abc systemu Windows 10 PL

Danuta Mendrala
Marcin Szeliga

Zaprzyjaźnij się z systemem Windows 10!

- Nowe firanki w starych okienkach, czyli czym może Cię zachwycić Windows 10
- Wirtualne pulpity i tryb continuum, czyli jak używać systemu na laptopie i tablecie
- Coś dla poszukiwaczy, czyli jak w pełni wykorzystać nowy eksplorator i centrum powiadomień

Helion

Redaktor prowadzący: Michał Mrowiec

Projekt okładki: Jan Paluch

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

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/abcw1p
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-0828-2

Printed in Poland.

SPIS TREŚCI

abc

6

SIECI LOKALNE

Dziś trudno sobie wyobrazić pracę z komputerem bez dostępu do lokalnej sieci komputerowej i do internetu. System Windows 10 zawiera funkcje sieciowe, które ułatwiają konfigurowanie i używanie sieci oraz czynią je bezpieczniejszymi i bardziej niezawodnymi. Są nimi grupy domowe, czyli zaufane sieci lokalne, w ramach których jest możliwa bezpieczna wymiana plików, udostępnianie drukarek czy przesyłanie multimediów. Najnowszy system Windows pozwala także zabezpieczyć połączenia bezprzewodowe i oznaczyć je jako połączenia taryfowe.

Z tego rozdziału dowiesz się, jak skonfigurować połączenie sieciowe, jakie narzędzia i technologie oferuje swoim użytkownikom system Windows 10 oraz jak udostępniać w sieci lokalnej zasoby komputera i korzystać z udostępnionych w tej sieci zasobów innych komputerów.

Ustawienia sieciowe

Windows 10 zapewnia kontrolę nad siecią na dwa sposoby:

1. Poprzez okno *Sieć i Internet* — to okno ustawień pozwala bezpośrednio lub poprzez znajdujący się w nim odnośnik do klasycznego okna konfiguracyjnego z żądanymi ustawieniami wybrać odpowiednią opcję.
2. *Centrum sieci i udostępniania* — jest to okno, w którym zebrano wszystkie zadania związane z siecią.

Sieć i Internet

Listę sekcji okna *Sieć i Internet* mieliśmy okazję poznać w poświęconym konfiguracji systemu rozdziale 3. W tym punkcie przyjrzymy się funkcjom sieciowym, które za jego pomocą mogą zostać skonfigurowane.

Sekcja *Wi-Fi* (dostępna tylko wtedy, jeśli komputer jest wyposażony w kartę bezprzewodową) zawiera listę dostępnych sieci W-Fi. Po kliknięciu dowolnej z nich będziemy mogli się podłączyć do danej sieci lub odłączyć od niej. Ta sekcja pozwala też skonfigurować sieci W-Fi, co zostało opisane w punkcie „Sieci bezprzewodowe".

Sekcja *Tryb samolotowy* pozwala włączyć lub wyłączyć tryb, w którym są wyłączone wszystkie urządzenia bezprzewodowe.

Trzecia sekcja okna zawiera informację na temat liczby danych pobranych przez poszczególne aplikacje w ciągu ostatniego miesiąca, czyli informacje przydatne osobom korzystającym z połączeń 3G i taryfowych.

Sekcja VPN pozwala przede wszystkim tworzyć i konfigurować połączenia VPN. Wirtualne sieci prywatne (ang. *Virtual Private Network*) to połączenia typu punkt-punkt (połączenia pomiędzy dwoma komputerami) przez sieć prywatną lub sieć publiczną (taką jak Internet), nawiązywane w celu zabezpieczenia przesyłanych przez nie danych przed podsłuchaniem i modyfikacją. Aby to osiągnąć, w sieciach VPN używa się specjalnych protokołów tunelowania, takich jak L2TP czy SSTP. Te protokoły pełnią trzy funkcje:

1. Opakowują (hermetyzują) przesyłane dane, tak aby mogły być one przesłane przez sieci TCP/IP, takie jak Internet.
2. Pozwalają uwierzytelnić użytkownika na zdalnym serwerze.
3. Szyfrują przesyłane dane, chroniąc w ten sposób ich poufność.

Poniższe informacje pozwolą wybrać odpowiedni z wbudowanych w system Windows 10 protokołów tunelowania.

1. Protokół PPTP (ang. *Point-to-Point Tunneling Protocol*) do szyfrowania danych używa opracowanego przez Microsoft protokołu MPPE (ang. *Microsoft Point-to-Point Encryption*). Ta metoda szyfrowania była w przeszłości łamana i chociaż Microsoft ją udoskonalił, nie cieszy się ona powszechnym zaufaniem. Zaletą protokołu PPTP jest to, że hermetyzuje on pakiety protokołu IP (opakowuje je w datagramy protokołu PPP, ang. *Point-to-Point Protocol*), co oznacza, że jego konfiguracja jest łatwa, a połączenie VPN można zestawić między dowolnymi sieciami. Do uwierzytelniania są używane protokoły MS-CHAP v2 lub EAP-TLS, co oznacza, że tożsamość użytkownika może być potwierdzona za pomocą hasła lub certyfikatu (np. zapisanego na karcie inteligentnej). Proces tworzenia tunelu PPTP przebiega według następującego schematu:
   - **a)** Klient zdalnego dostępu wysyła na port TCP 1723 komunikat SCCR (ang. *Start Control Connection Request*).
   - **b)** Serwer RAS w odpowiedzi wysyła na dynamicznie przydzielony port TCP komunikat SCCRe (ang. *Start Control Connection Reply*).
   - **c)** Klient odpowiada, wysyłając komunikat OCR (ang. *Outgoing Call Request*). Ten komunikat zawiera wykorzystywany przez protokół GRE identyfikator *Call ID*.
   - **d)** Potwierdzeniem utworzenia tunelu jest wysłanie przez serwer komunikatu OCRe (ang. *Outgoing Call Reply*).

