WiFi od Microchipa

Moduł MRF24WB0MA z wbudowaną anteną

Firma Microchip jest jednym z liderów stosowania rozwiązań sieciowych w układach z mikrokontrolerami. Znany i dystrybuowany bezpłatnie stos TCP/IP jest przykładem trafnego przewidywania tendencji rozwoju zastosowań techniki mikroprocesorowej. W ofercie producenta jest dostępny również moduł MRF24WB0MA, zgodny IEEE 802.11b, obsługujący 14 kanałów i mający wszystkie niezbędne certyfikaty: ETSI oraz znaczek WiFi certified (WiFi Alliance). Maksymalny zasięg wynosi ok. 400 m, a maksymalna prędkość transferu danych 1 lub 2 Mb/s.

Trzeba sobie zdawać sprawę, że mimo dostarczenia przez firmę Microchip bezpłatnych, przetestowanych procedur, napisanie działającego programu wykorzystującego komunikację sieciową nie jest zadaniem banalnym szczególnie dla tych, którzy dopiero zaczynają. Dla nich razem ze stosem są dostarczane gotowe, działające aplikacje i dobrze przygotowane pliki pomocy. Aplikacje te mogą być natychmiast testowane na firmowych modułach ewaluacyjnych, a po drobnych modyfikacjach również we własnym środowisku sprzętowym. Nic tak nie zachęca do dalszej pracy jak szybkie uruchomienie interesującego nas zadania.

Podłączenie do sieci LAN urządzenia z mikrokontrolerem wymaga – oprócz zaimplementowania rodziny protokołów TCP/IP – użycia interfejsu fizycznego PHY.

Najbardziej znanym interfejsem fizycznym jest przewodowy interfejs standardu Ethernet. Microchip ma w ofercie własny, bardzo popularny układ ENC28J60 (10 Mbps PHY+MAC), który staje się nieformalnym standardem w ethernetowych interfejsach stosowanych w mikrokontrolerach. Poza tym, dostępne są szybkie interfejsy ENC624J600 (100 Mbps MAC+PHY)), 8-bitowe mikrokontrolery z rodziny PIC18F97J60 z wbudowanym interfejsem Ethernet (MAC+PHY) i 32-bitowe z rodziny PIC32MX6xx i PIC32MX6xx z wbudowanym modułem MAC.

Standard Ethernet charakteryzuje się dużą prędkością i niezawodnością przesyłania danych przy umiarkowanych kosztach wykonania połączeń kablowych. Jest ciągle bardzo popularny w sieciach LAN. Jednak wszyscy wiemy, że coraz bardziej gorącym tematem są połączenia radiowe. Chyba każdy, kto się zetknął z zagadnieniami dotyczącymi połączenia komputera z Internetem słyszał o sieciach WiFi. Praktycznie wszyscy operatorzy dostarczający łącza internetowe indywidualnym odbiorcom oferują routery z opcją bezprzewodowego połączenia WiFi i niemal każdy produkowany obecnie laptop oraz smartfon ma wbudowany taki interfejs. Skąd taka popularność bezprzewodowych połączeń sieciowych? Zapewne przyczyną jest wygoda użytkowania. Można korzystać z połączenia internetowego w dowolnym miejscu mieszkania nie troszczyć się o plączące się kable. Poza tym łącze radiowe daje możliwość bezpłatnego łączenia się w miejscach publicznych (Hotspot), czy komercyjnego dostępu do Internetu w miejscach pozbawionych możliwości łączności przewodowej. Bezprzewodowe połączenie radiowe rozwiązuje problemy z okablowaniem w obiektach przemysłowych. W niektórych zastosowaniach może okazać się wręcz niezastąpione, bo zapewnia izolację galwaniczną pomiędzy układami pracującymi z dużymi różnicami potencjałów, na przykład w energetyce.

Zaleta łączności radiowej jest też jej wadą, ponieważ wszechobecność sygnału radiowego sprawia, że dociera on również do potencjalnych włamywaczy. Bezpieczeństwo transmisji danych wymusza stosowanie mechanizmów kodowania i autoryzacji.

Połączenie Wi-Fi kojarzone jest z sieciami, w których pracują komputery z odpowiednio dużymi zasobami pamięci i mocy obliczeniowej, ale czy możliwe jest połączenie w ten sposób sterownika mikroprocesorowego z siecią WLAN? Jak najbardziej jest możliwe, a odpowiednie rozwiązania oferuje miedzy innymi firma Microchip.

