



**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**

BRNO UNIVERSITY OF TECHNOLOGY



**FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH  
TECHNOLOGIÍ**

**ÚSTAV AUTOMATIZACE A MĚŘICÍ TECHNIKY**

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION  
DEPARTMENT OF CONTROL AND INSTRUMENTATION

## **MOST ETHERNET-IEEE802.15.4**

HW AND SW FOR ETHERNET-TO-IEEE802.15.4 BRIDGE

**BAKALÁŘSKÁ PRÁCE**

BACHELOR'S THESIS

**AUTOR PRÁCE**

AUTHOR

**TOMÁŠ RŮŽIČKA**

**VEDOUCÍ PRÁCE**

SUPERVISOR

**Ing. PETR FIEDLER, Ph.D.**

BRNO 2010



VYSOKÉ UČENÍ  
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky  
a komunikačních technologií

Ústav automatizace a měřicí techniky

# Bakalářská práce

bakalářský studijní obor  
**Automatizační a měřicí technika**

**Student:** Tomáš Růžička

**ID:** 77930

**Ročník:** 3

**Akademický rok:** 2009/2010

**NÁZEV TÉMATU:**

**Most Ethernet-IEEE802.15.4**

**POKYNY PRO VYPRACOVÁNÍ:**

Vypracujte koncepci zařízení, které umožní přenos dat z bezdrátové sítě dle standardu IEEE 802.15.4 na síť Ethernet s protokolem TCP/IP.

**DOPORUČENÁ LITERATURA:**

Dle vlastního literárního průzkumu a doporučení vedoucího práce.

**Termín zadání:** 8.2.2010

**Termín odevzdání:** 31.5.2010

**Vedoucí práce:** Ing. Petr Fiedler, Ph.D.

**prof. Ing. Pavel Jura, CSc.**

*Předseda oborové rady*

**UPOZORNĚNÍ:**

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

## Abstrakt

Předkládaná práce obsahuje teoretické informace o síťových protokolech Ethernet (TCP/IP) a IEEE 802.15.4. Práce dále obsahuje návrh převodníku realizovaného za pomoci vývojového kitu RCM 3365 od firmy Rabbit Semiconductor. Převodník pracuje s pakety protokolu UDP, které umí převést na pakety bezdrátového standartu, nebo z bezdrátového paketu umí vytvořit paket protokolu UDP. Bezdrátová část byla nahrazena sériovým rozhraním RS-232, po kterém putují pakety bezdrátového standartu IEEE 802.15.4. K vytvoření a monitorování dat na straně Ethernetu a na lince RS-232 je využito trojice externích programů.

## Klíčová slova

Ethernet, IEEE 802.15.4, TCP/IP, UDP, ISO/OSI, síť, převodník

## Abstract

The present work includes theoretical information about network protocols, Ethernet (TCP/IP) and IEEE 802.15.4. Work also includes design of the converter realized using the development kit RCM 3365 from the Rabbit Semiconductor company. The converter works with the UDP, which can be converted to packets of wireless standard, or from a wireless packet can create a UDP packet. The wireless part was replaced with a serial interface RS-232, after which the packets travel in wireless standard IEEE 802.15.4. To create and monitor data on the Ethernet and RS-232 three external programs are used.

## Keywords

Ethernet, IEEE 802.15.4, TCP/IP, UDP, ISO/OSI, network, converter

## Bibliografická citace díla

RŮŽIČKA, T. *Most Ethernet-IEEE802.15.4*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 49 s. Vedoucí bakalářské práce Ing. Petr Fiedler, Ph.D.

## Prohlášení

„Prohlašuji, že svou bakalářskou práci na téma Most Ethernet-IEEE802.15.4 jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.“

V Brně dne: **31. května 2010**

.....  
podpis autora

## Poděkování

Děkuji vedoucímu bakalářské práce Ing. Petru Fiedlerovi, Ph.D. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