   Po utworzeniu tunelu, aby kontrolować nawiązane połączenie, oba tworzące go komputery okresowo wymieniają między sobą komunikaty *Echo Request* i *Echo Reply*. W wypadku wystąpienia jakiegoś błędu serwer VPN informuje o nim wszystkich klientów, wysyłając komunikat WEN (ang. *WAN Error Notify*).

   Dane przesyłane poprzez tunel PPTP zostają kilkakrotnie „opakowane”:
   - **a)** Dane PPP zostają zaszyfrowane i kapsułkowane (opakowywane w dane innego protokołu) w celu utworzenia ramki PPP.
   - **b)** Następnie ramka PPP zostaje kapsułkowana za pomocą nagłówka protokołu GRE[1].
   - **c)** Kolejnym etapem jest kapsułkowanie otrzymanego pakietu za pomocą nagłówka IP adresu klienta i serwera RAS.
   - **d)** Ostatnim etapem jest dodanie nagłówka warstwy łącza danych. Umożliwia to przesłanie pakietu IP poprzez dowolną sieć

[1] Protokół GRE (ang. *Generic Routing Encapsulation*) jest przykładem prostego protokołu kapsułkowania danych przesyłanych przez sieci IP. Firma Microsoft zmodyfikowała opisany w dokumentach RFC 1701 oraz 1702 standard, dostosowując go do potrzeb protokołu PPTP.

komputerową (jeżeli tunel został utworzony przez komputery znajdujące się w tej samej sieci typu Ethernet, pakiet zostanie opatrzony nagłówkiem i stopką protokołu Ethernet).

Po otrzymaniu danych przesłanych przez tunel PPTP dane zostają kolejno „odpakowane" i odczytane. Proces zamykania tunelu PPTP przebiega następująco:

a) Klient wysyła komunikat CCR (ang. *Call Clear Request*).

b) Po jego otrzymaniu serwer wysyła do klienta komunikat CDN (ang. *Call Disconenct Notify*). Za pomocą tego komunikatu serwer informuje, że nawiązane połączenie zostanie zamknięte (ten komunikat zostanie wysłany również w wypadku zainicjowanego przez serwer zamknięcia tunelu).

c) Klient wysyła komunikat StCCR (ang. *Stop Control Connection Request*), informując serwer, że połączenie kontroli tunelu zostaje przerwane.

d) W odpowiedzi serwer wysyła komunikat StCCRe (ang. *Stop Control Connection Reply*), co przerywa połączenie z klientem.

2. Protokół L2TP (ang. *Layer Two Tunneling Protocol*) jest połączeniem protokołu PPTP i L2F (ang. *Layer 2 Forwarding)* — technologii opracowanej przez firmę Cisco Systems. Do szyfrowania jest używany standardowy protokół IPSec. Podobnie jak protokół PPTP, protokół L2TP kapsułkuje ramki protokołu PPP w celu przesłania ich przez sieć IP. Jednak w tym wypadku zarówno komunikaty sterujące, jak i dane protokołu L2TP, są przesyłane w postaci komunikatów protokołu UDP. Proces utworzenia tunelu L2TP przebiega według następującego schematu:

a) Klient dostępu zdalnego wysyła, w celu ustanowienia połączenia kontroli, komunikat SCCR. Ten komunikat zawiera pole *Tunnel ID*, wykorzystywane do identyfikacji tunelu.

b) W odpowiedzi serwer RAS wysyła komunikat SCCRe.

c) Po otrzymaniu komunikatu SCCRe klient wysyła komunikat SCCC (ang. *Start Control Connection Connected*), potwierdzając poprawne ustanowienie tunelu.

d) Następnie klient wysyła komunikat OCR, będący prośbą o nawiązanie połączenia L2TP. Ten komunikat zawiera pole *Call ID*, wykorzystywane do identyfikacji połączenia w ramach ustanowionego tunelu.

e) W odpowiedzi serwer wysyła do klienta komunikat OCRe.

f) Po jego otrzymaniu klient ponownie wysyła komunikat SCCC, potwierdzając poprawne nawiązanie połączenia.

Po utworzeniu połączenia oba tworzące go komputery okresowo wymieniają między sobą komunikaty *Hello*. Jeżeli nie otrzymają na nie odpowiedzi, tunel jest likwidowany. W wypadku wystąpienia jakiegoś błędu serwer informuje o nim wszystkich klientów, wysyłając komunikat WEN. Dane przesyłane poprzez tunel L2TP również zostają kilkakrotnie „opakowane":

a) Dane protokołu PPP zostają kapsułkowane w celu utworzenia ramki PPP.

b) Następnie dane zostają kapsułkowane za pomocą nagłówka protokołu L2TP.

c) Kolejnym etapem jest kapsułkowanie za pomocą nagłówka protokołu UDP, w którym zarówno port źródłowy, jak i docelowy są ustawione na 1701.

d) Opcjonalnie datagramy UDP zostają zaszyfrowane i kapsułkowane za pomocą nagłówka i stopki protokołu IPSec ESP. Dodatkowo do ramki jest dołączana stopka protokołu IPSec AH.

e) Następnie pakiet IPSec zostaje kapsułkowany za pomocą nagłówka IP, zawierającego adresy serwera i klienta zdalnego połączenia.

f) Ostatnim etapem jest dodanie nagłówka warstwy łącza danych. Umożliwia to przesłanie pakietu IP poprzez dowolną sieć komputerową.