Tabela 1. Najbardziej popularne standardy WiFi

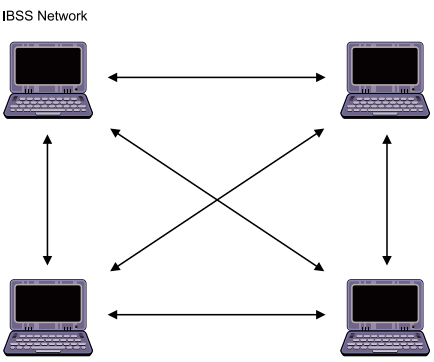
Standard	Prędkość transferu	pasmo
802.11a	54 Mb/s	5 GHz
802.11b	11 Mb/s	2,4 GHz
802.11g	54 Mb/s	2,4 GHz
802.11h	54 Mb/s	5 GHz

Tabela 2. Częstotliwości kanałów w standardzie 802.11b

Kanał	Dolna częstotliwość kanału [GHz]	Środkowa częstotliwość kanału [GHz]	Górna częstotliwość kanału [GHz]
1	2,401	2,412	2,423
2	2,406	2,417	2,428
3	2,411	2,422	2,433
4	2,416	2,427	2,438
5	2,421	2,432	2,443
6	2,426	2,437	2,448
7	2,431	2,442	2,453
8	2,436	2,447	2,458
9	2,441	2,452	2,463
10	2,446	2,457	2,468
11	2,451	2,462	2,473
12	2,456	2,467	2,478
13	2,461	2,472	2,483
14	2,473	2,484	2,495

Parametry i topologia sieci WiFi

Organizacja IEEE opracowała standard IEEE 802.11 przeznaczony do transferu danych w sieciach bezprzewodowych WLAN. Obecnie najbardziej znane są 4 wersje tego standardu: 802.11a, 802.11b 802.11g i 802.11h. Ich podstawowe parametry zamieszczono w **tabeli 1**. Najbardziej popularnym jest 802.11b umożliwiający wymianą danych z teoretyczną prędkością 11 Mb/s. Wbudowany mechanizm *dynamic rate shifting* pozwala na dynamiczną zmianę szybkości transmisji w zależności od stanu kanału transmisyjnego. Wraz ze spadkiem poziomu sygnału lub ze wzrostem poziomu zaburzeń, prędkość przesyłu danych jest zmniejszana do 5,5; 2 lub 1 Mb/s. Równolegle rozwijany standard 802.11a, mimo że zapewnia prawie 5-krotny wzrost prędkości transferu, nie zdobył popularności w Europie. Po pierwsze pracuje w paśmie 5 GHz. W UE to pasmo jest zarezerwowane do celów wojskowych i nie



Rysunek 1. Sieć Ad Hoc

można bez ograniczeń wykorzystywać go dla sieci bezprzewodowych. W Polsce może być używane tylko wewnątrz budynków. Po drugie, nie jest kompatybilny z 802.11b.

W 2003 roku zatwierdzono standard 802.11g mający w założeniu łączyć zalety 802.11a i 802.11b. Znacząca różnica w prędkości wymusiła inne metody modulacji. Nadajnik standardu 802.11b pracuje z modulacją CCK (*Complementary Code Keying*), a 802.11g z modulacją OFDM (*Orthogonal Frequency Division Multiplexing*). Oczywiście, trudno oczekiwać w takiej sytuacji kompatybilności i trzeba stosować karty dwusystemowe. W dwusystemowych modułach WiFi jest wykorzystywany mechanizm protekcji, wykrywający i przełączający moduł na dany typ modulacji. Pasmo 2,4 GHz przydzielone do standardu 802.11b jest podzielone na 14 kanałów każdy o szerokości 22 MHz każdy – wymieniono je w **tabeli 2**. Częstotliwości sąsiednich kanałów zachodzą na siebie. Modulacja CCK pozwala na odseparowanie zaburzeń od nadajników pracujących na częściowo się pokrywających częstotliwościach. W praktyce dąży się do tego, aby bliskie stacje pracowały na tak odległych od siebie częstotliwościach, jak to tylko możliwe.

Topologia sieci Wi-Fi

Sieci WiFi mogą pracować w dwóch trybach: *Ad Hoc* lub *Infrastructure*. Tryb *Ad Hoc* jest typową siecią peer-to-peer i pozwala na tworzenie sieci radiowej wykorzystującej tylko komputery wyposażone w karty sieciowe WiFi. Taka topologia jest nazywana IBSS (*Independent Basic Service Set*). Każdy komputer może się komunikować bezpośrednio ze wszystkimi w sieci (**rysunek 1**). Główną zaletą takiej sieci jest szybka i tania instalacja. Oprócz komputerów z kartami sieciowymi nic innego nie jest potrzebne. Ponieważ wszystkie komputery mogą się komunikować ze sobą to można w prosty sposób zwiększać zasięg sieci, bo część z nich może spełniać rolę „stacji przekaźnikowych". Wadą takiej sieci jest mała liczba pracujących komputerów. Wyłączenie jednego z komputerów spełniających role przekaźnika może spowodować utratę połączenia pomiędzy innymi komputerami w sieci.

Tryb *Infrastructure* wymaga przynajmniej jednego punktu dostępowego tzw. *Access Point*. Każdy komputer w sieci komunikuje się z punktem dostępowym i przez niego przechodzi cała transmisja danych. Komputery nie mogą komunikować się bezpośrednio, jak to jest możliwe w sieci *Ad Hoc*. Wykorzystując tryb *Infrastructure* z przynajmniej jednym punktem dostępowym, tworzy się topologię sieci nazywaną BSS (Basic Service Set). Pokazano ją na **rysunku 2**. Punktem dostępowym może być router z modemem ADSL z funkcją WiFi. Urządzenia tego typu są coraz częściej wykorzystywane w sieciach domowych z dostępem do szerokopasmowego Internetu, dzielonym pomiędzy wszystkie komputery w sieci.