V Brně dne: **1. června 2010**

.....  
podpis autora

## 1. OBSAH

<b>1. OBSAH</b> .....	<b>5</b>
<b>2. ÚVOD</b> .....	<b>7</b>
<b>3. TEORIE SÍTÍ</b> .....	<b>8</b>
3.1 ISO/OSI MODEL .....	8
3.1.1 Fyzická vrstva .....	9
3.1.2 Linková vrstva .....	9
3.1.3 Síťová vrstva .....	9
3.1.4 Transportní vrstva .....	10
3.1.5 Relační vrstva .....	10
3.1.6 Prezenční vrstva .....	10
3.1.7 Aplikační vrstva .....	11
3.2 IP ADRESA .....	11
3.3 MASKA PODSÍTĚ (SUBNET MASK) .....	11
<b>4. ETHERNET</b> .....	<b>12</b>
4.1.1 Ethernetový rámec .....	12
4.2 MAC ADRESA .....	13
<b>5. TCP/IP</b> .....	<b>14</b>
5.1 TCP .....	15
5.2 UDP .....	17
5.3 TCP vs. UDP .....	17
5.4 INTERNET PROTOKOL (IP) .....	18
5.5 ARP .....	20
5.6 DHCP .....	21
<b>6. BEZDRÁTOVÉ SÍŤE</b> .....	<b>22</b>
6.1 IEEE 802.15.4 .....	22
6.1.1 Architektura .....	23
6.2 FYZICKÁ VRSTVA IEEE 802.15.4 .....	23
6.2.1 Frekvenční rozsahy .....	24
6.2.2 Rozdělení kanálů .....	24
6.2.3 Rámec fyzické vrstvy .....	25
6.3 PODVRSTVA MAC .....	26

6.3.1	<i>Hlavička podvrstvy MAC (MHR)</i> .....	26
6.3.2	<i>Zápatí MAC (MFR)</i> .....	29
6.3.3	<i>Struktura super-rámu</i> .....	31
6.3.4	<i>Formát majákového rámu</i> .....	32
<b>7.</b>	<b>NÁVRH PŘEVODNÍKU</b> .....	<b>36</b>
7.1	PŘIPOJENÍ PŘEVODNÍKU DO SÍTĚ .....	39
7.1.1	<i>Možnosti přidělení IP adresy</i> .....	39
7.2	PŘENOS DAT VE SMĚRU ETHERNET – IEEE 802.15.4 .....	41
7.3	PŘENOS VE SMĚRU IEEE 802.15.4 – ETHERNET .....	44
<b>8.</b>	<b>ZÁVĚR</b> .....	<b>47</b>
	<b>SEZNAM POUŽITÉ LITERATURY</b> .....	<b>48</b>
	<b>SEZNAM POUŽITÝCH ZKRATEK</b> .....	<b>49</b>

## 2. ÚVOD

V dnešních sítích se používá několik druhů síťových protokolů. Tyto protokoly jsou navzájem různé, a pokud chceme komunikovat mezi sítěmi s různými protokoly, musíme vytvořit vhodný převodník.

Cílem této práce je návrh převodníku mezi protokoly IEEE 802.15.4 a Ethernetem. Ethernet je dnes velice rozšířeným protokolem, především pak díky internetu. Naopak protokol IEEE 802.15.4 byl oficiálně normalizován v roce 2003, od této doby prošel několika aktualizacemi, naposledy pak v roce 2009. Bezdrátový protokol IEEE 802.15.4 je o poznání jednodušší než Ethernet s protokoly TCP/IP, proto není možné všechny informace obsažené v paketu Ethernetu přenést pomocí paketu IEEE 802.15.4.

V tomto textu jsou nejprve obsaženy teoretické informace o obou protokolech a dále pak návrh samotného převodníku. K realizaci převodníku je použita základní deska se síťovým modulem od firmy Rabbit Semiconductor a jejich vývojové prostředí Dynamic C. Bezdrátová část je simulována sériovým rozhraním RS-232, po kterém „proudí“ pakety protokolu IEEE 802.15.4.