Po otrzymaniu danych przesłanych przez tunel L2TP dane zostają kolejno „odpakowane" i odczytane. Do uwierzytelnienia przekazu jest używana stopka IPSec AH, do jego odszyfrowania — nagłówek IPSec ESP, a do identyfikacji tunelu i połączenia — pola *Tunnel ID* oraz *Call ID*, znajdujące się w nagłówku L2TP. Proces zamykania tunelu L2TP przebiega następująco:

a) Dowolny z komputerów biorących udział w komunikacji wysyła komunikat CDN, informując w ten sposób, że nawiązane połączenie zostanie przerwane.

b) W odpowiedzi drugi komputer wysyła komunikat StCCRe, informując, że tunel zostanie zlikwidowany.

3. Protokół SSTP (ang. *Secure Socket Tunneling Protocol*) jest nowym protokołem tunelowania korzystającym z protokołu HTTPS realizowanego za pośrednictwem portu TCP 443 w celu przepuszczenia ruchu przez zapory i serwery Proxy w sieci Web, które mogą blokować ruch PPTP i L2TP/IPsec. Protokół SSTP zapewnia mechanizm hermetyzacji ruchu PPP w kanale SSL (ang. *Secure Sockets Layer*) protokołu HTTPS — używanie protokołu PPP umożliwia obsługę metod silnego uwierzytelniania, takich jak EAP TLS, natomiast kanał SSL dostarcza zabezpieczenia na poziomie transportu z szyfrowaniem i sprawdzaniem integralności danych.

Tworzenie połączenia VPN sprowadza się do:

1. Przejścia do sekcji VPN okna *Sieć i Internet*.
2. Kliknięcia przycisku *Dodaj połączenie VPN*.
3. Wybrania wbudowanego w Windows 10 dostawcy sieci VPN.
4. Podania nazwy połączenia (np. *Praca*).
5. Wpisania adresu IP lub nazwy serwera VPN.
6. Wyboru protokołu tunelowania oraz sposobu uwierzytelniania.
7. Po kliknięciu przycisku *Zapisz* połączenie zostanie utworzone i pojawi się na liście dostępnych połączeń VPN. Żeby je nawiązać, wystarczy zaznaczyć połączenie VPN i kliknąć przycisk *Połącz*.

Sekcja *Połączenia telefoniczne* pozwala, wbrew nazwie, tworzyć połączenia różnych typów: telefoniczne (zawiązywane za pośrednictwem modemu) oraz VPN. Pozwala ona również konfigurować dostępne w sieci urządzenia sieciowe, takie jak routery — wszystkie te operacje możemy przeprowadzić, klikając odnośnik *Skonfiguruj nowe połączenie*.

W sekcji *Ethernet*, oprócz odnośników do różnych zadań Panelu Sterowania oraz Centrum sieci i udostępniania, znajdują się ikony połączeń sieciowych. Po kliknięciu dowolnego z nich zostanie wyświetlone okno pozwalające wyłączyć dane połączenie oraz skopiować do schowka jego dane konfiguracyjne (w tym adresu IP i MAC). Konfiguracja połączeń sieciowych została opisana w dalszej części rozdziału.

Ostatnia sekcja *Serwer Proxy* pozwala skonfigurować serwer pośredniczący — serwer przechowujący lokalną kopię zasobów wybranych serwerów WWW i FTP. Po jego włączeniu połączenie ze stroną WWW jest realizowane według następującego schematu:

1. Żądanie klienta zostaje wysłane do serwera Proxy zamiast do docelowego serwera WWW.
2. Serwer Proxy sprawdza, czy żądane dane (np. strona WWW) zostały już zbuforowane. Jeżeli tak, zostają one wysłane do klienta. Jeśli nie, serwer Proxy łączy się z docelowym serwerem WWW, pobiera potrzebne dane, buforuje je i odsyła do klienta.

W rezultacie nie tylko dane trafiają do klienta szybciej, ale dodatkowo klient pozostaje anonimowy — w końcu to serwer Proxy, a nie jego komputer, połączył się z serwerem WWW.

Serwer Proxy można skonfigurować automatycznie lub ręcznie. Automatyczna (domyślnie włączona) konfiguracja polega na włączeniu lub wyłączeniu mechanizmu WPAD (ang. *Web Proxy Auto-Discovery Protocol*). Jego działanie polega na pobraniu przez Windows 10 pliku *wpad.dat*, a następnie skonfigurowaniu na jego podstawie reguł przesłania danych przez serwer Proxy. Do wykrycia komputera udostępniającego plik *wpad.dat* są kolejno stosowane:

1. Serwer DHCP (jest do niego wysyłane żądanie *Proxy autodiscovery*).
2. Serwer DNS/LLMNR (do serwera DNS jest wysyłane zapytanie typu A, czyli zapytanie o adres hosta, w wypadku braku odpowiedzi jest rozgłaszany komunikat LLMNR (ang. *Link-local Multicast Name Resolution*).
3. Protokół NetBIOS (jest rozgłaszane zapytanie o host *wpad*).