Zabezpieczenia sieci Wi-Fi

Wspomniałem już o jednej z wad sieci Wi-Fi: o podanosci na ataki. Standard IEEE 802.11 ma wbudowany szyfrowany mechanizm zabezpieczenia przed nieautoryzowanym podsłuchem i dostępem WEP. Algorytm szyfrowania opiera się na kluczu o stałej długości 40, 64, 128, 152 lub 256 bitów. Długość klucza jest wybierana przez użytkownika, a sam klucz jest generowany na podstawie podanego hasła. Co ważne, klucz nigdy nie jest przesyłany droga radiową, ale zawsze tworzony lokalnie w każdym urządzeniu należącym do sieci, w tym również w punkcie dostępu. Ma to znacznie utrudnić podsłuchanie przesyłanych zaszyfrowanych danych. W praktyce WEP okazał się bardzo słabym zabezpieczeniem. Klucz nie jest zmieniany w całym czasie posługiwania się hasłem i na dodatek łatwo go złamać za pomocą oprogramowania udostępnianego w Internecie. Dlatego sieci zabezpieczone szyfrowaniem WEP nie są uważane za bezpieczne. Lepszym zabezpieczeniem jest standard WPA. W trakcie transmisji danych klucze szyfrujące są zmieniane dynamicznie, dzięki czemu jest trudniej podsłuchać przesyłanie danych i włamać się do sieci. Autoryzacja w szyfrowaniu WPA może przebiegać ma dwa sposoby. Pierwszy sposób polega łączeniu z serwerem autoryzacji (np. Radius). Drugi wykorzystuje hasło użytkownika, podobnie jak w WEP. Na jego podstawie jest tworzony klucz PSK. WPA jest obsługiwany przez coraz większą liczbę Acces Pointów, a póki co tak zabezpieczona sieć jest uważana za bezpieczną.

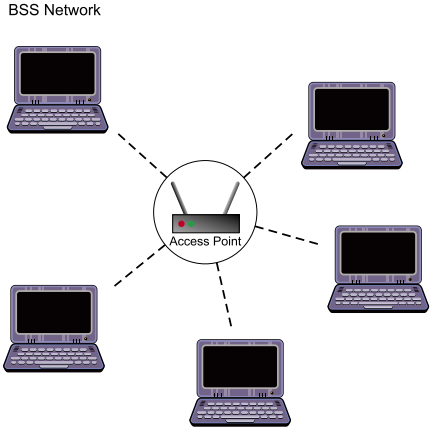
Kolejnym sposobem mającym za zadanie utrudnić życie hakerom jest blokowanie rozgłaszania SSID tj. nazwy sieci. Wyłączenie jej rozgłaszania powoduje, że trudniej jest ją wykryć, bo nazwa nie pojawi się na liście dostępnych sieci.

Problem bezpieczeństwa powoduje, że szuka się innych metod zabezpieczanie przed włamaniem np. filtrowanie adresów MAC kart sieciowych. Jednak jest to zabezpieczenie kłopotliwe i mało skuteczne, ponieważ dzisiaj stosunkowo łatwo można zmienić programowo adresy MAC. Dużo lepiej wyglądają zabezpieczenia definiowane w normie IEEE 802.11i. Wykorzystywany jest tam algorytm silnego szyfrowania AES z kluczami o długości 128, 192 lub 256 bitów oraz uwierzytelnienie EAP i protokół dynamicznej zmiany klucza TKIP. Niestety, ta norma nie jest kompatybilna z IEEE 802.11b.

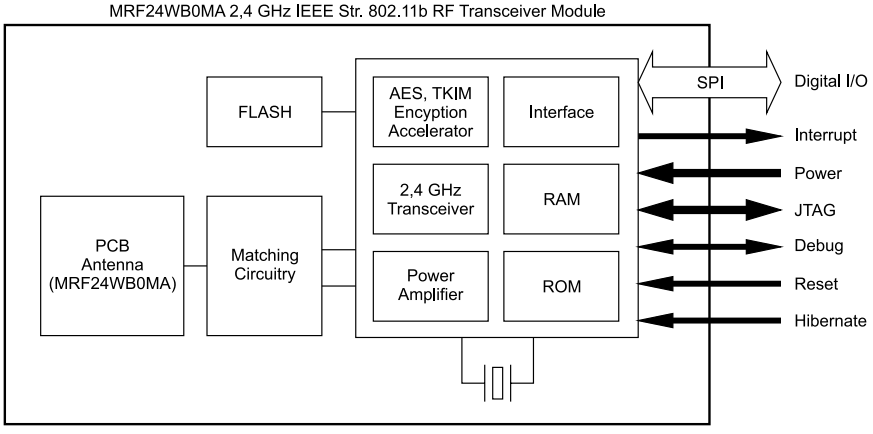
Moduł MRF24WB0MA z wbudowaną anteną

Moduł MRF24WB0MA jest zgodny z normą IEEE 802.11b: obsługuje wszystkie 14 kanałów i ma niezbędne certyfikaty: ETSI i WiFi Alliance (*WiFi certified*). Maksymalny zasięg transmisji wynosi ok. 400 m, a maksymalna prędkość transferu danych 1 lub 2 Mb/s. Aby zapewnić jak najlepsze warunki do przesyłania danych, zastosowano modulowanie nośnej typu DSSS. Jest to technika rozpraszania widma w systemach szerokopasmowych za pomocą ciągów kodowych.