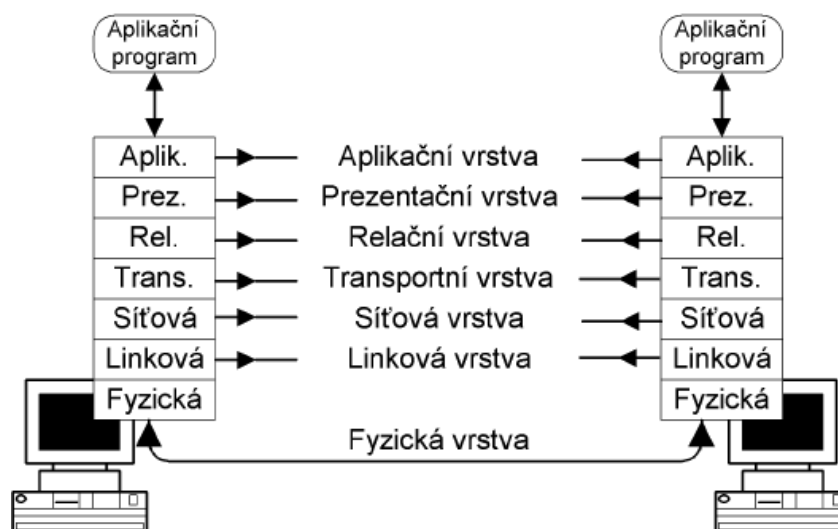
### 3. TEORIE SÍTÍ

Sítí se dá označit propojení minimálně dvou zařízení, které si mezi sebou vyměňují data. Přenos těchto dat je řízen určitými pravidly. Tato pravidla jsou obsažena v tzv. protokolech. Zařízení mohou být propojena pomocí metalických, nebo optických kabelů, ale stejně tak dobře mohou být zařízení v síti zapojena bezdrátově. Typy sítí:

- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (World Area Network)

#### 3.1 ISO/OSI MODEL

Pro výklad o sítích je vhodný tzv. ISO/OSI model. Tento model vznikl již před řadou let. A přesto, že se považuje za základ pro síťové technologie, nebyl nikdy přesně realizován. Podle OSI modelu je vždy možno komunikovat pouze s vrstvou nad nebo pod. A všechny vrstvy musí být v komunikaci obsaženy, což v řadě praktických úloh přináší zbytečnou zátěž (časovou i datovou). Přesto je OSI model vhodný pro výklad a teoretický popis sítí.



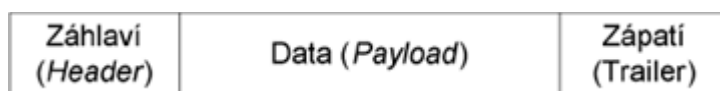
Obr. 1: ISO/OSI model [1]

### 3.1.1 Fyzická vrstva

Definuje přenosové médium, určuje tvar koncovek. Dále říká, jaké bude stínění a další fyzické vlastnosti sítě. Na fyzické vrstvě dochází k reálnému přenosu dat. Tato vrstva přistupuje ke každému bitu stejně a nepozná, které bity patří k sobě.

### 3.1.2 Linková vrstva

Linková vrstva zajišťuje předávání datových rámců fyzické vrstvě v případě, že jsou data odesílána. V opačném případě data z fyzické vrstvy seskupuje do rámců. Každý rámec má záhlaví (header), data (payload) a zápatí (trailer).

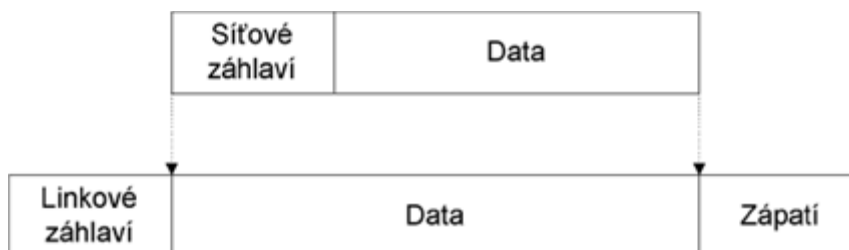


Obr. 2: Linková vrstva [1]

Záhlaví nese informace o adrese příjemce, linkovou adresu odesílatele a další řídicí informace. Oblast dat většinou nese paket vrstvy síťové a zápatí pak kontrolní součet.

### 3.1.3 Síťová vrstva

Tato vrstva se stará o přenos dat mezi vzdálenými počítači, obstarává tedy tzv. směrování. Základní jednotkou je paket, který se balí do datového rámce vrstvy linkové. I paket obsahuje záhlaví a data. A však se zápatím se zde setkáváme pouze zřídka.