Ręczna konfiguracja polega na:

1. Włączeniu serwera Proxy.
2. Podaniu adresu tego serwera.
3. Opcjonalnym podaniu listy wyjątków (adresów, z którymi komputer będzie się łączył bezpośrednio).

Centrum sieci i udostępniania

Centrum sieci i udostępniania zawiera informacje o sieci, do której jest podłączony komputer, oraz sprawdza, czy jest możliwe nawiązanie połączenia z internetem. Jest także możliwe 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. 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*.
2. W sekcji *Wyświetl podstawowe informacje o 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).

3. W sekcji *Zmień ustawienia sieciowe* znajdują się odnośniki do:
   a) Kreatora konfiguracji nowego połączenia, pozwalającego połączyć się z internetem, utworzyć połączenie VPN[2] (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.

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 10 — jeżeli komputer jest wyposażony w wiele kart sieciowych, dla każdej z nich jest tworzone połączenie z kolejnym numerem.

W wypadku większości kart wystarczy podłączyć je do komputera i uruchomić Windows 10, 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 za pomocą kabla RJ-45.
2. Jeżeli nadal nie będziesz miał połączenia z siecią, kliknij ikonę połączenia sieciowego prawym przyciskiem myszy i wybierz opcję *Diagnozuj*.

[2] 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.

3. Jeżeli problem występuje po stronie systemu Windows 10 (problemy sieciowe mogą być też skutkiem awarii urządzeń sieciowych), będzie możliwe jego automatyczne rozwiązanie. Zaakceptuj zaproponowane przez kreator rozwiązanie.

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.

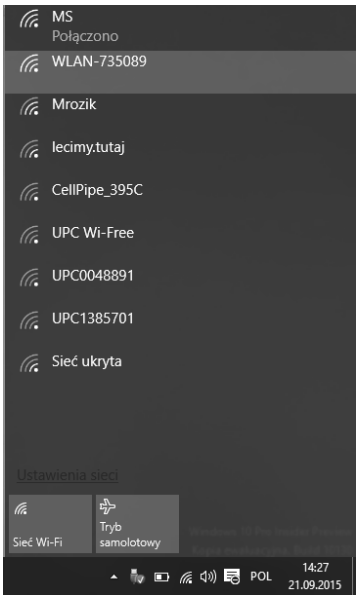
Konfiguracja sieci bezprzewodowych w systemie Windows 10 jest szybka, łatwa i bezpieczna. Po pierwsze, funkcja rozpoznawania sieci lokalizuje dostępne sieci bezprzewodowe, informuje o ich konfiguracji oraz wykrywa zmiany w konfiguracji sieci i dostosowuje do nich system operacyjny. Po drugie, dzięki pełnej obsłudze bezpiecznych protokołów zabezpieczeń bezprzewodowych, takich jak WPA2, przesyłane dane są odpowiednio zabezpieczane.

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 znacznie obniżyć poziom bezpieczeństwa sieci bezprzewodowej.

Żeby połączyć się z siecią bezprzewodową:

1. Włącz kartę bezprzewodową.
2. Kliknij znajdujący się w dolnej części paska ustawień przycisk *Dostępne* — zostaną wyświetlone dostępne sieci bezprzewodowe (rysunek 6.1).
3. Ewentualnie 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 to 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.

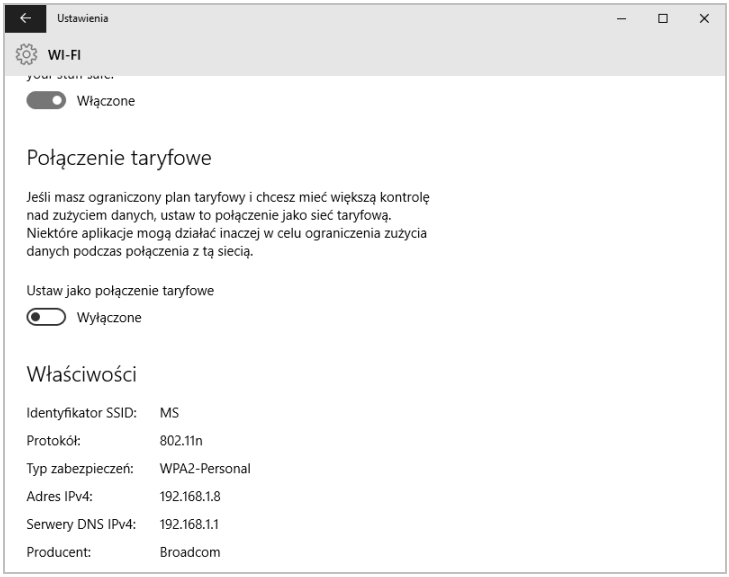


Rysunek 6.1. Okno dostępnych sieci bezprzewodowych. Niezabezpieczone sieci bezprzewodowe będą oznaczone ikoną ostrzeżenia — odradzamy korzystanie z takich połączeń

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

Konfiguracja sieci bezprzewodowych musi być przeprowadzona częściowo w okienku *Ustawień*, częściowo poprzez Panel sterowania. Zaczniemy od przedstawienia opcji dostępnych w sekcji Wi-Fi okna ustawień:

1. Wyświetl listę dostępnych sieci i kliknij znajdujący się na jej dole odnośnik *Ustawienia sieci*, albo naciśnij kombinację klawiszy *Windows +I* i wybierz kategorię *Sieć i Internet*.
2. Kliknij znajdujący się poniżej listy sieci odnośnik *Opcje zaawansowane* — wyświetli się okienko kontekstowe pozwalające włączyć lub wyłączyć udostępnianie zasobów komputera innym użytkownikom tej sieci i określić połączenie jako taryfowe (takie, w którym płacimy za ilość przesłanych danych). Dodatkowo zostanie wyświetlona konfiguracja aktywnego połączenia bezprzewodowego (rysunek 6.2).