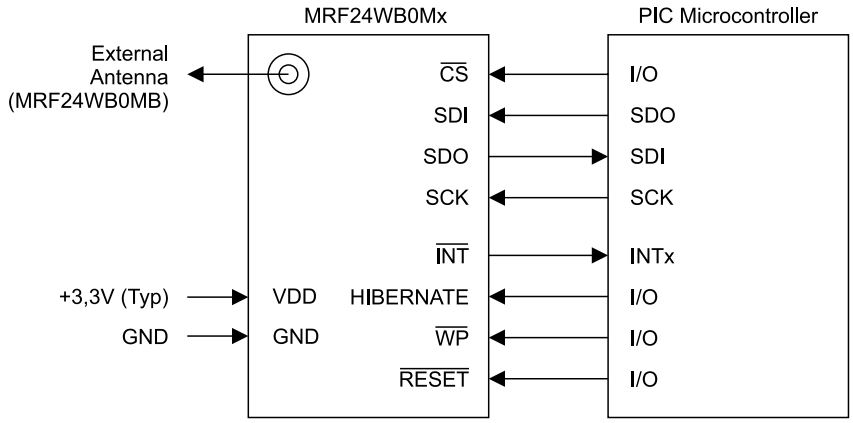
Ciekawie tez wygląda wsparcie technik zabezpieczenia sieci. Wbudowane układy logiczne zapewniają sprzętowe wsparcie kodowania AES i RC4 (RC4 jest używany przy kodowaniu WEP). W praktyce oznacza to możliwość wykorzystania do zabezpieczenia transmisji kodowania WEP, WPA-PSK i WPA2-PSK.



Rysunek 2. Siec Infrastructure



Rysunek 3. Schemat blokowy modułu MRF24WB0MA



Rysunek 4. Połączenie modułu MRF24WB0MA z systemem nadrzędnym

Na **rysunku 3** pokazano schemat blokowy modułu. Mikrokontroler komunikuje się z MRF24WB0MA poprzez 4-przewodową magistralę SPI (**rysunek 4**). Oprócz sygnałów interfejsu SPI są wykorzystywane dodatkowe linie sterujące:

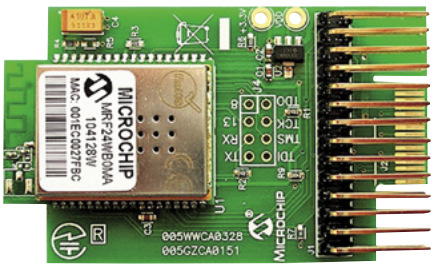
Reset – sprzętowe zerowanie modułu.

Int – wyjście zgłaszające przerwanie (typu otwarty dren).

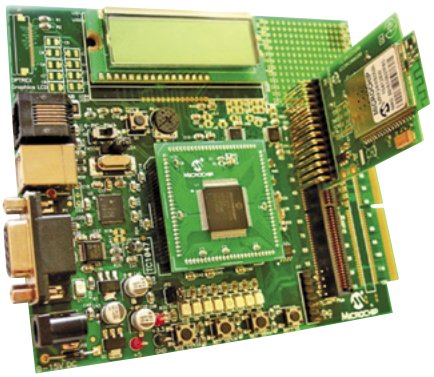
Hibernate – wejście wymuszające stan hibernacji (ograniczanie zużycia energii).

WP – ochrona zapisu wewnętrznej pamięci Flash.

Microchip ma w ofercie również moduł MRF24WB0MB z wejściem dla anteny zewnętrznej. Próby z wykorzystaniem sieci WiFi można znacznie przyspieszyć wykorzystując moduł *WiFi PICtail* przystosowany do zamontowania w złączu szczelinowym popularnego zestawu ewaluacyjnego *Explorer16* – pokazano go na **fotografii 5**. Na płytce oprócz MRF24WB0MA zamontowano stabilizator LDO (+3,3 V) oraz kilka elementów biernych: rezystorów ustalających stany na wejściach modułu i kondensatorów filtrujących napięcie zasilające. Zestaw ewaluacyjny z zamontowanym modułem WI-Fi PicTail pokazano na **fotografii 6**.



