
	Odtwarzanie filmów i muzyki .....	260
	Windows Media Player .....	261
	Nagrywanie płyt audio .....	261
	Przeglądarka fotografii systemu Windows .....	262
	Rejestrator dźwięków .....	263
	Podstawowe programy Windows .....	263
<b>8</b>	<b>Zarządzanie systemem .....</b>	<b>265</b>
	Monitorowanie i optymalizacja pracy systemu .....	266
	Poznaj swój system .....	266
	Menedżer zadań .....	267
	Centrum akcji i aktualizacje automatyczne .....	272
	Monitor wydajności i niezawodności .....	275
	Podgląd zdarzeń .....	281
	Harmonogram zadań .....	283
	Dyski twarde .....	285
	Zarządzanie pamięcią .....	288
	Rozwiązywanie problemów .....	291
	Raportowanie problemów i automatyczne wyszukiwanie ich rozwiązań .....	291
	Automatyczne rozwiązywanie problemów .....	291
	Pomoc zdalna .....	292
	Rejestrator problemów .....	294
	Zintegrowane śledzenie i logowanie operacji sieciowych .....	295
	Problemy z systemem operacyjnym .....	296
	Problemy z połączeniami sieciowymi .....	301
	Problemy z aplikacjami .....	304

<b>9</b>	<b>Bezpieczeństwo i prywatność .....</b>	<b>307</b>
	Granice bezpieczeństwa systemu Windows 8 .....	309
	Komputer .....	311
	System operacyjny .....	311
	Sesja użytkownika .....	312
	Wirtualna maszyna Javy i mechanizm bezpieczeństwa kodu zarządzanego opartego na uprawnieniach .....	313
	Centrum akcji .....	314
	Kontrola konta użytkownika .....	316
	Działanie funkcji kontroli konta użytkownika .....	319
	Konfiguracja funkcji kontroli konta użytkownika .....	321
	Inspekcja użytkowników .....	324
	Windows BitLocker i BitLockerToGo .....	326
	Mechanizm działania .....	326
	Konfiguracja .....	329
	Odzyskiwanie hasła .....	330
	Szyfrowanie dysków .....	332
	System szyfrowania plików EFS .....	334
	Zasady sterowania aplikacjami .....	335
	Domyślne i automatycznie wygenerowane reguły .....	336
	Reguły dodatkowe .....	337
	Wymuszanie reguł .....	339
	Windows Defender .....	339
	Zapora systemu Windows .....	342
	<b>Skorowidz .....</b>	<b>345</b>





## SIECI LOKALNE

**D**ziś trudno sobie wyobrazić pracę z komputerem bez dostępu do lokalnej sieci komputerowej i internetu. System Windows 8 zawiera funkcje sieciowe, które ułatwiają konfigurowanie i używanie sieci oraz czynią je bezpieczniejszymi i bardziej niezawodnymi, takie jak grupy domowe (czyli zaufane sieci lokalne, w ramach których możliwa jest bezpieczna wymiana plików, udostępnianie drukarek czy przesyłanie multimediiów) bądź możliwość zabezpieczenia połączeń bezprzewodowych i oznaczenia ich jako połączeń taryfowych.

Z tego rozdziału dowiesz się, jak skonfigurować połączenie sieciowe, jakie narzędzia i technologie oferuje swoim użytkownikom system Windows 8 oraz jak udostępniać w sieci lokalnej zasoby komputera i korzystać z udostępnionych w tej sieci zasobów innych komputerów.

## Centrum sieci i udostępniania

Windows 8 zapewnia kontrolę nad siecią dzięki Centrum sieci i udostępniania — jest to okno, w którym zebrano wszystkie zadania związane z siecią. Centrum sieci i udostępniania zawiera informacje o sieci, do której jest podłączony komputer, oraz sprawdza, czy możliwe jest nawiązanie połączenia z internetem. Możliwe jest także szybkie łączenie się z innymi dostępnymi sieciami i tworzenie zupełnie nowych połączeń. W rezultacie możesz przeglądać i konfigurować najważniejsze ustawienia sieci w jednym miejscu. Centrum sieci i udostępniania ułatwia także połączenie się z domu z siecią w miejscu pracy.

Żeby wyświetlić Centrum sieci i udostępniania:

- 1.** Wyświetl klasyczny pulpit (zastosuj kombinację klawiszy *Windows+D*).
- 2.** Kliknij znajdującą się w obszarze powiadomień ikonę połączenia sieciowego, a następnie odnośnik *Otwórz Centrum sieci i udostępniania* lub wyświetl Panel sterowania i kliknij odnośnik *Wyświetl stan sieci i zadania*.
- 3.** W sekcji *Wyświetlanie aktywnych sieci* znajdują się:
  - a)** Informacja na temat dostępu do internetu.
  - b)** Odnośnik pozwalający skonfigurować grupę domową, opisaną w dalszej części rozdziału.
  - c)** Odnośnik do okna właściwości połączenia sieciowego (konfiguracji połączeń sieciowych poświęcono następny punkt).
- 4.** W sekcji *Zmień ustawienia sieciowe* znajdują się odnośniki do:
  - a)** kreatora konfiguracji nowego połączenia, pozwalającego połączyć się z internetem, utworzyć połączenie VPN<sup>1</sup> (ang. *Virtual Private Network*) z miejscem pracy, utworzyć bezprzewodową sieć ad hoc czy skonfigurować połączenie telefoniczne;
  - b)** opisanych w rozdziale 8. narzędzi do rozwiązywania problemów sieciowych.

---

<sup>1</sup> Sieci VPN to tunele internetowe, w których przesyłane dane są szyfrowane. Użytkownicy mogą więc korzystać z sieci VPN tak, jakby mieli rzeczywiste — a nie wirtualne — połączenie z siecią firmową.

## Połączenia sieciowe

Aby komputer mógł pracować w sieci, musi być wyposażony w kartę sieciową będącą fizycznym interfejsem między komputerem a kablem sieciowym. Umożliwia ona komunikację, zamieniając dane generowane przez system operacyjny na impulsy elektryczne, które są przesyłane przez sieć. Karta sieciowa, tak jak każde inne urządzenie, musi być poprawnie zainstalowana w systemie Windows 8 — jeżeli komputer jest wyposażony w wiele kart sieciowych, dla każdej z nich jest tworzone połączenie z kolejnym numerem.

W przypadku większości kart wystarczy podłączyć je do komputera i uruchomić Windows 8, który sam wykryje urządzenie dzięki mechanizmowi „Plug and Play” i zainstaluje odpowiednie sterowniki. Jeżeli po podłączeniu karty sieciowej komputer nie ma połączenia z siecią lokalną, wyświetl Centrum sieci i udostępniania:

1. Jeżeli w głównym oknie wyświetli się komunikat *W tej chwili nie masz połączenia z żadną siecią*:
  - a) Uruchom zadanie *Zmień ustawienia karty sieciowej*.
  - b) Wyświetli się lista wszystkich połączeń sieciowych komputera — przy każdym z nich będzie widniał opis jego bieżącego stanu.
  - c) Skoro komputer nie jest połączony z żadną siecią, połączenia sieciowe będą wyłączone, rozłączone lub będą raportować brak połączenia — upewnij się, czy karta sieciowa jest włączona i czy komputer jest prawidłowo połączony z siecią kablem RJ-45.
2. Jeżeli nadal nie będziesz miał połączenia z siecią, kliknij ikonę połączenia sieciowego prawym przyciskiem myszy i wybierz opcję *Diagnostuj*.
3. Jeżeli problem występuje po stronie systemu Windows 8 (problemy sieciowe mogą być też skutkiem awarii urządzeń sieciowych), możliwe będzie jego automatyczne rozwiązanie. Zaakceptuj zaproponowane przez kreator rozwiązania.

## Sieci bezprzewodowe

Opracowane w 1991 roku sieci bezprzewodowe umożliwiają wymianę danych za pośrednictwem standardowych protokołów sieciowych, z tym że zamiast poprzez kable czy światłowody, pakiety są przesyłane za pośrednictwem fal radiowych. Ponieważ taki sygnał jest rozgłaszany i może być odebrany przez wszystkie komputery znajdujące się w zasięgu punktu dostępowego, podsłuchiwanie sieci bezprzewodowych jest nie tylko proste, ale również niewykrywalne. Oznacza to, że w sieciach Wi-Fi każdy ma dostęp do wszystkich przesyłanych przez sieć danych, w tym loginów i haseł wysyłanych przez innych użytkowników sieci oraz adresów

odwiedzanych przez nich stron WWW. Co więcej, przejęcie kontroli nad punktem dostępowym pozwala atakującemu nie tylko podsłuchiwać, ale również dowolnie modyfikować przesyłane dane. Informacje na temat najczęściej używanych standardów sieci bezprzewodowych zawiera tabela 6.1.

**Tabela 6.1.** Porównanie standardów sieci Wi-Fi

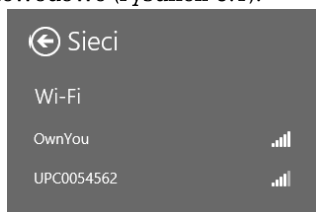
Standard	Przepustowość	Częstotliwość	Modulacja sygnału	Uwagi
802.11	1 lub 2 Mb/s	2,4 GHz	FHSS, DSSS	Pierwszy standard; definiuje warstwy fizyczną i MAC.
802.11a	6, 9, 12, 18, 24, 36, 48 lub 54 Mb/s	5,0 GHz	OFDM	Standard niekompatybilny z pozostałymi standardami, z reguły wykorzystywany w sieciach ATM.
802.11b	1, 2, 5.5 lub 11 Mb/s	2,4 GHz	DSSS, HR-DSSS	Standard popularny w sieciach domowych.
802.11g	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 lub 54 Mb/s	2,4 GHz	DSSS, HR-DSSS, OFDM	Standard kompatybilny z 802.11b. Oferuje większą niż on przepustowość, ale na mniejsze odległości.
802.11n	100, 150, 300, 450 lub 600 Mb/s	2,4 lub 5 GHz	OFDM	Technologia MIMO umożliwiająca nadawanie i odbieranie sygnału przez wiele anten.

Konfiguracja sieci bezprzewodowych w systemie Windows 8 jest szybka, łatwa i bezpieczna. Po pierwsze, funkcja rozpoznawania sieci wykrywa dostępne sieci bezprzewodowe, informuje o ich konfiguracji oraz wykrywa zmiany w konfiguracji sieci i dostosowuje do nich system operacyjny. Po drugie, dzięki pełnej obsłudze bezpiecznych protokołów zabezpieczeń bezprzewodowych, takich jak WPA2, przesyłane dane są odpowiednio zabezpieczone.

Połączenie się z dowolną siecią bezprzewodową wymaga określenia numeru kanału (częstotliwości), na której działają obsługujące ją punkty dostępowe, oraz podania identyfikatora sieci SSID (ang. *Service Set Identifier*). SSID jest ciągiem znaków, którego podstawowym zadaniem jest odróżnianie od siebie różnych sieci Wi-Fi działających na tych samych kanałach, a nie sprawdzanie tożsamości klientów — dlatego punkty dostępowe rozgłaszają swoją obecność, wysyłając SSID w pakietach nawigacyjnych. Choć rozgłaszanie identyfikatorów SSID można wyłączyć, to w żaden sposób nie poprawi to bezpieczeństwa sieci bezprzewodowej. Co gorsza, wyłączenie rozgłaszania identyfikatora SSID może spowodować, że klient będzie próbował połączyć się z wszystkimi znajdującymi się w jego zasięgu punktami dostępowymi, co oznacza, że będzie wysyłał do nich dane uwierzytelniające. Odebranie takich danych przez wrogi punkt dostępowy pozwoli atakującemu podłączyć się do zabezpieczonej za pomocą technologii WPA lub WEP sieci, a więc de facto wyłączenie rozgłaszania identyfikatorów SSID może obniżyć poziom bezpieczeństwa sieci bezprzewodowej.

Żeby połączyć się z siecią bezprzewodową:

1. Włącz kartę bezprzewodową.
2. Zastosuj kombinację klawiszy *Windows+I* i kliknij znajdujący się w dolnej części paska ustawień przycisk *Dostępne* — wyświetlone zostaną dostępne sieci bezprzewodowe (rysunek 6.1).