Rysunek 6.2. W systemie Windows 10 jest możliwość określenia połączeń bezprzewodowych jako taryfowych. Jeżeli płacisz za przesyłane przez daną sieć dane (jak to ma miejsce między innymi w sieciach 4G), ustawienie połączenia taryfowego spowoduje ograniczenie pobieranych przez nią danych — wówczas na przykład będą pobierane wyłącznie krytyczne aktualizacje zabezpieczeń, dołączony do systemu program pocztowy będzie pobierał jedynie 20 KB każdej wiadomości e-mail, a Outlook nie będzie domyślnie pobierał przez takie sieci żadnych wiadomości

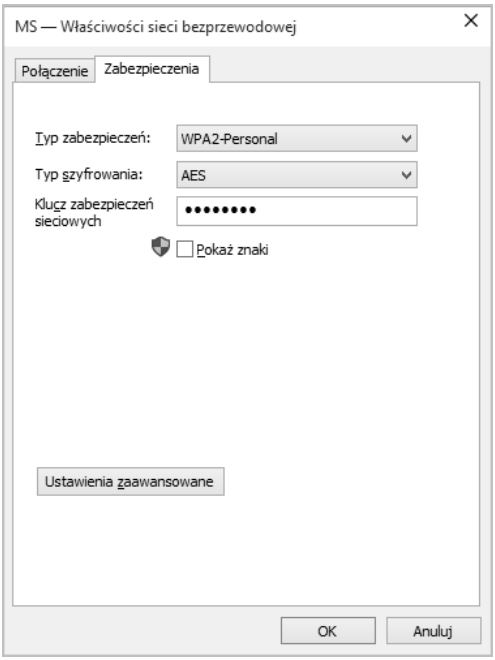
3. Naciśnij znajdujący się w lewym górnym rogu okienka przycisk *Wstecz* — ponownie zostanie wyświetlona sekcja *Wi-Fi* okienka ustawień.
4. Kliknij odnośnik *Zarządzaj ustawieniami sieci Wi-Fi*. Zostanie wyświetlone okno pozwalające skonfigurować funkcje udostępniania sieci bezprzewodowych. Łącząc się z siecią Wi-Fi, możemy zdecydować, czy chcemy udostępnić ją znajomym. Jeśli to zrobimy, a nasz znajomy znajdzie się w zasięgu takiej sieci, będzie się mógł z nią automatycznie połączyć bez podawania współdzielonego hasła do tej sieci. W tym miejscu możemy włączyć to udostępnianie i zdecydować, dla których kontaktów (np. znajomych z serwisu Facebook) będzie ona włączona.

Pozostałe ustawienia połączenia bezprzewodowego, w tym hasło do sieci, możemy odczytać i zmienić poprzez *Centrum sieci i udostępniania*:

1. Kliknij prawym przyciskiem myszy widoczną na pasku zadań ikonę połączenia sieciowego i wybierz z menu kontekstowego opcję *Otwórz Centrum sieci i udostępniania*.
2. Dwukrotnie kliknij lewym przyciskiem myszy ikonę połączenia W-Fi.
3. Kliknij przycisk *Właściwości sieci bezprzewodowej*.
4. 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 zabezpieczane



Ponieważ atakujący, dysponując odpowiednio czułą i dużą anteną kierunkową, jest w stanie odebrać sygnał punktu dostępowego z odległości kilku kilometrów, w 1999 roku 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 wypadku 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 jest wyliczana 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 przy użyciu algorytmu 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 kilkukrotnie 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 nagłówków. 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. Ten standard 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 przy użyciu algorytmu 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 zabezpieczana przy użyciu technologii 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*.

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 wypadku 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 z nich korzystać 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 10 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@sswOrd
```

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

```
netsh wlan start hostednetwork
```

4. Zostanie utworzone 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 przy użyciu przycisku *OK*.

Protokół TCP/IP

TCP/IP (ang. *Transmission Control Protocol/Internet Protocol*) jest standardowym, rutowalnym (umożliwiającym przesyłanie pakietów pomiędzy sieciami) 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 wypadków, aby uzyskać dostęp do wszystkich wymaganych usług sieciowych, jest potrzebna 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 *Wi-Fi*).
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 wypadku 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 10 rozwiązanie problemu.
   c) Wydając polecenie `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 Twojego 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 jest możliwa 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 10 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. Ta funkcja 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 (liczba 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 wypadku dużego okna odbiorczego TCP znacznie zwiększa ona wysyłaną liczbę 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 dane są przesyłane . Jeżeli jednak router lub znajdująca się po drodze zapora 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 10. Nie oznacza to jednak, że jest to konfiguracja w każdym wypadku 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 wydaj poniższe polecenie:

```
netsh interface tcp show global
Querying active state...