Fotografia 5. Wygląd modułu MRF24WB0MA ze złączem do zestawu Explorer 16



Fotografia 6. Zestaw Explorer16 z zamontowanym modułem WI-Fi Pictail

Do najnowszej wersji stosu TCP/IP jest dołączonych wiele programów demonstracyjnych. Jednym z nich jest projekt *TCPIP WiFI EasyConfig Demo App*. Posłuży on nam do zapoznania się z możliwościami pracy sterownika mikroprocesorowego w sieci Wi-Fi. Po zainstalowaniu stosu TCP/IP w katalogu *TCPIP WiFi EasyConfig Demo App* otwieramy gotowy projekt *TCPIP WiFI EasyConfig Demo App – C30 EXPLORER16_16_MRF24WBOM*. Pierwsze próby będą przeprowadzane z konfiguracją sieci IBSS czyli *Ad Hoc*. Nie będzie potrzebny punkt dostępu, bo sterownik będzie komunikował się bezpośrednio z komputerem. Konfiguracja sieci jest zawarta w pliku nagłówkowym *WF_Config.h*, którego fragment zamieszczono na **listingu 1**.

Rozgłaszana nazwa SSID jest wpisywana do tablicy MY_DEFAULT_SSID_NAME. W tym wypadku będzie to EasyConfig. Można ja zmienić na dowolną inną. Topologia sieci jest definiowana za pomocą deklaracji MY_DEFAULT_NETWORK_TYPE. Definiując WF_INFRASTRUCTURE spowodujemy, że sterownik będzie pracował w sieci typu BSS (*Infrastructure*). Domyślnie w projekcie jest to sieć *Ad Hoc*. Definicja MY_DEFAULT_CHANNEL_LIST określa pulę skanowanych kanałów WiFi. Na początek pozostawimy wszystkie domyślne ustawienia konfiguracyjne.

W kolejnym kroku możemy ustawić zabezpieczenia sieci. W dokumentacji projektu zaleca wyłączenie wszystkich zabezpieczeń. Jest do przyjęcia w trakcie prób, ale na krótki czas – ułatwi to diagnostykę, gdy

Listing 1. Fragment pliku WF_Config.h zawierający konfigurację sieci

```
/*-------------------------------------------*/
/* Default settings for Connection Management */
/*-------------------------------------------*/
#define MY_DEFAULT_SSID_NAME      "EasyConfig"
#define MY_DEFAULT_NETWORK_TYPE   WF_ADHOC   //WF_INFRASTRUCTURE or WF_ADHOC
#define MY_DEFAULT_SCAN_TYPE      WF_ACTIVE_SCAN  //WF_ACTIVE_SCAN or WF_
PASSIVE_SCAN
#define MY_DEFAULT_CHANNEL_LIST   {1,6,11}  // use {} to scan all channels
```

Listing 2. Definicja zabezpieczeń

```
/*   WIFI SECURITY COMPILE-TIME DEFAULTS
Security modes available on WiFi network:
  WF_SECURITY_OPEN  :No security
  WF_SECURITY_WEP_40  :WEP Encryption using 40 bit keys
  WF_SECURITY_WEP_104  :WEP Encryption using 104 bit keys
  WF_SECURITY_WPA_WITH_KEY  :WPA-PSK Personal where binary key is given to
MRF24WB0M
  WF_SECURITY_WPA_WITH_PASS_PHRASE  :WPA-PSK Personal where passphrase is
given to MRF24WB0M and it calculates the binary key
  WF_SECURITY_WPA2_WITH_KEY  :WPA2-PSK Personal where binary key is given to
MRF24WB0M
  WF_SECURITY_WPA2_WITH_PASS_PHRASE  :WPA2-PSK Personal where passphrase is
given to MRF24WB0M and it calculates the binary key
  WF_SECURITY_WPA_AUTO_WITH_KEY  :WPA-PSK Personal or WPA2-PSK Personal where
binary key is given and MRF24WB0M will connect at highest level AP supports
(WPA or WPA2)
  WF_SECURITY_WPA_AUTO_WITH_PASS_PHRASE :WPA-PSK Personal or WPA2-PSK Personal
where passphrase is given to MRF24WB0M and it calculates the binary key and
connects at highest level AP supports (WPA or WPA2) */
```

Listing 3. Definicja zabezpieczeń WEP

```
//-------------------------------------------
// Default WEP keys used in WF_SECURITY_WEP_40
// and WF_SECURITY_WEP_104 security mode
//-------------------------------------------
#define MY_DEFAULT_WEP_PHRASE     "WEP Phrase"
// string 4 40-bit WEP keys -- corresponding to passphraseof "WEP Phrase"
#define MY_DEFAULT_WEP_KEYS_40 "\
\x5a\xfb\x6c\x8e\x77\
\xc1\x04\x49\xfd\x4e\
\x43\x18\x2b\x33\x88\
\xb0\x73\x69\xf4\x78"
// string containing 4 104-bit WEP keys -- corresponding to passphraseof "WEP
Phrase"
#define MY_DEFAULT_WEP_KEYS_104 "\
\x90\xe9\x67\x80\xc7\x39\x40\x9d\xa5\x00\x34\xfc\xaa\
\x77\x4a\x69\x45\xa4\x3d\x66\x63\xfe\x5b\x1d\xb9\xfd\
\x82\x29\x87\x4c\x9b\xdc\x6d\xdf\x87\xd1\xcf\x17\x41\
\xcc\xd7\x62\xde\x92\xad\xba\x3b\x62\x2f\x7f\xbe\xfb"
/* Valid Key Index: 0, 1, 2, 3  */
#define MY_DEFAULT_WEP_KEY_INDEX        (0)
```