**Rysunek 6.1.**

Okno dostępnych sieci bezprzewodowych. Niezabezpieczone sieci bezprzewodowe oznaczone będą ikoną ostrzeżenia — odradzamy korzystanie z takich połączeń

3. Ewentualnie wyświetl klasyczny pulpit i kliknij powiadomienie *Nie połączono* — *dostępne są połączenia*. Jeżeli to powiadomienie jest niewidoczne, kliknij prawym przyciskiem myszy znajdującą się na pasku powiadomień

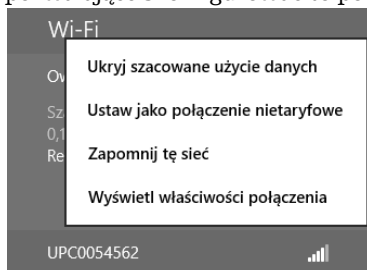
ikonę połączenia sieciowego, wybierz opcję *Otwórz centrum sieci i udostępniania* i kliknij odnośnik *Połącz z siecią*.

4. Kliknij nazwę sieci, z którą chcesz się połączyć. Sieci mające wyłączone rozgłaszanie nazw (identyfikatorów SSID) są widoczne jako *Sieć ukryta*. Podłączając się do tego typu sieci, będziesz musiał dodatkowo podać jej nazwę.



Korzystanie z wielu publicznych sieci bezprzewodowych wymaga wcześniejszego zalogowania się poprzez stronę WWW. Jeżeli wskazana przez Ciebie sieć również tego wymaga, po jej wybraniu wyświetli się odpowiednia informacja.

5. Jeżeli następnym razem połączenie z tą siecią ma być automatycznie nawiązane (np. jest to Twoja sieć domowa), upewnij się, czy zaznaczone jest pole *Połącz automatycznie*, i kliknij przycisk *Połącz*.
6. Pojawi się komunikat z prośbą o wpisanie klucza zabezpieczeń sieci — wpisz podany przez jej administratora klucz i kliknij *OK*.
7. Jeżeli wpisane przez Ciebie hasło było prawidłowe, połączysz się z siecią bezprzewodową, a skonfigurowane połączenie zostanie dodane do listy połączeń sieci bezprzewodowych.
8. Kliknij prawym przyciskiem myszy aktywne połączenie — wyświetli się menu kontekstowe pozwalające skonfigurować to połączenie (rysunek 6.2).



**Rysunek 6.2.**

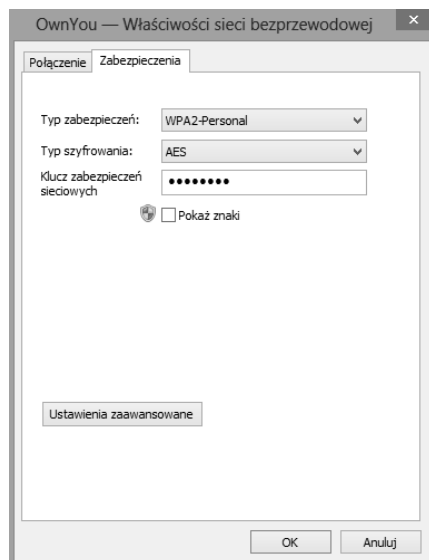
Nowością w systemie Windows 8 jest możliwość określenia połączeń bezprzewodowych jako taryfowych. Jeżeli płacisz za przesyłane przez daną sieć dane (jak to ma miejsce np. w sieciach 4G), ustawienie połączenia taryfowego spowoduje ograniczenie pobieranych przez nią danych, np. pobierane będą wyłącznie krytyczne aktualizacje zabezpieczeń, a dołączony do systemu program pocztowy będzie pobierał jedynie 20 KB każdej wiadomości e-mail

9. Kliknij odnośnik *Wyświetl właściwości połączenia*. Wyświetli się okno *Właściwości sieci bezprzewodowej*.

- 10.** Na zakładce *Połączenie* będziesz mógł skonfigurować opcje automatycznego łączenia się z tą siecią, na zakładce *Zabezpieczenia* — wybrać typ zabezpieczeń i szyfrowania (muszą one odpowiadać konfiguracji punktu dostępowego) oraz zmienić hasło (klucz) sieci bezprzewodowej (rysunek 6.3).

**Rysunek 6.3.**

O ile dostęp do przełączników i kabli można kontrolować, to uniemożliwienie atakującym odbierania i nadawania fal radiowych jest praktycznie niemożliwe, dlatego sieci bezprzewodowe muszą być dodatkowo zabezpieczone



Ponieważ atakujący dysponujący odpowiednio czułą i dużą anteną kierunkową jest w stanie odebrać sygnał punktu dostępowego z odległości kilku kilometrów, w 1999 r. został przyjęty (opracowany dwa lata wcześniej) standard WEP (ang. *Wired Equivalent Privacy*). Zgodnie z nazwą miał on zapewnić poziom bezpieczeństwa sieci Wi-Fi podobny jak w przypadku sieci przewodowych. Niestety, standard ten nie określa wielu kwestii mających wpływ na bezpieczeństwo, w tym mechanizmów udostępniania i zmieniania klucza WEP (klucza współdzielonego przez wszystkich użytkowników sieci, którego podanie jest wymagane do połączenia się z punktem dostępowym). Równie nieefektywne jest szyfrowanie zastosowane w standardzie WEP. Przebiega ono następująco:

- 1.** Najpierw wyliczana jest suma kontrolna CRC pakietu.
- 2.** Obliczona suma jest dołączana do pakietu.
- 3.** Następnie karta sieciowa generuje 24-bitowy wektor inicjujący IV.
- 4.** Klucz WEP (K) oraz wektor inicjujący są używane do zaszyfrowania strumieni pakietów algorytmem RC4 według wzoru: szyfrogram = K,IV(P,c).

W rezultacie otrzymano rozwiązanie, którego słabymi punktami są:

- 1.** Zbyt mała liczba wektorów inicjujących. Podstawą bezpieczeństwa szyfrów strumieniowych (do których należy algorytm RC4) jest nieużywanie kilkakrotnie tego samego klucza. Tymczasem 24-bitowy wektor inicjujący może przyjąć tylko jedną z 16 777 216 różnych wartości. Oznacza to, że przechwycenie 5000 pakietów daje atakującemu 50-procentową szansę na znalezienie powtórzonych wektorów inicjujących i złamanie klucza WEP.
- 2.** Brak określonego mechanizmu generowania wektorów inicjujących (niektóre karty sieciowe po prostu zwiększają o jeden wartość tego wektora dla każdego wysłanego pakietu).
- 3.** Szyfrowanie tylko treści przesyłanych pakietów, bez ich nagłówek. W rezultacie atakujący może nie tylko podsłuchać adresy źródłowe i docelowe komputerów, ich adresy MAC czy identyfikatory SSID sieci bezprzewodowej, ale również zmienić adresy docelowe pakietów. Oznacza to podatność na ataki typu „człowiek pośrodku”, możliwość przekierowywania pakietów IP oraz możliwość przeprowadzania ataków odmowy obsługi.
- 4.** Zastosowany sposób dołączania sum kontrolnych zaszyfrowanych pakietów — ponieważ przesyłane dane są nakładane za pomocą operatora XOR na strumień klucza, dany bajt szyfrogramu jest zależny od odpowiadającego mu pozycją bajta jawnej wiadomości. Próba odgadnięcia ostatniego bajta wiadomości wymaga zatem usunięcia ostatniego bajta szyfrogramu i zastąpienia go innym, a następnie wysłania zmodyfikowanego pakietu z powrotem do sieci. Jeśli bajt nie został odgadnięty, punkt dostępowy odrzuci pakiet z niepoprawną sumą kontrolną. Powtórzenie procedury dla wszystkich bajtów wiadomości pozwala odszyfrować pakiet WEP i odtworzyć strumień klucza (tę słabość wykorzystuje atak KoreKa pozwalający w mniej niż minutę złamać klucz WEP).
- 5.** Występowanie zależności pomiędzy szyfrogramem a kluczem i wektorem inicjującym (tę słabość wykorzystuje atak PTW pozwalający w mniej niż minutę złamać klucz WEP).

Dopiero w 2001 roku, po wykładach na temat WarDrivingu wygłoszonych przez Petera Shipleya na konferencji DefCon, międzynarodowe organizacje podjęły bardziej zdecydowane kroki w celu faktycznego zabezpieczenia sieci bezprzewodowych. Ich efektem jest standard 802.11i WPA przyjęty w 2003 roku przez organizację Wi-Fi Alliance. Standard ten został pomyślany jako rozwiązanie przejściowe, pozwalające w miarę bezpiecznie używać urządzeń bezprzewodowych zgodnych z wcześniejszym standardem WEP, dopóki ich producenci nie wprowadzą na rynek urządzeń zgodnych ze standardem WPA2.

Tak samo jak w standardzie WEP, dane przesyłane w sieciach WPA są szyfrowane algorytmem RC4, ale:



1. WPA używa 128-bitowego klucza uzupełnionego o dłuższy, 48-bitowy wektor inicjujący.
2. WPA automatycznie zarządza kluczami za pośrednictwem protokołu TKIP, który wymusza częstą zmianę kluczy szyfrujących, co w połączeniu ze zwiększonym rozmiarem ( $2^{48} = 281\,474\,976\,710\,656$ ) wektora IV chroni przed atakami pełnego przeglądu.
3. Standard WPA umożliwia uwierzytelnianie klientów nie tylko na podstawie znajomości współdzielonego, 256-bitowego klucza (tryb WPA-Personal), ale również za pośrednictwem serwera RADIUS.
4. WPA znacznie lepiej chroni integralność przesyłanych danych — o ile WEP po prostu wyliczał sumę kontrolną pakietów, co umożliwiało atakującym ich modyfikowanie bez konieczności wcześniejszego odszyfrowania, WPA korzysta w tym celu z kryptograficznej funkcji mieszania MIC.



Podstawowe znaczenie dla bezpieczeństwa sieci WPA-Personal ma długość współdzielonego klucza oraz to, czy nie znajduje się on w słowniku dowolnego języka — najbardziej rozpowszechniony atak na sieci WPA polega na odgadnięciu współdzielonego klucza na podstawie podsłuchanych komunikatów uwierzytelniania klienta (pakietów protokołu EAPOL). Jeżeli z jakiegoś powodu Twoja sieć Wi-Fi nadal jest zabezpieczona technologią WPA, użyj co najmniej 30-znakowego, pseudolosowego klucza — w jego wymyśleniu pomoże Ci generator dostępny pod adresem [http://www.yellowpipe.com/yis/tools/WPA\\_key/generator.php](http://www.yellowpipe.com/yis/tools/WPA_key/generator.php).

**Jedynym skutecznym sposobem zabezpieczenia sieci bezprzewodowej jest standard 802.11i WPA2.** Standard IEEE 802.11i, tak jak pierwsza wersja WPA, może być używany w trybie Personal (ze współdzielonym kluczem) lub w połączeniu z serwerem RADIUS. Do szyfrowania przesyłanych danych używa on bazującego na algorytmie AES algorytmu CCMP ze 128-bitowym kluczem i 48-bitowym wektorem inicjującym. Ten ogólnie uważany za bezpieczny algorytm jest wykorzystywany również do automatycznego zarządzania kluczami.

Najpopularniejsze ataki na sieci WPA2 polegają na odgadywaniu współdzielonego klucza na podstawie podsłuchanych komunikatów uwierzytelniania klienta, czyli podatne na niego są wyłącznie sieci Wi-Fi chronione słabymi hasłami. Wymagania dotyczące hasła umożliwiającego w trybie PSK dostęp do sieci są takie same jak w przypadku technologii WPA, tzn. hasło może liczyć od 8 do 63 znaków ASCII, ale

żeby uzyskać wysoki poziom bezpieczeństwa, powinno składać się z co najmniej 30 przypadkowych znaków.

## Sieci ad hoc

Sieci bezprzewodowe mogą być tworzone bezpośrednio pomiędzy komputerami wyposażonymi w karty bezprzewodowe. Ponieważ w sieciach ad hoc nie jest używany punkt dostępowy, możemy korzystać z nich w celu przesyłania danych pomiędzy komputerami, ale żeby połączyć się przez nie z internetem, jeden z połączonych komputerów musi udostępnić własne połączenie internetowe.