TCP Global Parameters
----------------------------------------------
Receive-Side Scaling State          : enabled
Chimney Offload State               : disabled
NetDMA State                        : disabled
Direct Cache Access (DCA)           : disabled
Receive Window Auto-Tuning Level    : normal
Add-On Congestion Control Provider  : none
ECN Capability                      : disabled
RFC 1323 Timestamps                 : disabled
Initial RTO                         : 3000
Receive Segment Coalescing State    : disabled
Non Sack Rtt Resiliency             : disabled
Max SYN Retransmissions             : 2
```

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 autodostrajania okna odbierania, wydaj polecenie:

```
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 są coraz częściej łączone 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[3].

Zastosowaną po raz pierwszy w systemie Windows Vista (w 2006 roku) drugą wersję protokołu SMB (SMB2) opracowano[4] z myślą o:

---

[3] 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.

[4] W przeciwieństwie do protokołu SMB, protokół SMB2 został w całości opracowany przez firmę Microsoft i jest jej intelektualną własnością.

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^{64}) i zwiększenie limitu udziałów do 4 294 967 296 (2^{32}).
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 wypadku 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 otworzenia 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 są przesyłane 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[5] czasu oczekiwania na wyniki typowych operacji sieciowych, takich jak przeglądanie udostępnionych w sieci udziałów.
3. **Poprawie bezpieczeństwa** — pakiety SMB2 są podpisywane nawet w wypadku, gdy nie zostanie to uzgodnione między klientem a serwerem. Do podpisywania pakietów jest używana kryptograficzna funkcja mieszania HMAC SHA-256, a nie przestarzała i niegwarantująca bezpieczeństwa funkcja MD5.

[5] 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.

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

1. Uruchom Panel sterowania.
2. Kliknij znajdujący się w sekcji *Sieć i Internet* odnośnik *Wybierz grupę domową i opcje udostępniania*.

3. Przejdź do sekcji *Grupa domowa*.

4. Jeżeli urządzenie będzie podłączone do sieci, w której istnieje grupa domowa, zostanie ona znaleziona. W takim wypadku kliknij przycisk *Przyłącz się teraz* — zostanie uruchomiony kreator dołączania do grupy domowej:
   a) Odpowiadając na pierwsze pytanie kreatora, kliknij przycisk *Dalej*.
   b) Zostanie wyświetlona lista zasobów (bibliotek oraz drukarek), które możesz udostępnić innym użytkownikom grupy. Decydując się na ich udostępnienie, pamiętaj, że udostępnione w ten sposób zasoby będą dostępne dla wszystkich innych członków grupy domowej, a więc dla wszystkich osób, które zalogują się na dowolnym z należących do tej grupy urządzeń. Po zdecydowaniu, które zasoby zostaną udostępnione, kliknij przycisk *Dalej*.
   c) Wpisz hasło grupy domowej (jeżeli używasz konta Microsoft, a grupa domowa została założona przez Ciebie na innym urządzeniu, wpisywanie hasła nie będzie konieczne) i kliknij przycisk *Dalej*.
   d) Jeżeli w przyszłości będziesz chciał opuścić grupę domową, wystarczy raz jeszcze wyświetlić listę jej ustawień, przewinąć ekran w dół i wybrać opcję *Opuść*.

5. Jeżeli sieć, do której urządzenie jest podłączone, została określona jako prywatna, ale grupa domowa nie została w niej znaleziona, będzie dostępna opcja *Utwórz grupę domową* — wybierz ją (te same opcja są dostępne w Eksploratorze, po wybraniu w okienku nawigacji grupy domowej). Zostanie uruchomiony kreator tworzenia grupy domowej:
   a) Kliknij przycisk *Dalej*.
   b) Wybierz zasoby, które będą udostępniane w grupie domowej — domyślnie są udostępniane pliki multimedialne i drukarki.
   c) Kliknij przycisk *Dalej* i zapisz hasło grupy domowej. To hasło będzie potrzebne do podłączenia do grupy domowej innych komputerów z systemem Windows 10, 8 lub 7 (urządzenia z zainstalowanym systemem Windows 8 lub 10, na których są założone konta tego samego użytkownika, zostaną automatycznie dodane do grupy domowej).

Zmienić ustawienia grupy domowej, w tym określić udostępniane w niej zasoby, możemy w każdej chwili, wpisując w okienku wyszukiwania frazę `grupa domowa` i uruchamiając znalezione w ten sposób okienko konfiguracyjne.

Praca w sieci

Po skonfigurowaniu połączenia sieciowego możesz rozpocząć pracę w sieci — Windows 10 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 wypadkach 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. Jest też możliwa bezpośrednia interakcja z wybranymi urządzeniami — na przykład sterowanie odtwarzaniem muzyki.

Wykonaj poniższe czynności, żeby przejrzeć zasoby sieci lokalnej:

1. Uruchom Eksplorator plików.
2. Wybierz lokalizację *Sieć* lub *Grupa domowa* — można to zrobić:
   a) Wpisując lub wybierając te opcje w pasku adresu.
   b) Klikając je 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 wypadku 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 wypadku 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, która będzie symbolizować dany 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 przycisk *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 opcję *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 10 udostępnianie zasobów Twojego 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 *Eksplorator plików* i znajdź folder lub bibliotekę, które chcesz udostępnić innym użytkownikom sieci lokalnej lub grupy domowej.
2. 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%`.