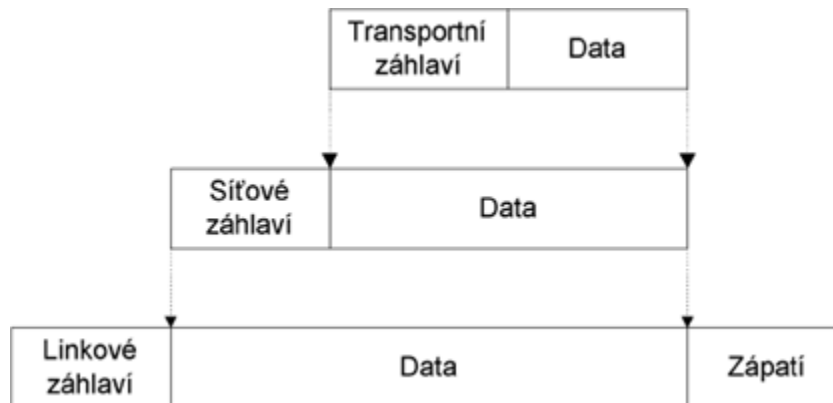


Obr. 3: Síťová vrstva [1]

Na síťové vrstvě pracují veškeré směrovače. V této vrstvě je v celé WAN adresováno síťové rozhraní. Takovýmto rozhraním může být i karta pro Ethernet.

### 3.1.4 Transportní vrstva

Transportní vrstva se zcela spoléhá na služby nižších vrstev. Předpokládá tedy, že spojení mezi počítači je zajištěno, a tak se plně věnuje spojení mezi vzdálenými aplikacemi.



Obr. 4: Transportní vrstva [1]

Mezi počítači může být několik transportních spojení. Počítače jsou z hlediska síťové vrstvy adresovány adresou počítače a z hlediska vrstvy transportní jsou adresovány jednotlivé aplikace. Aplikace jsou dále jednoznačně adresovány v rámci jednoho počítače.

### 3.1.5 Relační vrstva

Relační vrstva zajišťuje zřízení, použití a ukončení spojení (relace) mezi dvěma aplikacemi na různých počítačích. Zajišťuje podporu transakcí, nebo zabezpečení přenášených dat (jejich šifrování), případně i řízení toku a poloduplexnosti (aby například klient nezahltl server příliš mnoha požadavky).

### 3.1.6 Prezenční vrstva

Prezenční vrstva je zodpovědná za reprezentaci a zabezpečení dat. Reprezentace dat může být na různých počítačích různá. Mezi funkce této vrstvy patří např. převod kódů a abeced, modifikace grafického uspořádání, přizpůsobení pořadí bajtů a podobně. Vrstva se zabývá jen strukturou dat, ne jejich významem. Ten je znám jen vrstvě aplikační.

### 3.1.7 Aplikační vrstva

Je to nevyšší vrstva v ISO/OSI modelu. Aplikační vrstva předepisuje, v jakém formátu a jak mají být data přebírána/předávána od aplikačních programů.

## 3.2 IP ADRESA

Jednoznačně identifikuje zařízení v síti. Skládá se ze 4 částí tzv. oktetů. Každá část je velká 8 bitů a odděluje se tečkou. Teoretický rozsah adresování je tedy od „0.0.0.0“ do „255.255.255.255“. Adresa se zapisuje dekadicky, ačkoliv je prezentována binárním číslem.

Při vzniku protokolu IPv4 se zdál rozsah adres více než dostatečný. Sítě byly rozděleny do pěti základních tříd, přičemž první čtyři bity IP adresy rozhodovaly o třídě sítě. Při komunikaci se nepoužívala maska podsítě, protože ta byla napevno dána adresou. V dnešní době tomu už tak není, ale je zde dobře vidět propojení mezi IP adresou a maskou sítě. Proto zde tuto tabulku uvádím.