Żeby w systemie Windows 8 utworzyć sieć ad hoc, musimy skorzystać z rozwiązania firm trzecich (np. programu dostępnego pod adresem <http://www.connectify.me>) albo z narzędzia wiersza polecenia netsh:

1. Zastosuj kombinację klawiszy *Windows+X* i wybierz opcję *Wiersz polecenia (administrator)*.

2. Utwórz sieć bezprzewodową działającą w trybie ad hoc:

```
netsh wlan set hostednetwork mode=allow ssid=AdHoc key=P@ssw0rd
```

3. Uruchom na swoim komputerze punkt dostępowy do tej sieci:

```
netsh wlan start hostednetwork
```

4. Utworzone zostanie nowe połączenie sieciowe. Skonfiguruj je zgodnie ze swoimi potrzebami. Żeby na przykład udostępnić w sieci ad hoc połączenie internetowe:

- a) Wyświetl okno *Centrum sieci i udostępniania*.
- b) Kliknij odnośnik *Zmień ustawienia karty sieciowej*.
- c) Wyświetl właściwości połączenia ad hoc.
- d) Przejdź na zakładkę *Udostępnianie* i zezwól innym użytkownikom na łączenie się poprzez połączenie internetowe tego komputera.
- e) Zatwierdź zmiany przyciskiem *OK*.

## Protokół TCP/IP

TCP/IP (ang. *Transmission Control Protocol/Internet Protocol*) jest standardowym, rutowalnym protokołem, który obsługuje większość systemów operacyjnych. Protokół TCP/IP, będąc najczęściej używanym protokołem, jaki kiedykolwiek powstał, jest także używany przez największe na świecie sieci. Idealnym przykładem jest tu internet.

Każdy komputer pracujący w sieci musi mieć poprawnie zainstalowany i skonfigurowany protokół TCP/IP. Podstawowa konfiguracja obejmuje niepowtarzalny adres IP oraz maskę podsieci. Te dwa parametry są wystarczające, aby komputer mógł się porozumiewać z pozostałymi komputerami w sieci. Jednak w większości przypadków, aby uzyskać dostęp do wszystkich wymaganych usług sieciowych, potrzebna jest dodatkowa konfiguracja.

## Automatyczne konfigurowanie protokołu TCP/IP

Serwer, który umożliwia automatyczną konfigurację protokołu TCP/IP, wykorzystywanego w prawie wszystkich sieciach, nazywa się serwerem DHCP (ang. *Dynamic Host Configuration Protocol*). Za jego uruchomienie i konfigurację odpowiada administrator sieci, jednak najczęstsze związane z tym serwerem problemy możesz rozwiązać samodzielnie.

Aby zdiagnozować problem:

1. Wyświetl okno *Centrum sieci i udostępniania*.
2. Kliknij odnośnik do aktywnego połączenia (w sieciach przewodowych jest to połączenie *Ethernet*, w sieciach Wi-Fi — połączenie *WiFi*).
3. Kliknij przycisk *Szczegóły*. Wyświetli się okno dialogowe zawierające szczegółowe informacje o konfiguracji połączenia sieciowego, w tym:
  - a) Adres karty sieciowej (adres MAC).
  - b) Informacje o tym, czy komputer jest skonfigurowany jako klient DHCP.
  - c) Adres IP protokołu w wersji 4.
  - d) Maska podsieci.
  - e) Adres bramy domyślnej.
  - f) Adresy serwerów DNS i WINS.
  - g) Informacje o konfiguracji wersji 6. protokołu IP.
4. Jeżeli komputer jest klientem DHCP, sprawdź, czy adres IP komputera nie należy do zakresu od 169.254.0.0 do 169.254.255.255 i czy maska podsieci nie jest ustawiona na 255.255.0.0. Jeżeli tak jest, to znaczy, że **komputer nie mógł nawiązać połączenia z serwerem DHCP i w rezultacie sam nadał sobie adres IP, wykorzystując technologię APIPA** (ang. *Automatic Private IP Addressing*).
5. Jeżeli adres IP został skonfigurowany, ale połączenie sieciowe nie działa, możliwe, że przez przypadek inny serwer DHCP wydzierżawił adres IP. W takim przypadku należy zrezygnować z dzierżawy tego adresu, a następnie zażądać nowej dzierżawy od odpowiedniego serwera DHCP. Można to zrobić:

- a) wyłączając i ponownie włączając połączenie;
- b) diagnozując to połączenie i akceptując znalezione przez Windows 8 rozwiązanie problemu;
- c) wykonując instrukcję `ipconfig/renew` w oknie wiersza polecenia działającym z uprawnieniami administratora.

## Statyczne konfigurowanie protokołu TCP/IP

Jeżeli w jakiejś sieci nie działa serwer DHCP, będziesz musiał ręcznie skonfigurować protokół TCP/IP dla swojego połączenia. W tym celu:

1. Otwórz Centrum sieci i udostępniania i kliknij odnośnik do aktywnego połączenia.
2. Następnie kliknij przycisk *Właściwości*.
3. Wyświetli się okno właściwości wybranego połączenia. Pozwala ono dodawać, usuwać i konfigurować protokoły i usługi dla tego połączenia.
4. Zaznacz opcję *Protokół internetowy w wersji 4* i kliknij przycisk *Właściwości*.
5. Jeżeli jest to komputer stacjonarny, niepodłączony do sieci, w których działa serwer DHCP, zaznacz pole wyboru *Użyj następującego adresu IP* i wpisz podane przez administratora Twojej sieci:
  - a) adres IP Twojego komputera,
  - b) maskę podsieci,
  - c) adres bramy domyślnej (urządzenia, poprzez które możliwa jest komunikacja z innymi sieciami, np. z internetem),
  - d) adres przynajmniej jednego serwera DNS — serwery DNS zastępują w pełni kwalifikowane nazwy komputerów ich adresami IP i odwrotnie, umożliwiając posługiwanie się łatwymi do zapamiętania nazwami (np. *www.helion.pl*), a nie tylko adresami IP (np. *213.186.88.113*) komputerów, z którymi chcesz się połączyć.
6. Jeżeli jest to komputer przenośny, podłączany czasami do sieci, w których działa serwer DHCP, przejdź na zakładkę *Konfiguracja alternatywna* i wpisz podane przez administratora Twojej sieci dane dotyczące konfiguracji protokołu IP.

## Stos nowej generacji protokołów TCP/IP

Zastosowany w systemie Windows 8 stos nowej generacji protokołów TCP/IP zawiera szereg funkcji i rozwiązań pozwalających skrócić czas operacji sieciowych, w tym:

- 1.** Implementację standardów *RFC 2582* i *RFC 3782 The NewReno Modification to TCP's Fast Recovery Algorithm*, pozwalających nadawcy wysyłać więcej danych bez czekania na potwierdzenie ich odebrania przez odbiorcę.
- 2.** Funkcję ograniczenia liczby ponownie przesyłanych pakietów za pomocą komunikatów SACK (ang. *Selective Acknowledgements*) oraz implementację opisanego w dokumencie *RFC 413* algorytmu *Forward RTO-Recovery (F-RTO): An Algorithm for Detecting Spurious Retransmission Timeouts with TCP and the Stream Control Transmission Protocol (SCTP)*.
- 3.** Funkcję wykrywania niedostępności sąsiadów w ruchu IPv4 (ang. *Neighbour Unreachability Detection*). Ta funkcja protokołu IPv6 pozwala komputerom stale sprawdzać, czy sąsiednie węzły są dostępne, przez co można szybciej wykryć błędy i omijać je w sytuacji, gdy któryś z węzłów nagle stanie się niedostępny. Stos nowej generacji TCP/IP wspiera tę funkcję także dla ruchu IPv4 poprzez śledzenie stanu sąsiadów IPv4 i zapamiętywanie go w pamięci podręcznej routingu IPv4. Funkcja ta weryfikuje, czy sąsiedni węzeł jest dostępny, wymieniając z nim komunikaty protokołu ARP (ang. *Address Resolution Protocol*) REQUEST i REPLY, albo posiłkuje się w tym celu protokołami wyższych warstw.
- 4.** Funkcję skalowania po stronie odbiorcy RSS (ang. *Receive Side Scaling*) — funkcja RSS pozwala efektywnie wykorzystać moc obliczeniową wszystkich dostępnych procesorów do przetwarzania odbieranych przez kartę sieciową pakietów.
- 5.** Funkcję autodostrajania okna odbierania, pozwalającą dostosowywać rozmiar okna odbiorczego TCP (ilość danych, jaką odbiorca pozwala wysyłać nadawcy bez konieczności potwierdzenia ich odbioru) do bieżących warunków panujących w sieci. Rozmiar okna odbiorczego jest zwiększany w sieciach o przepustowości większej niż 5 Mb/s przy opóźnieniach RTT przekraczających 10 ms.
- 6.** Funkcję CTCP (ang. *Compound TCP*), optymalizującą przepustowość po stronie nadawcy — w przypadku dużego okna odbiorczego TCP znacznie zwiększa ona wysyłaną ilość danych, co w sieciach o dużej przepustowości i jednocześnie dużym opóźnieniu RTT pozwala nawet dwukrotnie skrócić czas przesyłania plików.

- 7.** Funkcję testowania nieaktywnych bram, pozwalającą nie tylko wykrywać i omijać nieaktywne bramy (routery), ale również sprawdzić, czy nieaktywna brama nie zaczęła ponownie działać.
- 8.** Funkcję wykrywania routerów PMTU działających jak czarne dziury — zdefiniowany w dokumencie RFC 1191 sposób wykrywania maksymalnego rozmiaru jednostek PMTU (ang. *Path Maximum Transmission Unit*) polega na wymianie komunikatów *Destination Unreachable-Fragmentation Needed* oraz *Don't Fragment (DF) Set* protokołu ICMP (ang. *Internet Control Message Protocol*) z routerami, przez które przesyłane są dane. Jeżeli jednak router lub znajdująca się po drodze zaporą sieciowa blokują te komunikaty, a jakiś segment sieci ma mniejsze MTU (ang. *Maximum Transmission Unit*), przesłanie przez niego niepodzielonych pakietów jest niemożliwe, a nadawca nie jest o tym informowany. Funkcja wykrywania routerów PMTU działających jak czarne dziury przeprowadza ponowne transmisje dużych segmentów TCP i automatycznie dopasowuje PMTU danego połączenia, zamiast polegać na odbiorze komunikatów protokołu ICMP.
- 9.** Funkcję dodatkowej kontroli przeciążenia ECN (ang. *Explicit Congestion Notification*) — jeżeli jakiś pakiet TCP zostanie utracony, nadawca uznaje, że przyczyną jest zatłoczenie danego segmentu sieci i zmniejsza tempo wysyłania pakietów. Gdy funkcja ECN zostanie włączona na komunikujących się ze sobą komputerach oraz znajdujących się pomiędzy nimi routerach, przeciążone routery będą odpowiednio oznaczać pakiety przed przekazaniem ich dalej. Odbiorca, otrzymując tak oznakowane pakiety, sam zażąda obniżenia tempa transmisji, aby rozładować tłok w sieci i zapobiec w ten sposób utracie przesyłanych pakietów.
- 10.** Technologię odciążania (ang. *TCP Chimney Offload*), pozwalającą na przekazanie pracy związanej z przetwarzaniem odbieranych z sieci danych z procesora komputera do jego karty sieciowej. Włączenie tej opracowanej przez firmę Alacritech technologii odciążania procesora pozwala poprawić wydajność serwerów, których głównym ograniczeniem jest czas przetwarzania pakietów odbieranych z sieci.

Domyślna konfiguracja stosu nowej generacji protokołów TCP/IP została opracowana tak, aby zapewnić poprawne działanie systemu Windows 8. Nie oznacza to jednak, że jest to konfiguracja w każdym przypadku optymalna.