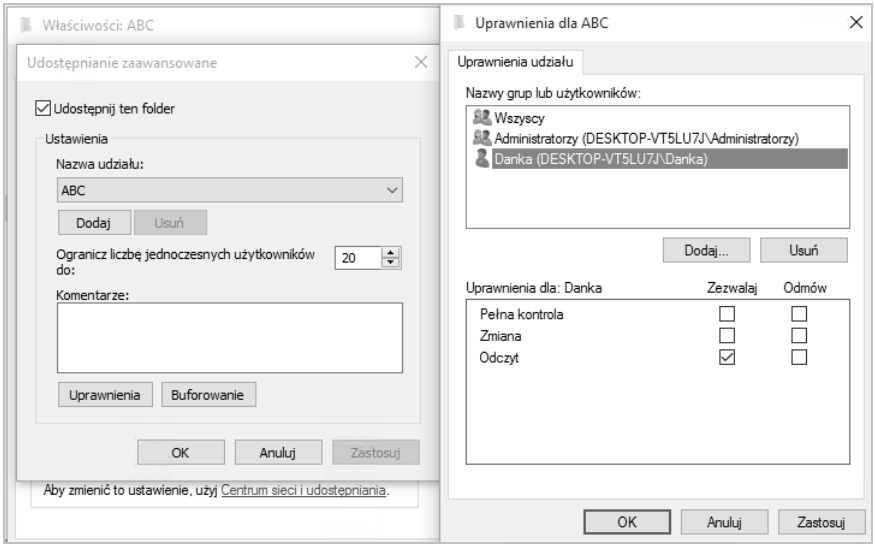
2. Zaznacz dowolny plik lub podfolder. W oknie szczegółów wyświetli się informacja o jego udostępnieniu.

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) Zostanie określona maksymalna liczba użytkowników jednocześnie korzystających z udziału (system Windows 10 Pro 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 udostępnionym folderom 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 10 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:

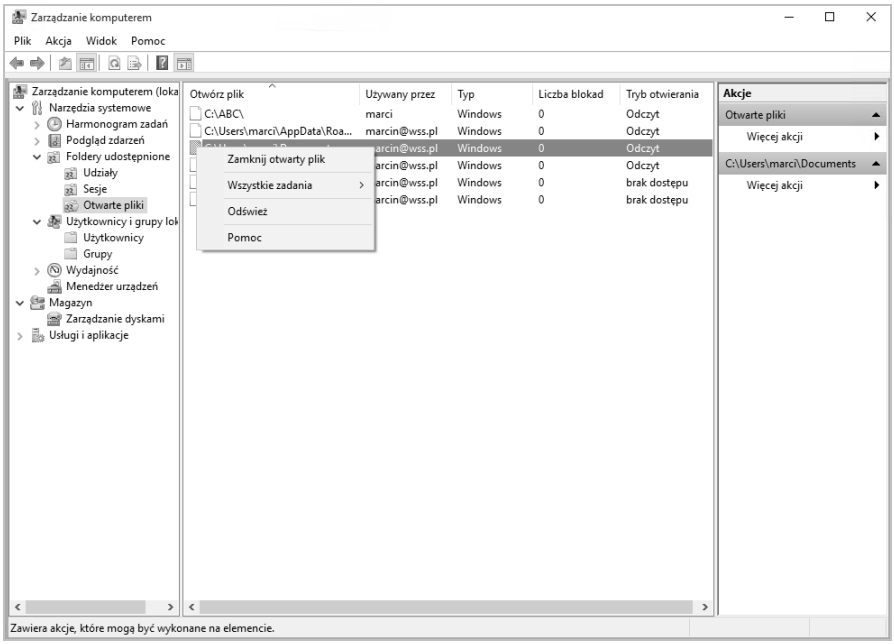
1. Zastosuj kombinację klawiszy *Windows+X* i wybierz opcję *Zarządzanie komputerem*. Wyświetli się konsola administracyjna Zarządzanie komputerem — rozwiń zarejestrowaną w niej konsolę *Foldery udostępnione*. Innym sposobem jest wpisanie na ekranie startowym polecenia `fsmgmt.msc` i uruchomienie znalezionego programu.

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[6].

4. Żeby zobaczyć, kto w tym momencie przegląda zasoby Twojego komputera, kliknij sekcję *Sesje*. Wskazane sesje będziesz mógł natychmiast zakończyć.

5. Zaznacz sekcję *Otwarte pliki* — w głównym oknie konsoli wyświetlą się informacje na temat plików wykorzystywanych przez użytkowników innych komputerów (rysunek 6.5).



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

[6] Po zatrzymaniu ich udostępniania zostaną one ponownie automatycznie udostępnione po kolejnym uruchomieniu komputera.

DirectAccess

Funkcja DA (ang. *DirectAccess*) umożliwia pracownikom korzystanie z zasobów sieci firmowych poprzez internet, a więc niezależnie od tego, gdzie się akurat znajdują. Pamiętaj, że skorzystanie z niej wymaga serwera Windows 2008 R2 lub nowszego oraz edycji Windows 10 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[7].

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 przy użyciu protokołu ESP) do serwera dostępowego firmy:

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,

[7] Administrator sieci może określić, które zasoby i programy będą dostępne dla poszczególnych użytkowników łączących się poprzez połączenia DA.