Listing 4. Definiowanie aktywnego interfejsu SPI

```
/*-------------------------
    MRF24WB0M WiFi I/O pins
  -------------------------
If you have a MRF24WB0M WiFi PICtail, you must uncomment one of these
two lines to use it. SPI1 is the top-most slot in the Explorer 16
(closer to the LCD and prototyping area) while SPI2 corresponds to
insertion of the PICtail into the middle of the side edge connector slot. */

#define MRF24WB0M_IN_SPI1
//#define MRF24WB0M_IN_SPI2
// PIC24FJ256GA110 PIM on Explorer 16 must use SPI2, not SPI1
#if defined(MRF24WB0M_IN_SPI1) && defined(__PIC24FJ256GA110__)
  #undef MRF24WB0M_IN_SPI1
  #define MRF24WB0M_IN_SPI2
#endif
```

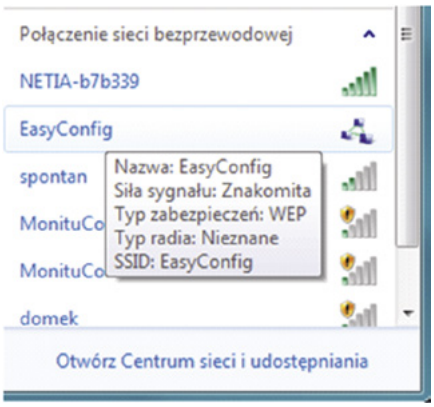
Listing 5. Definicje linii sterujących

```
// MRF24WB0M in SPI1 slot
  #define WF_CS_TRIS      (TRISBbits.TRISB2)
  #define WF_CS_IO        (LATBbits.LATB2)
  #define WF_SDI_TRIS     (TRISFbits.TRISF7)
  #define WF_SCK_TRIS     (TRISFbits.TRISF6)
  #define WF_SDO_TRIS     (TRISFbits.TRISF8)
  #define WF_RESET_TRIS   (TRISFbits.TRISF0)
  #define WF_RESET_IO     (LATFbits.LATF0)
```

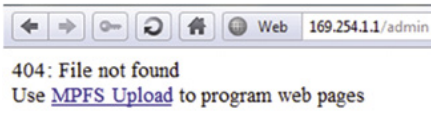
coś nie działa. Dla sieci *Ad Hoc* można użyć zabezpieczenia WEP (WPA jest niedostępne), zastosowałem WEP z kluczem 40-bitowym. Dla tego zabezpieczenia trzeba podać domyślna frazę hasła definiowana w tablicy MY_DEFAULT_WEP_PHRASE i wyliczony klucz startowy zapisany w tablicy MY_DEFAULT_WEP_KEYS_40 (**listing 3**).

Drugim plikiem, do którego warto zajrzeć, jest *HardwareProfile EXPLORER_16_MRF24WB0M C30.h*. Są tam zdefiniowane ustawienia sprzętowe. Dla konfiguracji sprzętowej z fot. 6 nie ma potrzeby niczego tam zmieniać, ale dla innej pewnie trzeba będzie zdefiniować ustawienia. Najważniejsze z nich to definicje linii portu SPI i dodatkowych linii sterujących modułem. Na początku określa się, który ze sprzętowych interfejsów SPI będzie użyty do komunikacji (**listing 4**). Na **listingu 5** zamieszczono definicję linii SPI i sygnału zerowania (RESET). Poziomy na pozostałych liniach sterujących jest wymuszany przez rezystory na płytce WiFi PICtail.

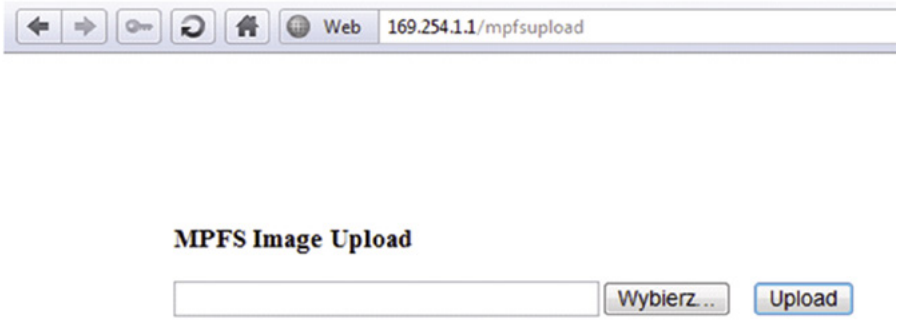
Skonfigurowany projekt trzeba skompilować kompilatorem MPLAB C-30 i wgrać do pamięci Flash mikrokontrolera PIC24FJ128GA010. Po wyzerowaniu mikrokontrolera sterownik zacznie rozgłaszać SSID *EasyConfig*. Ustawiony w pobliżu komputer powinien zidentyfikować sterownik z tą nazwą SSID w sieci *Ad Hoc*, co pokazano na **rysunku 7**. Aby połączyć komputer ze sterownikiem, trzeba kliknąć przycisk *Połacz* umieszczony obok ikony *EasyConfig* i wpisać klucz. Połączenie jest potrzebne, Aby wgrać plik binarny *EasyConfig.bin* z katalogu projektu do pamięci EEPROM umieszczonej na płytce Explorera16. Plik ten zawiera obraz strony internetowej niezbędnej do dalszych eksperymentów z siecią WiFi. W przeglądarce na pasku adresu wpisujemy http://169.254.1.1/admin, co powinno spowodować otwarcie się strony pozwalającej na wgranie pliku (**rysunek 8**). Po kliknięciu na *MPFS Upload* otwiera się strona o adresie http://169.254.1.1/mpfsupload (**rysunek 9**).