Żeby wyświetlić bieżącą konfigurację stosu nowej generacji protokołów TCP/IP:

- 1.** Zastosuj kombinację klawiszy *Windows+X* i wybierz opcję *Wiersz polecenia (administrator)*.
- 2.** Potwierdź posiadanie uprawnień administracyjnych lub wpisz hasło lokalnego administratora.

**3.** Wpisz i wykonaj poniższą instrukcję:

```
netsh interface tcp show global
Wykonywanie zapytania stanu aktywnego...
```

```
Parametry globalne TCP
```

```
-----
Stan skalowania odbioru : enabled
Stan odciążania (technologia Chimney) : automatic
Stan NetDMA : enabled
Bezpośredni dostęp do pamięci podręcznej (DCA) : disabled
Poziom autoostrajania okna odbierania : normal
Dostawca dodatkowej kontroli przeciążenia : none
Funkcja ECN : disabled
Sygnatury czasowe RFC 1323 : disabled
Początkowe RTO : 3000
Receive Segment Coalescing State : disabled
```

Odpowiednie opcje stosu nowej generacji protokołów TCP/IP można ustawić za pomocą instrukcji `netsh interface tcp set global`. Na przykład:

**1.** Żeby zmienić (zgodnie z poprawką KB929868) poziom autoostrajania okna odbierania, wykonaj poniższą instrukcję:

```
netsh interface tcp set global autotuninglevel=highlyrestricted
Ok.
```

**2.** Wykonanie poniższej instrukcji włączy technologię odciążania:

```
netsh int tcp set global chimney=enabled
Ok.
```

**3.** Natomiast wykonanie poniższej instrukcji spowoduje włączenie funkcji ECN (domyślnie wyłączonej, ponieważ korzystanie z niej wymaga odpowiedniego skonfigurowania urządzeń sieciowych):

```
netsh int tcp set global ecn=enabled
Ok.
```

## Druga wersja protokołu SMB

Opracowany w latach 80. protokół SMB (ang. *Server Message Block*) do dziś jest używanym w większości sieci Windows protokołem zdalnego dostępu do plików. Tymczasem w ciągu ostatniego ćwierćwiecza infrastruktura sieciowa została całkowicie zmieniona:

- 1.** Typowa przepustowość sieci lokalnych wzrosła z 10 Mb/s do 1 Gb/s (a więc stukrotnie) i w najbliższym czasie wzrośnie do 10 Gb/s.
- 2.** Modemowe połączenia internetowe o przepustowości 64 Kb/s zostały zastąpione szerokopasmowymi połączeniami o szybkości 1 Mb/s.

3. Sieci lokalne coraz częściej łączone są w sieci rozległe, w których użytkownicy przesyłają pliki pomiędzy znacznie oddalonymi od siebie komputerami (np. pracownicy lokalnych oddziałów firmy pobierają dokumenty udostępnione przez serwer znajdujący się w centrali firmy). Przesłanie danych na duże odległości (np. pomiędzy miastami) wprowadza jednak znacznie większe opóźnienia niż przesłanie danych przez sieci lokalne.
4. Średnia liczba komputerów podłączonych do sieci Windows wzrosła z kilkunastu do kilkuset.
5. Pojawiły się i upowszechniły sieci bezprzewodowe charakteryzujące się większym ryzykiem utraty przesyłanych pakietów oraz możliwością automatycznego przełączania się komputera pomiędzy punktami dostępowymi AP (ang. *Access Point*).
6. We względnie bezpiecznych, liczących od kilkunastu do kilkudziesięciu komputerów sieciach lokalnych z lat 80. i 90. ryzyko ataku typu *man-in-the-middle* było niewielkie, a więc używane w nich protokoły (w tym pierwsza wersja protokołu SMB) nie zapewniały im ochrony przed takimi atakami<sup>2</sup>.

Zastosowaną po raz pierwszy w systemie Windows Vista (w 2006 roku) drugą wersję protokołu SMB (SMB2) opracowano<sup>3</sup> z myślą o:

1. **Zapewnieniu lepszej skalowalności** — obsługę coraz większych sieci Windows umożliwiło zwiększenie limitu jednocześnie podłączonych użytkowników i otwartych plików do 18 446 744 073 709 551 616 (2<sup>64</sup>) i zwiększenie limitu udziałów do 4 294 967 296 (2<sup>32</sup>).

<sup>2</sup> Atak typu *man-in-the-middle* na protokół SMB można przeprowadzić za pomocą dostępnego w sieci narzędzia SMB Relay lub modułu SMB Relay popularnej platformy metasploit. Przebieg ataku jest następujący:

1. Atakujący przekonuje ofiarę, żeby połączyła się z jego komputerem (np. udostępniając w sieci folder o nazwie *Zdjęcia szefa*).
2. Atakujący odbiera żądanie nawiązania sesji SMB i zamiast odpowiedzieć na nie komunikatem wezwania, odsyła odebrane żądanie do komputera ofiary.
3. Komputer ofiary standardowo reaguje na żądanie nawiązania połączenia i wysyła atakującemu komunikat wezwania.
4. Atakujący odsyła ofierze ten sam komunikat wezwania.
5. Komputer ofiary oblicza odpowiedź na otrzymane wezwanie (odebrane wezwanie jest identyczne z wysłanym) i wysyła je atakującemu.
6. Atakującemu wystarczy odesłać do komputera ofiary otrzymaną odpowiedź, żeby połączyć się z nim z uprawnieniami zalogowanego na tym komputerze użytkownika.

<sup>3</sup> W przeciwieństwie do protokołu SMB protokół SMB2 został w całości opracowany przez firmę Microsoft i jest jej intelektualną własnością.



**2. Poprawieniu wydajności, szczególnie w sieciach rozległych**

— w 1-gigabitowych sieciach z opóźnieniem RTT wynoszącym 100 ms czas kopiowania plików jest ponad dwudziestokrotnie krótszy niż w przypadku protokołu SMB1. Tak duży wzrost wydajności osiągnięto dzięki:

- a) Zastąpieniu sekwencji synchronicznych komunikatów sterujących komunikatami asynchronicznymi. Ponieważ klient może jednocześnie wysłać do serwera wiele komunikatów i kontynuować operacje sieciowe bez czekania na kolejne odpowiedzi, wyeliminowało to opóźnienia występujące w sieciach o wysokim RTT.
- b) Możliwości jednoczesnego wysłania wielu komunikatów sterujących.
- c) Buforowaniu odpowiedzi serwera.
- d) Zastąpieniu skomplikowanych sekwencji komunikatów sterujących pojedynczymi komunikatami — na przykład zmiana nazwy udostępnionego w sieci pliku za pomocą protokołu SMB wymagała wysłania trzech komunikatów (CREATE w celu utworzenia pliku, SET\_INFO w celu zmiany jego nazwy i CLOSE w celu zamknięcia pliku). Wykonanie tej samej operacji przy użyciu protokołu SMB2 wymaga wysłania tylko jednego komunikatu.
- e) Zwiększeniu rozmiarów pojedynczych pakietów, w których przesyłane są duże pliki — z 60 KB do 2 MB.
- f) Zmianie funkcji API Windows CopyFileEx() — w systemach Windows Vista SP1 i nowszych pozwala ona przesyłać dane za pośrednictwem większych buforów oraz asynchronicznie wysyłać i odbierać dane bezpośrednio z sieci, bez ich wcześniejszego zapisywania na dysku. Efektem wszystkich wymienionych zmian jest nawet dwukrotne skrócenie<sup>4</sup> czasu oczekiwania na wyniki typowych operacji sieciowych, takich jak przeglądanie udostępnionych w sieci udziałów.

**3. Poprawie bezpieczeństwa** — pakiety SMB2 są podpisywane nawet w przypadku, gdy nie zostanie to uzgodnione między klientem a serwerem. Do podpisywania pakietów używana jest kryptograficzna funkcja mieszania HMAC SHA-256, a nie przestarzała i niegwarantująca bezpieczeństwa funkcja MD5.

**4. Zwiększeniu funkcjonalności przy jednoczesnym uproszczeniu listy komunikatów sterujących** — lista komunikatów protokołu SMB2 została skrócona do 19 i w przeciwieństwie do protokołu SMB:

---

<sup>4</sup> W 1-gigabitowych sieciach z opóźnieniem RTT wynoszącym 100 ms czas otwarcia w Eksploratorze plików udziału zawierającego 50 plików Excela skrócił się o połowę, z 4 do 2 sekund.

- a) Protokół SMB2 obsługuje utrzymywanie uchwytów do otwartych plików podczas chwilowego braku połączenia (taka sytuacja ma miejsce np. podczas przełączania się komputera z jednego punktu dostępowego sieci bezprzewodowej do innego) — w rezultacie przełączenie jest niewidoczne dla użytkowników i nie wymaga np. wznowiania operacji kopiowania plików.
- b) SMB2 w pełni obsługuje dowiązania symboliczne — wprowadzone w systemie Windows Vista dowiązania symboliczne są obiektami systemu plików NTFS wskazującymi na inne, zapisane na dyskach NTFS obiekty, takie jak pliki czy foldery. W przeciwieństwie do skrótów (plików *.lnk*) dowiązania symboliczne są elementem systemu plików NTFS i są właściwie interpretowane przez wszystkie aplikacje (a nie tylko przez powłokę systemu Windows). Żeby przekierowanie do innego pliku było poprawne i nie narażało bezpieczeństwa systemu, musi ono być przeprowadzone po stronie komputera klienckiego, a nie serwera udostępniającego pliki.



Druga wersja protokołu SMB jest automatycznie używana podczas wymiany danych z systemami Windows Vista i nowszymi.

## Grupa domowa

Grupa domowa ułatwia współdzielenie zasobów komputera w zaufanych sieciach domowych. Grupa domowa spełnia trzy funkcje:

1. Pozwala identyfikować komputery podłączone do sieci domowej.
2. Umożliwia wyselekcjonowanie zasobów komputera udostępnianych innym użytkownikom grupy domowej.
3. Umożliwia przeglądanie udostępnionych w grupie domowej zasobów innych zaufanych komputerów i korzystanie z nich.

Żeby utworzyć grupę domową lub połączyć się z już istniejącą grupą domową:

1. Zastosuj kombinację klawiszy *Windows+I*, a następnie kliknij przycisk *Zmień ustawienia*.
2. Wybierz sekcję *Grupa domowa*.
3. Jeżeli urządzenie będzie podłączone do sieci, w której istnieje grupa domowa, zostanie ona znaleziona, a informacje o użytkowniku, który ją utworzył,

wraz z nazwą jego urządzenia wyświetlą się w prawej części ekranu (jeżeli komputer był wcześniej podłączony do tej grupy domowej, wyświetlone będzie również chroniące ją hasło).

- a) W takim wypadku wpisz (uwzględniając wielkość liter) podane Ci przez tę osobę hasło grupy domowej i kliknij *Przyłącz*.
  - b) Wyświetli się lista zasobów (bibliotek oraz drukarek), które możesz udostępnić innym użytkownikom grupy domowej.
  - c) Jeżeli w przyszłości będziesz chciał opuścić grupę domową, wystarczy raz jeszcze wyświetlić listę jej ustawień, przewinąć ekran w dół i wybrać opcję *Opuść*.
4. Jeżeli sieć, do której urządzenie jest podłączone, określono jako prywatną, ale grupa domowa nie została w niej znaleziona, dostępna będzie opcja *Utwórz grupę domową* — wybierz ją.
- a) Wybierz zasoby, które będą udostępniane w grupie domowej — domyślnie udostępniane są pliki multimedialne i drukarki.
  - b) Przewiń ekran w dół i zapisz hasło grupy domowej — to hasło będzie potrzebne do podłączenia do grupy domowej innych komputerów z systemem Windows 8 lub 7.

## Praca w sieci

Po skonfigurowaniu połączenia sieciowego możesz rozpocząć pracę w sieci — Windows 8 jest sieciowym systemem operacyjnym, co oznacza, że nie wymaga on instalowania dodatkowego oprogramowania. Do najważniejszych zalet sieci komputerowych należą: możliwość wymiany danych (np. poprzez gry sieciowe), udostępnianie innym zasobów naszego komputera (takich jak pliki, foldery czy drukarki) i korzystanie z udostępnionych zasobów innych komputerów.