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 przy użyciu certyfikatów).
4. Odblokowania na zaporach sieci firmowej protokołów:
   a) IPv6 oraz IP 41:
   b) Teredo (portu UDP 3544);
   c) ICMPv6.
5. Jeżeli klienty 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 wypadku każdy z komputerów przechowuje inne zbuforowane pliki. Zanim komputer z systemem Windows 10 pobierze plik ze zdalnego (centralnego) serwera,

sprawdza, czy nie jest dostępna jego zbuforowana kopia; jeżeli tak, pobiera lokalną kopię pliku. Dzięki temu 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.

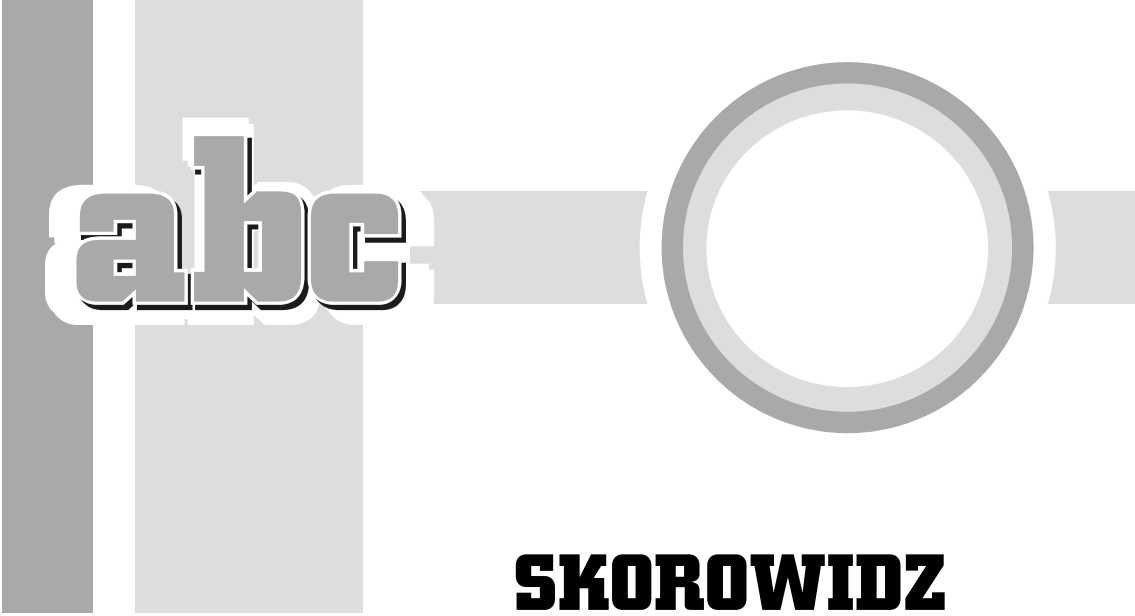
Konfiguracja

Domyślnie funkcja BC jest wyłączona. Żeby ją włączyć:

1. Po stronie komputerów klienckich uruchom konsolę administracyjną *Edytor zasad grupy* (na przykład wpisując polecenie `gpedit.msc` w polu wyszukiwania i uruchamiając znaleziony program).
2. Rozwiń sekcję *Konfiguracja komputera/Szablony administracyjne/Sieć/Usługa 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 jest przede wszystkim wykorzystywana 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

C

D

E

F

G

H

I

K

L

Ł

M

N

O

P

R

S

Ś

T

U

V

W

Z

abc systemu Windows 10 PL

- Instalacja i aktualizacja systemu
- Praca z systemem
- Konfiguracja systemu
- Konfiguracja urządzeń
- Administrowanie kontami użytkowników
- Sieci lokalne
- Internet i multimedia
- **Zabezpieczenia**

Windows 10 — nie daj się zaskoczyć!

Windows 10 niewątpliwie różni się od swoich poprzedników — nie tylko ma szansę w krótkim czasie zastąpić bardzo popularną siódemkę, lecz także jest prawdopodobnie ostatnią numerowaną wersją tego systemu. Jeśli Microsoft wywiąże się ze swoich obietnic, każdy z nas prędzej czy później będzie musiał zetknąć się z nim osobiście. Warto więc dowiedzieć się jak najszybciej, na jakie udogodnienia możemy liczyć jako użytkownicy nowych „okienek".

Ta książka pomoże Ci zorientować się w nowościach i zastosować najróżniejsze sztuczki ułatwiające pracę z systemem. Dowiesz się stąd, jak działa nowe menu Start, na czym polega ujednolicony mechanizm wyszukiwania i jak używać widoków zadań. Sprawdzisz, do czego służą zaufane aplikacje, i poprzypinasz okienka programów do rogów oraz krawędzi pulpitu. Zobaczysz, jak działa centrum powiadomień, wykorzystasz imponujące możliwości eksploratora, a może nawet napiszesz własne skrypty we wbudowanym w Windows środowisku PowerShell. Doceń wygodę i elegancję systemu Windows 10.

Helion

30030 numer katalogowy

księgarnia internetowa

http://helion.pl

zamówienia telefoniczne

0 801 339900

0 601 339900

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

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

ISBN 978-83-283-0828-2

9 788328 308282

Informatyka w najlepszym wydaniu

cena: 39,90 zł