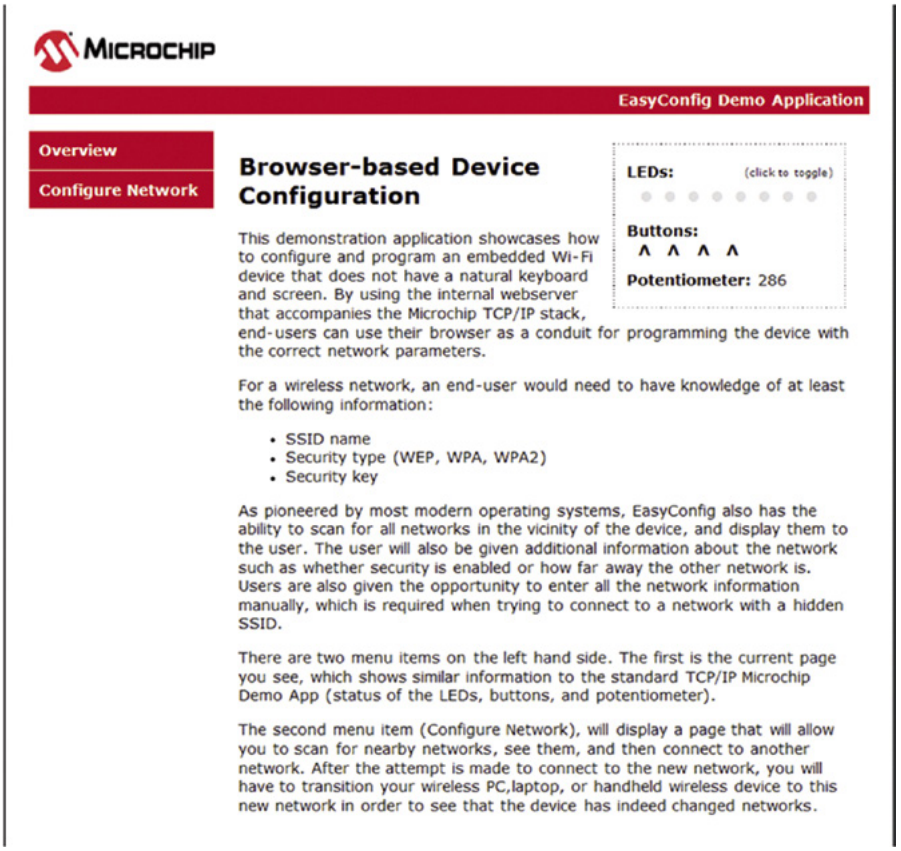
Rysunek 7. Wykrycie sterownika w sieci Ad Hoc (Windows 7)



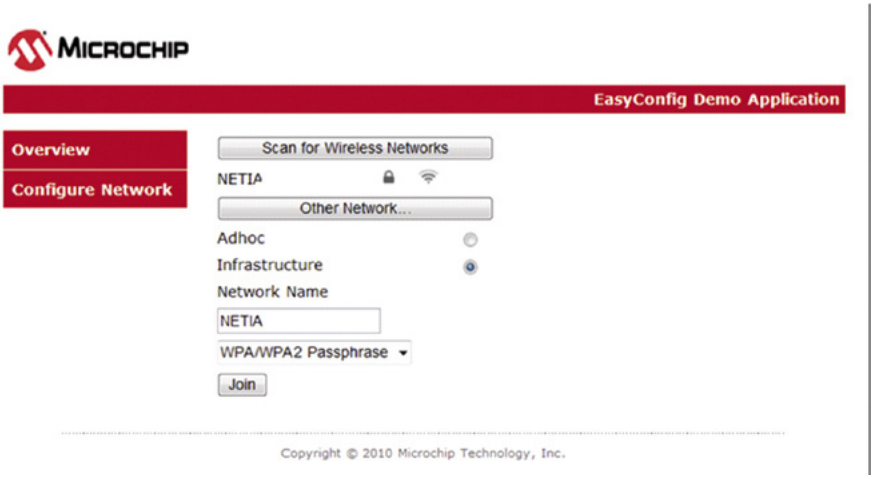
Rysunek 8. Strona po zaprogramowaniu mikrokontrolera



Rysunek 9. Strona wgrywania pliku



Rysunek 10. Strona główna projektu „WiFI EasyConfig"



Rysunek 11. Zmiana konfiguracji sieci

Po wybraniu pliku *EasyConfig.bin* z katalogu projektu i kliknięciu na *Upload* zostanie on przesłany przez sieć WiFi *Ad Hoc* i zapisany w pamięci EEPROM zestawu Explorer 16.