### Korzystanie z zasobów udostępnionych w sieci

Praca w grupie domowej różni się od pracy w sieci lokalnej głównie tym, że wybrane biblioteki i drukarki są automatycznie dostępne na wszystkich komputerach grupy roboczej, natomiast żeby z nich skorzystać w sieci lokalnej, trzeba znać nazwy i hasła użytkowników komputerów, na których są one udostępnione. W obu przypadkach skorzystanie z udostępnionego przez dany komputer zasobu (np. drukarki czy połączenia internetowego) jest możliwe tylko wtedy, gdy ten komputer jest włączony.

## Wyszukiwanie komputerów i udostępnionych przez nie zasobów

Eksplorator plików umożliwia nie tylko pracę z lokalnymi plikami czy folderami, ale również udostępnianie zasobów komputera oraz korzystanie z zasobów sieciowych. Na przykład w Eksploratorze plików są wyświetlane wszystkie podłączone do sieci komputery, urządzenia i drukarki. Możliwa jest też bezpośrednia interakcja z wybranymi urządzeniami — na przykład sterowanie odtwarzaniem muzyki.

Wykonaj poniższe czynności, żeby przejrzeć zasoby sieci lokalnej:

1. Uruchom Eksplorator plików.
2. Wybierz opcję *Sieć* lub *Grupa domowa* — można to zrobić:
  - a) wpisując lub wybierając tę opcję w pasku adresu,
  - b) klikając ją w oknie nawigacji.
3. W głównym oknie Eksploratora plików wyświetlą się komputery i urządzenia podłączone do grupy domowej lub sieci lokalnej.
4. Żeby zobaczyć udostępnione przez wybrany komputer zasoby (drukarki, pliki i foldery), wystarczy dwukrotnie kliknąć jego ikonę:
  - a) Jeżeli wybrany komputer należy do grupy domowej, zobaczysz listę jej użytkowników i bibliotek udostępnionych przez nich na poszczególnych komputerach.
  - b) Jeżeli wybrany komputer będzie należał do sieci lokalnej, wyświetli się okno z pytaniem o nazwę i hasło uprawnionego użytkownika. **W takim przypadku należy wpisać pełną nazwę użytkownika** (nazwę komputera lub domeny, oddzieloną ukośnikiem od nazwy użytkownika, np. *kompJacka\Marcin*), **który ma odpowiednie uprawnienia na zdalnym komputerze**.
5. Jeżeli chcesz zobaczyć dodatkowe informacje na temat udziału, ustaw na jego nazwie kursor myszy. Po kliknięciu nazwy udziału zobaczysz jego zawartość — dalsza praca z zasobami zdalnego komputera jest taka sama jak z folderami, plikami i drukarkami lokalnego komputera.

## Mapowanie dysków sieciowych

W przypadku regularnego korzystania z udostępnionego zasobu wygodniejsze będzie podłączenie go (mapowanie) jako dysku sieciowego. Dzięki temu będziesz mógł odwoływać się do zasobu zdalnego komputera jak do lokalnego dysku. Dysk sieciowy można podłączyć na co najmniej trzy sposoby.

**1.** Jeżeli znasz nazwę komputera, który udostępnił interesujący Cię folder:

- a) Zastosuj kombinację klawiszy *Windows+R*.
- b) W polu *Otwórz* wpisz nazwę tego komputera poprzedzoną dwoma ukośnikami (nazwy komputerów podłączonych do sieci lokalnej, czyli nazwy NetBIOS, zaczynają się zawsze od dwóch ukośników).
- c) Naciśnij klawisz *Enter* — w głównym oknie Eksploratora plików wyświetlą się udostępnione na tym komputerze udziały.
- d) Kliknij interesujący Cię udział prawym przyciskiem myszy i z menu podręcznego wybierz *Mapuj dysk sieciowy*.
- e) Wybierz literę dysku, na który zostanie zamapowany zasób. Jeżeli chcesz, aby przy następnym logowaniu automatycznie był podłączany ten dysk sieciowy, zaznacz pole wyboru *Połącz ponownie przy logowaniu*. Gdy aktualnie zalogowany użytkownik nie posiada odpowiednich uprawnień, możesz skorzystać z opcji *Połącz, używając innych poświadczeń*, co spowoduje wyświetlenie okna, w którym będziesz musiał wpisać nazwę użytkownika posiadającego uprawnienia do udziału oraz jego hasło.
- f) Kliknij *Zakończ*. W sekcji *Komputer* okna nawigacji Eksploratora plików zostanie podłączony dysk sieciowy, dostępny tak jak inne dyski. Aby odłączyć dysk sieciowy, kliknij go prawym przyciskiem myszy i z menu podręcznego wybierz *Odłącz*.

**2.** Jeżeli nie znasz nazwy komputera, który udostępnił interesujący Cię folder:

- a) Uruchom Eksplorator plików.
- b) W oknie nawigacji zaznacz *Sieć* lub *Grupa domowa* — w głównym oknie Eksploratora plików wyświetlą się komputery należące do sieci lub grupy domowej.
- c) Dwukrotnie kliknij ikonę właściwego komputera.
- d) Po wyświetleniu udziałów wybranego komputera postępuj w sposób opisany w punkcie 1.

**3.** Z wiersza polecenia:

- a) Uruchom wiersz polecenia.
- b) Wyświetl dostępne w sieci komputery:

```
net view
Nazwa serwera Uwaga
```

```
-----
-----
\\GONZALES
\\RUNNER
Polecenie zostało wykonane pomyślnie.
```

- c) Wyświetl udziały udostępnione przez wybrany komputer:

```
C:\Users\Marcin>net view \\runner  
Zasoby udostępnione na \\runner
```

```
Nazwa udziału Typ Używany jako Komentarz
```

```
-----  
-----
```

```
HP Officejet K7100 series Wydruk HP Officejet K7100 series
```

```
Tmp Dysk
```

```
Users Dysk
```

```
Polecenie zostało wykonane pomyślnie.
```

- d) Podłącz wybrany udział jako dysk sieciowy:

```
C:\Users\Marcin>net use x: \\runner\tmp
```

```
Polecenie zostało wykonane pomyślnie.
```

## Udostępnianie zasobów komputera

W systemie Windows 8 udostępnianie zasobów naszego komputera jest równie łatwe, jak korzystanie z udostępnionych zasobów innych komputerów:

1. Jeżeli komputer należy do grupy domowej, drukarki i publiczne biblioteki są automatycznie udostępniane.
2. Kreator udostępniania wyświetla informacje o wszystkich osobach, które mają konta na Twoim komputerze, i udziela prawa dostępu tylko tym użytkownikom, którym dany zasób chcesz udostępnić. Umożliwia on nawet automatyczne wysłanie wiadomości e-mail z łączem do udostępnionego pliku lub folderu, aby powiadomić osoby o udostępnionych udziałach.
3. Udostępniając bibliotekę, automatycznie udostępnisz zawartość wszystkich należących do niej folderów.

## Udostępnianie bibliotek i folderów

Aby udostępnić innym użytkownikom sieci zasoby Twojego komputera:

1. Uruchom Eksploratora plików i znajdź folder lub bibliotekę, które chcesz udostępnić innym użytkownikom sieci lokalnej lub grupy domowej.
2. Albo zaznacz udostępniany folder lub bibliotekę, przejdź do sekcji wstążki *Udostępnianie* i kliknij nazwę konta użytkownika, któremu chcesz ten udział udostępnić.
3. Albo kliknij prawym przyciskiem myszy nazwę tej biblioteki lub folderu i z menu podręcznego wybierz opcję *Udostępnij*:

- a) Jeżeli chcesz zezwolić członkom grupy domowej na odczytywanie (w tym kopiowanie) znajdujących się w tym udziale plików i folderów, wybierz *Grupa domowa (wyświetlanie)*.
- b) Żeby zezwolić członkom grupy domowej na odczytywanie i modyfikowanie znajdujących się w tym udziale plików i folderów, wybierz *Grupa domowa (wyświetlanie i edycja)*.
- c) Jeżeli chcesz wybranemu użytkownikowi (ta osoba musi mieć konto na Twoim komputerze) zezwolić na dostęp do zasobu, kliknij nazwę konta tego użytkownika albo wybierz opcję *Określone osoby*, a następnie wskaż konto użytkownika, który będzie mógł korzystać z zasobu poprzez sieć, i nadaj mu odpowiedni poziom dostępu (odczyt lub odczyt i zapis).

## Foldery publiczne

Innym sposobem umożliwiającym użytkownikom sieci korzystanie z Twoich plików i folderów jest skopiowanie ich do domyślnie udostępnianych folderów publicznych.

1. Uruchom Eksplorator plików i skopiuj folder lub plik, który chcesz udostępnić, do folderu *Użytkownicy\Publiczne* (oryginalną nazwą tego folderu jest *Users\Public* — i taką nazwą powinni posługiwać się użytkownicy sieci lokalnej, tylko Eksplorator plików wyświetla spolszczoną nazwę tego folderu).



Szybkim sposobem wyświetlenia folderu publicznego jest wpisanie w wierszu polecenia start `%public%`.

2. Zaznacz dowolny plik lub podfolder. W oknie szczegółów wyświetli się informacja o jego udostępnieniu.

## Modyfikowanie uprawnień do udostępnianych zasobów

Wyświetlając właściwości udostępnianego folderu, będziesz mógł precyzyjnie określić zakres uprawnień dla korzystających z niego poszczególnych użytkowników, ograniczyć liczbę jednocześnie połączonych z nim użytkowników czy podać opis udziału.

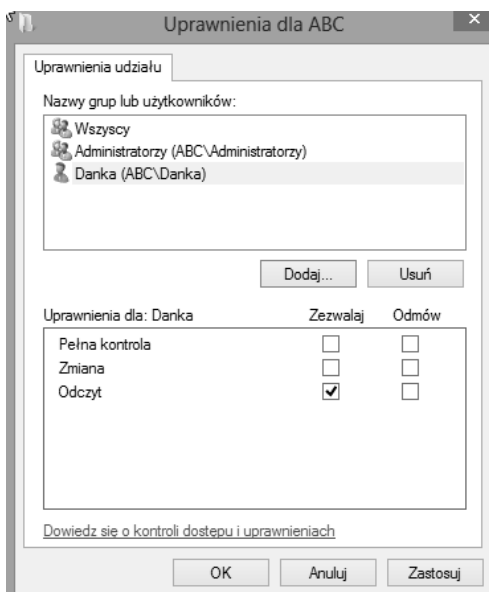
W tym celu:

1. Uruchom Eksplorator plików i znajdź udostępniany folder.
2. Kliknij go prawym przyciskiem myszy i wybierz opcję *Właściwości*.

3. Przejdź do zakładki *Udostępnianie*.
4. Kliknij przycisk *Udostępnianie zaawansowane*.
5. Gdy potwierdzisz posiadanie uprawnień administracyjnych, wyświetli się okno udostępniania, pozwalające na ustalenie, czy:
  - a) folder będzie udostępniany;
  - b) zostanie zmieniona nazwa udziału (domyślnie jest taka sama jak nazwa udostępnianego folderu);
  - c) zostaną wprowadzone dodatkowe nazwy — aliasy — udziału (ten sam folder może być równocześnie udostępniony pod różnymi nazwami);
  - d) będzie określona maksymalna liczba użytkowników jednocześnie korzystających z udziału (system Windows 8 dopuszcza maksymalnie 20 jednoczesnych sesji);
  - e) w sieci będzie widoczny komentarz (komentarze ułatwiają użytkownikom znalezienie w sieci interesujących ich udziałów);
  - f) zostaną określone zasady buforowania danych;
  - g) zostaną skonfigurowane szczegółowe uprawnienia do udziału.
6. Kliknij przycisk *Uprawnienia* — będziesz mógł dodać nazwy grup i użytkowników, którym chcesz nadać lub odebrać odpowiednie uprawnienia do udziału (rysunek 6.4).