**Tabulka 1: Rozdělení IP adres [1]**

Třída	První čtyři bity	1. byte	Standardní maska	Bitů sítě	Bitů stanice	Sítí	Stanic v každé síti	CIDR maska
<b>A</b>	0xxx	0–127	255.0.0.0	7	24	128	16 777 216	/8
<b>B</b>	10xx	128-191	255.255.0.0	14	16	16 384	65 536	/16
<b>C</b>	110x	192-223	255.255.255.0	21	8	2 097 152	256	/24
<b>D</b>	1110	224-239	255.255.255.255	multicast				/32
<b>E</b>	1111	240-255	vyhrazeno jako rezerva					

## 3.3 MASKA PODSÍTĚ (SUBNET MASK)

Určuje, která část IP adresy je síťová, a která pro hosty. V binárním tvaru obsahuje jedničky tam, kde se v adrese nachází síť a nuly tam, kde je klient. Maska podsítě je společně s IP adresou součástí základní konfigurace síťového rozhraní. Zapisuje se stejně jako IP adresa. Platná hodnota je taková, kde jsou zleva samé jedničky (v binárním zápisu) a zprava nuly. Jakmile se objeví v zápisu zleva první nula, dále musí následovat pouze samé nuly.

## 4. ETHERNET

Je jeden z řady síťových protokolů. Zabývá se především vrstvou síťového rozhraní. V lokálních sítích má největší zastoupení, především díky jeho jednoduchosti a tím pádem i snadné implementaci do provozu.

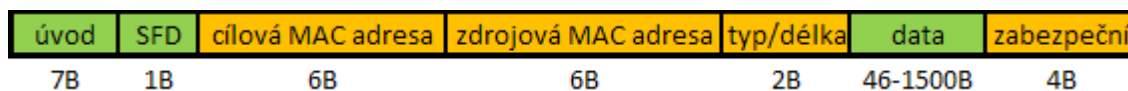
Na počátku byl navržen pro kancelářské aplikace a jeho přenosová rychlost dosahovala rychlostí 10Mbit/s. Postupem času prošel „evolucí“ a dnes se již běžně setkáváme s rychlostmi 1–10Gbit/s.

Ethernet není definován pouze pro klasické kabely (koaxiální, nebo kroucenou dvojlinku), ale i pro bezdrátový přenos a optické vlákno. Pomocí optického kabelu dokáže propojit dvě stanice na velké vzdálenosti s rychlostí vyšší než 1Gbit/s.

### 4.1.1 Ethernetový rámec

Data v síti putují v takzvaných rámcích, nikoliv v paketech. Pakety se tedy „balí“ do rámců, které vznikají až na fyzické vrstvě. Ethernetový rámec obsahuje hlavičku, stejně jako třeba paket.

Ethernetová hlavička obsahuje zdrojovou a cílovou MAC adresu a typ/délku. Typ v hlavičce určuje, jaký protokol je použit na vyšší vrstvě (IP, ARP, atp.). Pro rozlišení jednotlivých rámců se na začátku vysílá speciální úvod (Preamble) složený ze sekvence střídajících se jedniček a nul a také SFD - oddělovač začátku rámce.



**Obr. 5: Ethernetový rámec [9]**

1. *Synchronizace* - Pro rozlišení jednotlivých rámců se na začátku vysílá speciální úvod složený ze sekvence střídajících se jedniček a nul. SDF je oddělovač začátků rámce.

2. *Hlavička* - 14 bytů, které obsahují dvě šestibytové adresy (cílovou a zdrojovou) a dva byty typu polí.
3. *Datová oblast* - má proměnnou délku. Standardní délka je 46 – 1500bytů. Pokud by byla datová část kratší než 46 bytů, bude doplněn nedefinovanými znaky, nebo sadou znaků.
4. *Zabezpečení* - 4 byty obsahující CRC pro detekci vadných rámců.

## 4.2 MAC ADRESA

Jedná se o 48bitové číslo, které identifikuje síťovou kartu. Tato adresa je do karty implementována při výrobě a je celosvětově jedinečná. To zajišťuje výrobce karty spolu s centrálním správcem adresného prostoru. U starších karet byla vkládána přímo do EEPROM pamětí. U moderních karet ji lze dodatečně měnit. Podle standardu by se adresa měla zapisovat jako tři skupiny čtyř hexadecimálních čísel oddělených pomlčkou, nebo dvojtečkou. Častější zápis je takový, kde je adresa rozdělena na šest oddílů po dvou hexadecimálních číslech opět oddělených pomlčkou, nebo dvojtečkou.