Po wgraniu pliku strony sterownik staje się serwerem http o adresie IP http://169.254.1.1 Na stronie głównej pokazanej na **rysunku 10** można testować komunikację ze sterownikiem lub wybrać podstronę konfiguracji sieci klikając na przycisk *Configure Network*. Komunikacja w sieci WiFi pomiędzy komputerem z otwartą stroną (prawa górna część strony) a sterownikiem polega na:

- Ciągłym przesyłaniu stanu (zapalona lub zgaszona) diod LED D3…D10.
- Możliwości zapalania i gaszenia tych diod przez klikanie na ich symbolach – elementy *LEDs*.
- Przesyłanie stanu (przyciśnięcie lub zwolnienie) czterech przycisków S3…S5 – elementy *Buttons*.
- Przesyłanie napięcia ze ślizgacza potencjometru R6 – element *Potentiometer*.

W czasie testów wszystkie te funkcje działały prawidłowo.

Po przejściu do strony konfiguracji sieci i kliknięciu na *Scan for Wireless Network* są skanowane dostępne SSID oraz wyświetlane informacje o zabezpieczeniach i poziomach sygnałów (**rysunek 11**). Kiedy nowa sieć zostanie wykryta, można przekonfigurować sterownik aby w niej pracował. Ja postanowiłem go tak skonfigurować, aby pracował w mojej domowej sieci z punktem dostępu, którym jest router z modemem ADSL z funkcją WiFi. Aby to było możliwe trzeba zmienić konfigurację z *Ad Hoc* na Infrastructure, podać nazwę SSID punktu dostępu i ustalić rodzaj zabezpieczenia. Sieć jest zabezpieczona mechanizmami kodowania WEP-PSK. Jak wspomniałem, moduł wspiera sprzętowo to zabezpieczenie. Trzeba tylko zauważyć, że ze względu na niewielką w porównaniu z PC moc obliczeniową, potrzebuje do wyliczenia kluczy ok. 30 sekund. Po kliknięciu na przycisk *Join* i podaniu klucza router nawiązał połączenie ze sterownikiem i przydzielił mu wolny adres w lokalnej 192.168.1.4. Adres IP jest wyświetlany na wyświetlaczu Explorera 16, ale można go też odczytać ze strony konfiguracyjnej routera. Teraz strona sterownika jest dostępna pod adresem http://192.168.1.4 lub http://mchpboard i pracuje w tym połączeniu równie dobrze, jak w sieci *Ad Hoc*.

Program demonstracyjny ma funkcję konsoli znakowej ze złączem RS232. Do komunikacji można wykorzystać na przykład Hyper Terminal z systemu Windows. Parametry transmisji to: 19200, 8, N, 1. Na **rysunku 12** pokazano wydruk z konsoli w trakcie pierwszego uruchomienia sterownika po połączeniu z komputerem w sieci *Ad Hoc*. Można w ten sposób obserwować i ewentualnie debugować kolejne etapy łączenia się z siecią pokazane na **rysunku 13** i **rysunku 14**.

Podsumowanie

Sieć WiFi może być bardzo atrakcyjna wszędzie tam, gdzie wykonanie okablowania jest drogie, kłopotliwe lub nawet niewykonalne. Jej użycie powoduje uproszczenie połączeń przy sterowaniu rozproszonym, w którym jest potrzebny kanał łączności do wielu małych sterowników wykonujących na przykład pomiary. Program demonstracyjny Microchipa pokazuje, że włączenie do sieci WiFi sterownika mikroprocesorowego z modułem MRF24WB0MA jest stosunkowo łatwe. Co więcej, konfiguracja sprzętowo – programowa umożliwia zabezpieczenie kodowe WPA-PSK przed włamaniem. Microchip udostępnia wszystko, co niezbędne: darmowy stos TCP/IP oraz darmowy, działający program demonstracyjny, z kompletnym plikami źródłowymi . Jedynym ograniczeniem darmowej licencji jest stosowanie tych rozwiązań z mikrokontrolerami PIC. Zaawansowany programista nie będzie miał żadnych problemów z dopasowaniem programu demonstracyjnego do potrzeb.

Tomasz Jabłoński, EP

Rysunek 12. Wydruk po połączeniu się z siecią Ad Hoc

Rysunek 13. Wydruk po skanowaniu sieci SSID

Rysunek 14. Wydruk po połączeniu się do sieci typu Infrastructure