**Rysunek 6.4.**

Uprawnienia udziałów różnią się od opisanych w poprzednim rozdziale uprawnień NTFS i mogą być nadawane również do folderów znajdujących się na dyskach FAT







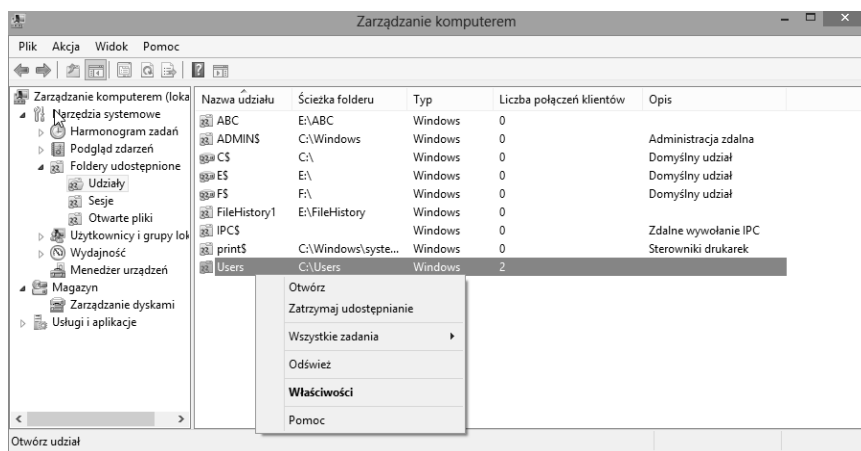
Można nadać tylko trzy uprawnienia do udziału: *Pełna kontrola*, *Zmiana* oraz *Odczyt*. Jeżeli udostępniany folder znajduje się na dysku NTFS, a użytkownik łączy się z nim przez sieć, Windows 8 sprawdzi zarówno uprawnienia do udziału, jak i uprawnienia NTFS, a wynikowe uprawnienia będą odpowiadać bardziej restrykcyjnym uprawnieniom. Na przykład osoba, która miała nadane uprawnienia NTFS *Pełna kontrola* i uprawnienia odczytu do udziału, będzie mogła tylko odczytać udostępnione pliki.

## Kontrolowanie udziałów i sesji

Konsola administracyjna Foldery udostępnione pozwala monitorować i kontrolować zdalnych użytkowników Twojego komputera. Żeby ją uruchomić:

1. Zastosuj kombinację klawiszy *Windows+X* i wybierz opcję *Zarządzanie komputerem*. Wyświetli się konsola administracyjna *Zarządzanie komputerem* — rozwiń zarejestrowaną w niej konsolę *Foldery udostępnione*. Innym sposobem jest wpisanie na ekranie startowym `fsmgmt.msc` i uruchomienie znalezionej aplikacji.
2. Zaznacz sekcję *Udziały* — w głównym oknie konsoli wyświetlą się wszystkie udziały udostępnione na komputerze.
3. Żeby skonfigurować udział, dwukrotnie kliknij jego nazwę lewym przyciskiem myszy. Zwróć uwagę, że udziały administracyjne (udziały, których nazwa kończy się znakiem *\$*) nie mogą być konfigurowane i nie można na trwałe zatrzymać ich udostępniania<sup>5</sup>.
4. Żeby zobaczyć, kto w tym momencie przegląda zasoby Twojego komputera, kliknij *Sesje*. Wskazane sesje będziesz mógł natychmiast zakończyć.
5. Zaznacz sekcję *Pliki* — w głównym oknie konsoli wyświetlą się informacje na temat plików wykorzystywanych przez użytkowników innych komputerów (rysunek 6.5).

<sup>5</sup> Po zatrzymaniu ich udostępniania zostaną one ponownie automatycznie udostępnione po kolejnym uruchomieniu komputera.



**Rysunek 6.5.** Konsola Foldery udostępnione pozwala zarządzać nie tylko udziałami, ale również sesjami, a nawet pojedynczymi plikami otwartymi w ramach tych sesji

## DirectAccess

Funkcja DA (ang. *DirectAccess*) umożliwia pracownikom korzystanie z zasobów sieci firmowych poprzez internet, a więc niezależnie od tego, gdzie się akurat znajdują. Niestety, skorzystanie z niej wymaga serwera Windows 2008 R2 lub nowszego oraz edycji Windows 8 Enterprise.

### Mechanizm działania

W przeciwieństwie do połączeń wirtualnych sieci prywatnych połączenia DA nie wymagają od użytkownika żadnej dodatkowej konfiguracji czy zestawiania osobnych połączeń z siecią firmową i pozwalają na pełne korzystanie ze wszystkich zasobów udostępnionych w sieci firmowej, takich jak serwery poczty, drukarki czy udziały sieciowe<sup>6</sup>.

Bezpieczeństwo połączeń DA gwarantuje zastosowany w tej funkcji bezpieczny protokół internetowy (IPSec) — klient DA wysyła dane poprzez tunele IPSec (wszystkie dane przesyłane tunelami IPSec są szyfrowane protokołem ESP) do serwera dostępowego firmy:

<sup>6</sup> Administrator sieci może określić, które zasoby i programy będą dostępne dla poszczególnych użytkowników łączących się poprzez połączenia DA.

1. Pierwszy tunel jest tworzony na podstawie certyfikatu komputera klienckiego i umożliwia bezpieczne przesłanie do firmowego kontrolera domeny danych uwierzytelniających użytkownika.
2. Drugi tunel dodatkowo wykorzystuje bilet Kerberos użytkownika i jest używany po jego zalogowaniu się do domeny AD w celu uzyskania dostępu do zasobów sieci firmowej.



Funkcja DA do połączenia komputerów klienckich z siecią firmową używa szóstej wersji protokołu IP. Ponieważ IPv6 wciąż nie jest obsługiwany przez większość (z wyjątkiem Chin) dostawców internetowych, połączenie DA może być zestawione poprzez IPv4 dzięki zastosowaniu technologii tunelowania ruchu IPv6, takich jak Teredo, 6to4 czy ISATAP (ang. *Intra Site Automatic Tunnel Addressing Protocol*).

Jedną z głównych zalet funkcji DA jest jej odseparowanie od połączenia internetowego — zasoby znajdujące się w sieci firmowej są dostępne poprzez bezpieczny tunel, natomiast zasoby internetu poprzez połączenie internetowe. Określenie, czy dany zasób jest zasobem firmowym, umożliwia NRPT (ang. *Name Resolution Policy Table*) — po zapisaniu w tabeli NRPT nazwy domeny (np. *firma.foo.pl*) i adresu serwera DNS, który odpowiada za tę domenę, wszystkie żądania adresowane do komputerów, które należą do wskazanej domeny, są przesyłane przez bezpieczny tunel, a nie przez połączenie internetowe.

## Konfiguracja

Uruchomienie funkcji DA wymaga:

1. domeny Active Directory;
2. przynajmniej jednego serwera Windows 2008 R2 lub nowszego, pełniącego funkcję kontrolera domeny i wyposażonego w minimum dwie karty sieciowe;
3. uruchomienia i skonfigurowania infrastruktury klucza publicznego (klienty DA muszą potwierdzać swoją tożsamość certyfikatami);
4. odblokowania na zaporach sieci firmowej protokołów:
  - a) IPv6 oraz IP 41,
  - b) Teredo (portu UDP 3544),
  - c) ICMPv6.

5. jeżeli klienci DA mają mieć dostęp do serwerów sieci firmowej używających wyłącznie czwartej wersji protokołu IP, należy uruchomić i skonfigurować urządzenie NAT-PT (ang. *Network Address Translation — Protocol Translation*).

Instalacja DA jest prawie całkowicie automatyczna — należy uruchomić dodaną konsolę administracyjną *Direct Access Management*, zaznaczyć pozycję *Direct Access* i kliknąć przycisk *Setup*.

## BranchCache

Dostępna w edycji Enterprise funkcja BC (ang. *BranchCache*) rozwiązuje problem wolnego przesyłania danych pomiędzy centralną siecią firmową a lokalnymi sieciami oddziałów firmy poprzez buforowanie raz przesłanych plików. Zbuforowane pliki mogą być przechowywane na wydzielonym serwerze Windows Server 2008 R2 lub nowszym albo na komputerach klienckich — w tym przypadku każdy z komputerów przechowuje inne, zbuforowane pliki. Zanim komputer z systemem Windows 8 pobierze plik ze zdalnego (centralnego) serwera, sprawdza, czy nie jest dostępna jego zbuforowana kopia; jeżeli tak, pobiera lokalną kopię pliku. Dzięki czemu operacja jest wykonywana kilkukrotnie szybciej, a wolne łącza pomiędzy oddziałami firmy nie są obciążane wielokrotnym przesyłaniem tych samych plików.



Zbuforowane kopie plików są szyfrowane, dzięki czemu użytkownik, który nie ma uprawnień do ich pobrania z serwera, nie będzie również mógł pobrać ich zbuforowanych kopii.

### Mechanizm działania

Zanim będzie można pobrać zbuforowany plik, komputer musi pobrać z serwera udostępniającego oryginał pliku jego cyfrową sygnaturę. Ta sygnatura pozwala:

1. sprawdzić, czy dany plik został zbuforowany i jest dostępny w sieci lokalnej;
2. sprawdzić, czy zbuforowana kopia pliku jest taka sama jak jego oryginał (jeżeli pliki będą różne, ich sygnatury również będą inne);
3. odszyfrować zbuforowaną kopię pliku (sygnatura pliku zawiera również pozwalający go odszyfrować klucz).

Po włączeniu funkcji BC w trybie rozproszonego buforowania przetwarzanie żądania pobrania pliku ze zdalnego serwera przebiega następująco:

1. Użytkownik pobiera plik z serwera centralnego.
2. Kolejny użytkownik, który chce pobrać ten sam plik, pobiera z serwera centralnego tylko jego sygnaturę.
3. Pobrana sygnatura zawiera informację o komputerze, który pobrał oryginalny plik. Na tej podstawie plik zostaje pobrany z komputera pierwszego użytkownika.
4. Gdy lokalna kopia pliku nie zostanie znaleziona, plik będzie pobrany z serwera centralnego.

Realizacja takiego samego żądania pobrania pliku po włączeniu BC w trybie z serwerem Windows wygląda następująco:

1. Użytkownik pobiera plik z serwera centralnego.
2. Lokalny serwer Windows pobiera kopię pliku z komputera użytkownika.
3. Kolejny użytkownik, który chce pobrać ten sam plik, pobiera z serwera centralnego tylko jego sygnaturę.
4. Pobrana sygnatura zawiera informację o lokalnym serwerze Windows, który przechowuje kopię pliku. Na tej podstawie plik zostaje pobrany z lokalnego serwera.
5. Gdy lokalna kopia pliku nie zostanie znaleziona, plik będzie pobrany z serwera centralnego.



Tryb z serwerem Windows zwiększa prawdopodobieństwo pobrania lokalnej kopii pliku — w przeciwieństwie do stacji roboczych serwery są z reguły dostępne 24 godziny na dobę. Funkcję lokalnego bufora plików można łączyć z innymi funkcjami i rolami, a więc ten tryb nie wymaga zainstalowania w oddziałach firmy dodatkowego serwera Windows.

## Konfiguracja

Domyślnie funkcja BC jest wyłączona.

1. Żeby ją włączyć po stronie komputerów klienckich, uruchom konsolę administracyjną Edytor zasad grupy (na przykład wpisując `gpedit.msc` w polu wyszukiwania i uruchamiając znaleziony program).

2. Rozwiń sekcję *Konfiguracja komputera/Szablony administracyjne/Sieć/Usluga BranchCache*.
3. Zasada *Włącz usługę BranchCache* pozwala włączyć omawianą funkcję.
4. Zasada *Ustaw tryb Rozproszona pamięć podręczna usługi BranchCache* pozwala włączyć buforowanie plików w trybie rozproszonym.
5. Zasada *Ustaw tryb Hostowana pamięć podręczna usługi BranchCache* pozwala włączyć buforowanie plików w trybie z lokalnym serwerem Windows i podać w pełni kwalifikowaną nazwę tego serwera.
6. Zasada *Konfiguruj usługę BranchCache dla plików sieciowych* pozwala określić opóźnienie łącza (w milisekundach), po którego przekroczeniu pliki będą buforowane.
7. Zasada *Ustaw procent wolnego miejsca na dysku używany przez pamięć podręczną komputera klienckiego* pozwala określić procent miejsca na dysku, które może być zajęte przez buforowane pliki.

Dodatkowo należy zezwolić komputerom klienckim na odbieranie pakietów protokołów HTTP i WS-Discovery (w trybie z lokalnym serwerem Windows pakiety protokołu WS-Discovery nie są używane). W tym celu:

1. Uruchom konsolę administracyjną Edytor zasad grupy.
2. Rozwiń sekcję *Konfiguracja komputera/Ustawienia systemu Windows/Ustawienia zabezpieczeń/Zapora systemu Windows z zabezpieczeniami zaawansowanymi*.
3. Kliknij prawym przyciskiem myszy *Reguły przychodzące* i wybierz z menu kontekstowego *Nowa reguła*. Uruchomi się kreator nowych reguł:
  - a) Jako typ reguły wybierz *Port*.
  - b) Wybierz protokół *TCP* i wpisz 80 w polu *Określone porty lokalne*.
  - c) Jako akcję wybierz *Zezwalaj na połączenie*.
  - d) Funkcja BC wykorzystywana jest przede wszystkim w sieciach firmowych, a więc odpowiadając na kolejne pytanie kreatora, usuń zaznaczenie pól *Prywatny* i *Publiczny*.
  - e) Podaj nazwę reguły (np. *Przychodzące http*) i zakończ działanie kreatora.
4. W taki sam sposób utwórz regułę *Przychodzące WS-Discovery*, zezwalającą na odbieranie pakietów protokołu UDP wysyłanych do portu 3702.



# SKOROWIDZ

## A

ACE, Access Control  
Entries, 164  
adres  
IP, 232  
URI, 231  
URL, 230  
akceleratory, 244  
aktualizacja, 33, 275  
do Windows 8, 34  
zabezpieczeń, 274, 310  
automatyczna, 272  
aktywacja MAK, 44  
pojedynczej kopii, 44  
systemu, 43  
anulowanie drukowania,  
152  
AP, Access Point, 214  
aplikacje  
i procesy, 268  
podpisane, 70  
Windows 8, 65  
architektura  
64-bitowa, 16  
klient-serwer, 230  
ASLR, Adress Space Layout  
Randomization, 249

atak  
typu man-in-the-middle,  
214  
XSS, 251, 253  
autentyczność danych, 327  
autoostrajanie okna  
odbierania, 211  
automatyczne  
generowanie reguł, 338  
logowanie, 180  
pobieranie  
sterowników, 136  
poprawianie błędów,  
111  
rozwiązywanie  
problemów, 291  
autoryzacja, 164  
przeglądarki, 249  
sieci, 207, 215  
sieci Wi-Fi, 205  
systemu, 309  
bezpieczny tunel, 225  
biblioteka, 84, 86  
obrazów, 86  
własna, 87  
predefiniowana, 85  
BitLocker, 326, 327  
BitLockerToGo, 326  
blokowanie  
komputera, 50  
pobierania, 254  
błędy dysków, 286  
BranchCache, 226  
buforowanie plików, 226

## B

BC, BranchCache, 226  
BCD, Boot Configuration  
Data, 298  
bezpieczeństwo, 166, 308,  
*Patrz także* granice  
bezpieczeństwa  
hasel, 185  
połączeń DA, 224

## C

CAS, Code Access Security,  
313  
centrum  
akcji, 272, 314  
pomocy, 95  
sieci i udostępniania,  
200  
certyfikat, 250

CTCP, Compound TCP, 211  
 czas aktywacji, 43  
 czas przechowywania  
 kopii, 88  
 częstotliwość  
 wykonywania kopii, 88

**D**

DA, DirectAccess, 224  
 DACL, Discretionary Access  
 Control List, 164  
 dane BCD, 298  
 defragmentacja, 286  
 DEP, Data Execution  
 Prevention, 17, 117, 249  
 diagnostyka połączeń  
 sieciowych, 301  
 DirectAccess, 224  
 DISM, Deployment Image  
 Servicing and  
 Management, 26  
 DNS, Domain Name  
 Services, 232  
 dodatkowe systemy  
 operacyjne, 29  
 dokument RFC, 230  
 domeny, 233  
 domyślny rozmiar alokacji,  
 79  
 dostęp do  
 drukarki, 150  
 przełączników, 205  
 dowiązania symboliczne,  
 127  
 drukarka  
 anulowanie  
 drukowania, 152  
 domyślna, 149  
 instalacja, 146  
 kolejność drukowania,  
 153  
 konfiguracja, 148  
 kontrola dostępu, 150  
 udostępnianie, 149  
 wstrzymywanie  
 drukowania, 152  
 zarządzanie  
 drukowaniem, 153,  
 155  
 drukarki, 133, 146  
 lokalne, 147  
 sieciowe, 148

drukowanie, 151  
 dysk  
 resetowania hasła, 185  
 dyski, 78  
 dynamiczne, 141  
 GPT, 138  
 MBR, 138  
 SAN, 327  
 SkyDrive, 144  
 twarde, 14, 137, 285  
 wirtualne30, 143  
 zewnętrzne, 80  
 działanie mechanizmu  
 WAT, 43  
 dzienniki zdarzeń, 282, 291

**E**

ECN, Explicit Congestion  
 Notification, 212  
 efekty wizualne, 116  
 ekran, 14, 112  
 blokowania, 49, 100  
 startowy, 55–58, 100  
 eksplorator plików, 75  
 EPT, Extended Page  
 Tables, 15

**F**

falszywe okna dialogowe,  
 317  
 falszywy kursor myszy,  
 317  
 FC, Fibre Channel, 327  
 filtr  
 SmartScreen, 250, 253,  
 308  
 XSS, 249, 251  
 filtrowanie  
 dokumentów, 92  
 plików i folderów, 82  
 filtry wyszukiwania, 94  
 firma VeriSign, 233  
 Flash Player, 232  
 flirt SmartScreen, 254  
 foldery  
 publiczne, 221  
 specjalne, 85  
 format  
 VHD, 144  
 VHDX, 144

formatowanie dysku, 79  
 FTP, File Transfer Protocol,  
 235  
 funkcja  
 BC, 226  
 BitLocker, 80, 328  
 funkcja CTCP, 211  
 DEP, 17  
 mieszająca MD, 190  
 PatchGuard, 17  
 RSS, 211  
 wysyłania nagłówków,  
 250  
 funkcjonalność  
 przeglądarki, 242  
 FVEK, Full Volume  
 Encryption Key, 328

**G**

gesty, 173  
 GPT, GUID Partition Table,  
 138  
 granice bezpieczeństwa,  
 309  
 komputer, 311  
 mechanizm CAS, 313  
 sesja użytkownika, 312  
 system operacyjny, 311  
 wirtualna maszyna  
 Javy, 314  
 grupa  
 domowa, 216  
 WSZYSTKIE PAKIETY  
 APLIKACJI, 151  
 grupy kafelków, 59  
 grupy użytkowników, 167

**H**

harmonogram zadań, 283  
 hasła, 49, 184  
 dysk resetowania, 185  
 łamanie, 190  
 resetowanie, 187  
 szyfrowanie, 190  
 zmiana, 187  
 hibernacja, 52  
 historia  
 aplikacji, 269  
 plików, 87  
 HTTPS, Secure HTTP, 232



**I**

identyfikacja kopii, 44  
 serwerów WWW, 250

identyfikator SID, 164

ikony pulpitu, 104

indeks wydajności, 113

informacje o systemie, 266  
 zasobach, 77

inicjalizacja dysku, 139

inspekcja użytkowników, 324

instalacja, 21, 31  
 aplikacji, 69  
 DA, 226  
 na dysku USB, 31  
 na dysku wirtualnym, 29  
 na nowym komputerze, 21  
 z folderu, 24  
 z obrazu ISO, 24

interfejs, 55

iSCSI, 327

klasyczny, 70

typograficzny, 47

użytkownika, 99

Internet Explorer 10  
 akceleratory, 244  
 bezpieczeństwo, 248  
 filtr XSS, 251  
 funkcjonalność, 242  
 kanały RSS, 246  
 karty, 243  
 konfiguracja, 257  
 pasek adresu, 242  
 pasek ulubionych, 245  
 prywatność, 256  
 wydajność, 242  
 zapisywanie stron, 247

IRC, Internet Relay Chat, 236

**K**

kafelki, 59

kanaly informacyjne, 246

karta graficzna, 14

karty inteligentne, 160

kategorie zdarzeń, 325

klasyczny pulpit, 56

klient poczty elektronicznej, 259

klucz  
 EFS, 335  
 SRK, 328

szyfrowania dysku  
 FVEK, 328  
 VMK, 328  
 WEP, 205

kod aktywacyjny, 44

kod PIN, 174

kolejny system operacyjny, 27

kompatybilność, 20

kompozycje, 102

kompresowanie plików i folderów, 84

komputer zdalny, 93

komunikatory internetowe, 236

koncentratory, 157

konektory wyszukiwania, 94

konfiguracja  
 BC, 227  
 DA, 225  
 drukarki, 148  
 funkcji i obiektów, 129

Internet Explorer 10, 257

konta, 169

profilu użytkownika, 178

protokołu TCP/IP, 209, 238

przeglądarki, 241

stosu nowej generacji, 212

systemu, 69, 99, 267

środowiska systemowego, 109

środowiska użytkownika, 99

urządzeń, 41

usługi wyszukiwania, 91

zapory systemu, 342

konsole Foldery, 224

konta, 167, 169, 176

konto Windows Live ID, 168, 171

kontrola dostępu, 164

kontrola konta użytkownika, 316–320  
 konfiguracja, 321–324

kontrola przeciążenia ECN, 212  
 rodzicielska, 196, 198

kontrolki ActiveX, 255

kontrolowanie udziałów i sesji, 223

kończenie pracy, 50

kopia systemu, 44

kopiowanie sterowników urządzeń, 37

KPP, Kernel Patch Protection, 17

kreator nowych reguł, 228

kryteria wyszukiwania, 91

**L**

lista serwerów głównych, 233

loader systemu, 298

logiczne dyski twarde, 140

logowanie, 48, 172

logowanie automatyczne, 179

lokalizacja zapisu biblioteki, 86

lokalne grupy wbudowane, 181  
 zasady grupy, 128

**Ł**

łamanie haseł, 190, 191

łączenie się z siecią, 203

**M**

MAC, Message Authentication Code, 327

macierz RAID, 138

magazyn rozruchowy, 29

mapowanie dysków sieciowych, 218

MBR, Master Boot Record, 138

MD, Message-Digest, 190

mechanizm  
 aktywacji kluczy  
 woluminowych, 44  
 ASLR, 249  
 CAS, 313  
 izolacji sesji, 312  
 WAT, 43

menedżer  
 Bootmgr, 298  
 zadań, 267, 277

menu  
 Plik, 73  
 Start, 55

Microsoft Security  
 Essentials, 340

migracja, 33, 36  
 plików, 38  
 ustawień  
 systemowych, 38

MIME, Multimedia  
 Internet Mail  
 Extension, 232

modem  
 DSL, 236  
 GSM, 236

moduł TPM, 14, 329  
 modyfikowanie kont, 176  
 monitor

niezawodności, 275,  
 279, 280  
 wydajności, 277  
 zasobów, 270

monitorowanie  
 drukarek, 154  
 operacji, 277  
 systemu, 266

montowanie obrazu, 26

MTU, Maximum  
 Transmission Unit, 212

## N

nagrywanie płyt audio, 261  
 napędy USB, 80  
 narzędzia diagnostyczne,  
 296

narzędzie  
 wiersz polecenia, 319  
 Arp, 302  
 Data Classification  
 Toolkit, 167  
 DISM, 26  
 ImageX, 25

IpConfig, 302  
 nbtstat, 303  
 net, 303  
 netsh, 303  
 netstat, 303  
 nslookup, 303  
 Oczyszczanie dysku, 36  
 pathping, 303  
 Ping, 302  
 route, 304  
 USMT, 38  
 UT, 295

Volume Activation  
 Management Tool, 44  
 NAT-PT, Network Address  
 Translation — Protocol  
 Translation, 226

nawigacja Aero, 74  
 niebezpieczne witryny, 254  
 niezawodność, 276  
 NP, Nested Page Tables, 15  
 NRPT, Name Resolution  
 Policy Table, 225  
 numery seryjne  
 podzespołów, 44

## O

OA, OEM Activation, 43  
 obiekt logiczny, 146  
 obraz WIM, 25  
 ochrona  
 klucza VMK, 331  
 systemu, 296

oczyszczanie dysku, 287  
 odświeżanie systemu, 300  
 odtwarzanie filmów  
 i muzyki, 260  
 odzyskiwanie  
 hasła, 330  
 systemu, 297

ograniczanie uprawnień  
 programów, 313  
 okna, 70

okno  
 akceleratora, 244  
 Centrum akcji, 273  
 Eksploratora plików, 77  
 nawigacji, 76  
 ustawień komputera,  
 109

okres prolongaty, 44

określanie połączeń  
 bezprzewodowych, 204  
 opcje logowania, 172  
 oryginalność (legalność)  
 kopii, 43

## P

pakowanie plików, 83  
 pamięć operacyjna, 14  
 panel sterowania, 119  
 pasek

aplikacji, 62, 63  
 charm, 62, 63  
 stanu, 73  
 ustawień, 64  
 wyszukiwania, 65  
 zadań, 61, 64, 104

PCR, Platform  
 Configuration Register,  
 328

plik  
 VHDX, 30  
 wf.msc, 342

pliki  
 .img, 81  
 .inf, 42  
 .iso, 81  
 i foldery, 82  
 WIM, 25  
 XML, 247

plugin, 232  
 płyta startowa Windows  
 PE, 24

PMTU, Path Maximum  
 Transmission Unit, 212  
 pobieranie sterowników, 136  
 poczta elektroniczna, 234  
 podgląd zdarzeń, 281  
 podpis cyfrowy programu,  
 320, 321

podsystem WOW16, 18  
 pokaz slajdów, 102  
 połączenia sieciowe, 201  
 połączenie internetowe, 236  
 modem DSL, 236  
 modem GSM, 236  
 punkt dostępowy, 236  
 VPN, 237

pomoc, 95  
 online, 96  
 zdalna, 292

- POP3, Post Office Protocol, 234  
 port 80, 231  
 powiadomienia, 101, 108  
 poziomy  
   bezpieczeństwa, 166  
   obowiązkowości, 317  
   ważności, 274  
 prawa, 192, 194  
 preferencje zasad grupy, 130  
 problemy, 291  
   z aplikacjami, 304  
   z siecią, 301  
   z systemem operacyjnym, 296  
 procesor, 14, 15  
 profile  
   mobilne, 117  
   użytkowników, 195  
 program  
   DiskPart, 30  
   DriverMax, 37  
   Łatwy transfer, 38  
   ophcrack, 191  
   Skype, 236  
   talk, 236  
   Windows Media Player, 261  
 programy  
   szyfrujące dyski, 326  
   uruchamiane automatycznie, 270  
   Windows, 263  
 protokół, 230  
   HTTP, 231  
   HTTPS, 232  
   IPSec, 224  
   NTLM, 190  
   POP3, 234  
   SMB, 213  
   SMB2, 216  
   TCP/IP, 208  
   stos nowej generacji, 211  
   TKIP, 207  
 przeglądanie InPrivate, 257  
 przeglądarka  
   fotografii, 262  
   Internet Explorer, 240  
 przełączanie  
   pomiędzy oknami, 60, 74  
   użytkowników, 50  
 przepustowość sieci lokalnych, 213
- przypinanie  
   aplikacji, 58  
   programów, 105  
 przywracanie  
   skasowanych plików, 89  
   sterowników, 135  
   systemu, 299  
 pulpit, 101  
 punkt dostępowy, 205, 214  
 punkty przywracania, 296
- ## R
- raportowanie problemów, 291  
 reguła Przychodzące WS-Discovery, 228  
 reguły  
   dodatkowe, 337  
   domyślne, 336, 337  
   zawężone, 337  
 rejestrator  
   dźwięków, 263  
   problemów, 294  
 rejestry PCR, 328  
 resetowanie  
   hasła, 187, 188  
   systemu, 300  
 RFC, Request for Comments, 230  
 rozdzielczość ekranu, 60, 112  
 rozmiar  
   jednostki alokacji, 79  
   skompresowanego folderu, 85  
 rozszerzony tryb ochrony, 249  
 rozwiązywanie problemów, 291  
 RSAT, Remote Server Administration Tool, 129  
 RSS, Really Simple Syndication, 246
- ## S
- SACK, Selective Acknowledgements, 211  
 SACL, System Access Control List, 164
- SAN, Storage Area Network, 327  
 scalanie ikon, 106  
 sekcja  
   Ogólne, 110  
   Personalizacja, 109  
   Powiadomienia, 109  
   Prywatność, 110  
   Udostępnianie, 110  
   Ułatwienia, 111  
   Uruchamianie i odzyskiwanie, 118  
   Windows, 112  
   Wyszukiwanie, 109  
 sektor  
   MBR, 29  
   rozduchowy, 81  
 serwer  
   DNS, 233  
   proxy, 239  
   wydruku, 154  
 serwery główne, 233  
 SID, Security Identifier, 164  
 sieć, 201  
   ad hoc, 208  
   bezwolnowodowa, 201  
   lokalna, 214, 238  
   WPA, 207  
   ukryta, 204  
   VPN, 237  
 skalowalność sieci, 214  
 skanery, 156  
 sklep Windows, 67, 68  
 składniki systemu, 122  
 SLAT, Second Level Address Translation, 15  
 SMB, Server Message Block, 213  
 sortowanie, 77  
 sprawdzanie  
   błędów, 285  
   integralności komputera, 328  
   kompatybilności, 20  
   konfiguracji urządzeń, 41  
   obrazu instalacyjnego, 26  
 SSID, Service Set Identifier, 203  
 standard  
   802.11i, 206  
   SLAT, 15

standard  
 URI, 231  
 WEP, 205  
 standardy sieci Wi-Fi, 202  
 sterowniki, 132, 136  
 sterowniki podpisane, 17  
 subskrypcja wiadomości  
 RSS, 247  
 sumy kontrolne, 328  
 sygnał punktu  
 dostępowego, 205  
 symbole wieloznaczne, 94  
 system UEFI, 15, 327  
 szybkie formatowanie, 79  
 szybkość odczytywania, 79  
 szyfrowanie, 327  
 dysku, 80, 332  
 dysku systemowego, 326  
 dysku USB, 333  
 folderu, 334  
 plików, 334  
 w WEP, 205

## Ś

śledzenie operacji  
 sieciowych, 295

## T

tabela NRPT, 225  
 tablice tęczowe, Rainbow  
 Tables, 191  
 TCG, Trusted Computing  
 Group, 14  
 technologia  
 EFS, 334  
 odciążania, 212  
 ReadyBoost, 289  
 SLAT, 16  
 testowanie nieaktywnych  
 bram, 212  
 tło pulpitu, 102  
 token  
 AT, 317  
 SAT, 317  
 TPM, Trusted Platform  
 Module, 14  
 translacja nazw, 232  
 tryb  
 CBC, 327  
 chroniony aplikacji, 318

chroniony  
 przeglądarki, 319  
 jądra, 17  
 pełnoekranowy, 57  
 TPM, 331  
 TPM + PIN, 331  
 TPM + USB, 331  
 USB, 331  
 tunele IPSec, 224  
 tworzenie  
 dysku resetowania  
 hasła, 186  
 grup lokalnych, 183  
 grupy domowej, 216  
 kont użytkowników,  
 174  
 partycji, 27  
 reguł domyślnych, 336  
 skrótów, 191  
 typ MIME, 232  
 typy bibliotek, 84

## U

uchwyt zmiany wielkości,  
 73  
 udostępnianie  
 bibliotek i folderów, 220  
 zasobów komputera,  
 220  
 ulubione strony WWW, 245  
 UNC, Universal Naming  
 Convention, 178  
 uprawnienia, 151, 192  
 do udostępnionych  
 zasobów, 221  
 NTFS, 192, 222  
 programów, 313  
 standardowego  
 użytkownika, 316  
 udziałów, 222  
 URI, Uniform Resource  
 Identifier, 231  
 URL, Uniform Resource  
 Locator, 230  
 uruchamianie systemu, 48,  
 297, 299  
 urządzenia, 133  
 audio, 157  
 biometryczne, 160  
 Bluetooth, 159  
 nietypowe, 137  
 USB, 157

usługa  
 BranchCache, 228  
 DNS, 232, 234  
 e-mail, 234  
 FTP, 235  
 IRC, 236  
 SkyDrive, 144  
 wczesnej ochrony, 16  
 Windows Anytime  
 Upgrade, 45  
 Windows Defender,  
 341  
 Windows Sklep, 67  
 wstępnego  
 wczytywania do  
 pamięci, 48  
 WWW, 230  
 wyszukiwania, 90  
 zarządzania kluczami,  
 44  
 usługi  
 internetowe, 230  
 systemowe, 124, 127  
 USMT, User State  
 Migration Tool, 38  
 ustawienia  
 domyślne, 123  
 konta, 177  
 systemu, 115  
 usuwanie prywatnych  
 danych, 256  
 uszkodzenie urządzenia, 80  
 uspienie systemu, 53  
 UT, Unified Tracing, 295  
 uwierzytelnianie, 164

## V

VHD, Virtual Hard Disk, 29  
 VPN, Virtual Private  
 Network, 237

## W

wady aktualizacji, 34  
 WAT, Windows Activation  
 Technologies, 43  
 WEP, Wired Equivalent  
 Privacy, 205  
 widoki, 78  
 WIM, Windows Imaging  
 Format, 25

Windows 8, 10, 18  
 Windows 8 Enterprise, 18  
 Windows 8 Pro, 18  
 Windows Defender, 339, 340  
 Windows Media Player, 261  
 Windows RT, 18  
 wirtualizacja Hyper-V, 16  
 wirtualna maszyna Javy, 313  
 wirtualny dysk twardy, 29  
 właściwości  
   komputera, 113  
   systemu, 114  
 woluminy, 140  
   dublowane, 142  
   łączone, 141  
   NTFS, 28  
   proste, 141  
   RAID 5, 142  
   rozłożone, 142  
 współdzielenie jednego  
   połączenia, 238  
 wstążka, 72  
 wstępne wczytywanie do  
   pamięci, 289  
 WWW, World Wide Web, 230  
 wybór architektury, 16  
 wydajność, 269  
   przeglądarki, 242  
   sieci, 215  
 wygaszacz ekranu, 103  
 wykres stabilności  
   systemu, 280  
 wykrywanie  
   niedostępności sąsiadów, 211  
 wykrywanie routerów, 212  
 wylogowywanie, 50  
 wyłączenie komputera, 53  
 wyłudzenie informacji, 253  
 wymagania sprzętowe, 14  
 wymuszanie reguł, 339  
 wyszukiwanie, 90, 91  
 wyszukiwanie  
   komputerów, 218

**X**

XSS, Cross-site-scripting, 251

**Z**

zaawansowane ustawienia  
   systemu, 115  
 zabezpieczenia systemu, 17  
 zakładka  
   Aplikacje, 268  
   Historia aplikacji, 269  
   Szczegóły, 271  
   Uruchamianie, 270  
   Użytkownicy, 270  
   Wydajność, 269  
 zamknięcie sesji, 81  
 zamykanie systemu, 48  
 zapisywanie  
   obrazu dysku, 81  
   płyt, 80  
   stron WWW, 247  
 zapomniane hasło, 186  
 zaporą systemu Windows, 342  
 zarządzanie  
   drukowaniem, 153  
   dyskami, 78  
   grupami lokalnymi, 180  
   kontami, 169  
   pamięcią, 288  
 zasady grupy, 69, 108, 126, 228  
   preferencje, 129  
 zasady grupy lokalne, 128  
 zasady sterowania  
   aplikacjami, 335, 336, 340  
 zasoby  
   pomocy technicznej, 96  
   udostępnione, 217  
   usług sieciowych, 93  
   zdalnych komputerów, 93  
 zasób firmowy, 225

zmiana  
   edycji systemu, 45  
   hasła, 187  
   kolejności drukowania, 153  
   wersji językowej, 121  
   wielkości woluminu, 140  
 zmienna  
   %username%, 179  
   Path, 119



# 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**