Jako příklad uvádím svou MAC adresu (fyzickou adresu), která je zapsána druhým z výše zmiňovaných způsobů zápisů. Fyzickou adresu PC je možné zjistit v příkazovém řádku příkazem „*ipconfig/all*“.

```
Popis : : NVIDIA nForce Networking Controller  
Fyzická Adresa : : 00-11-09-68-D6-A5
```

Obr. 6: Příklad zápisu MAC adresy

Protože moderní síťové karty umožňují změnu své fyzické adresy, nelze vyloučit, že se v síti mohou vyskytnout dvě zařízení se stejnou MAC adresou. V takovém případě není možné zaručit plně fungující spojení v dané síti.

## 5. TCP/IP

Obdobou OSI modelu je TCP/IP, u kterého můžeme říci, že vychází z OSI modelu, ale upravuje jej tak, aby byl více flexibilní. Pod zkratkou TCP/IP (Transmission Control Protocol/Internet Protocol) se skrývá soubor protokolů. Oproti OSI modelu má pouze čtyři vrstvy, ale více se blíží praxi.

**Tabulka 2: Srovnání TCP/IP s OSI modelem**

TCP/IP	OSI
Aplikační	Aplikační
	Prezenční
	Relační
Transportní	Transportní
Síťová	Síťová
Vrstva síťového rozhraní	Linková
	Fyzická

Při srovnání TCP/IP a OSI modelu je vidět, že velkou část úkolů z OSI modelu přebírá v TCP/IP aplikační vrstva. Ta pro nás však není tak zajímavá, jako právě zbylé tři vrstvy, které se nyní pokusím stručně přiblížit.

### **Aplikační vrstva**

Na této vrstvě pracují procesy, které využívají přenosu dat po síti ke konkrétním službám pro uživatelské aplikace.

### **Transportní**

Implementována až v koncových zařízeních. Umožňuje přizpůsobení sítě potřebám aplikace. Poskytuje transportní služby (TCP/UDP).

### **Síťová**

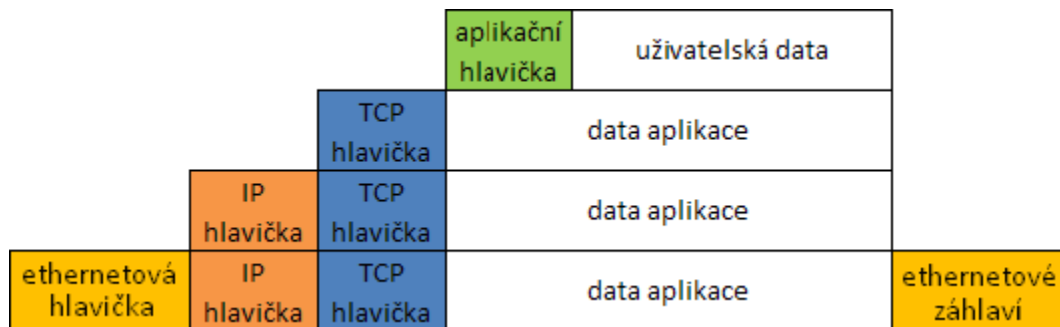
Zajišťuje především síťovou adresaci, směrování a předávání paketů. Je ve směrovacích i koncových zařízeních.

### **Vrstva síťového rozhraní**

Umožňuje přístup k fyzickému přenosovému médiu. Může být specifická pro každou síť.

Při odesílání dat v TCP/IP se provádí tzv. **zapouzdření**. Postup je následující:

1. Aplikační vrstva (aplikace) vezme data, která se mají odeslat, doplní je o aplikační hlavičku a pošle nižší vrstvě.
2. Transportní vrstva přichází data rozdělí na segmenty a přidá TCP (nebo UDP) hlavičku a vytvoří TCP segment.
3. Síťová vrstva doplní IP hlavičku a tím vznikne **paket** (nebo datagram), který je předán vrstvě síťového rozhraní.
4. V nejnižší vrstvě se paketu přiřadí Ethernetová hlavička na začátek a trailer na konec, ten obsahuje FCS (Frame Check Sequence) – kontrolní součet (často se používá pro jeho výpočet CRC – Cyclic Redundancy Check). Takto vznikne **Ethernetový rámeček**.



**Obr. 7: Zapouzdření**

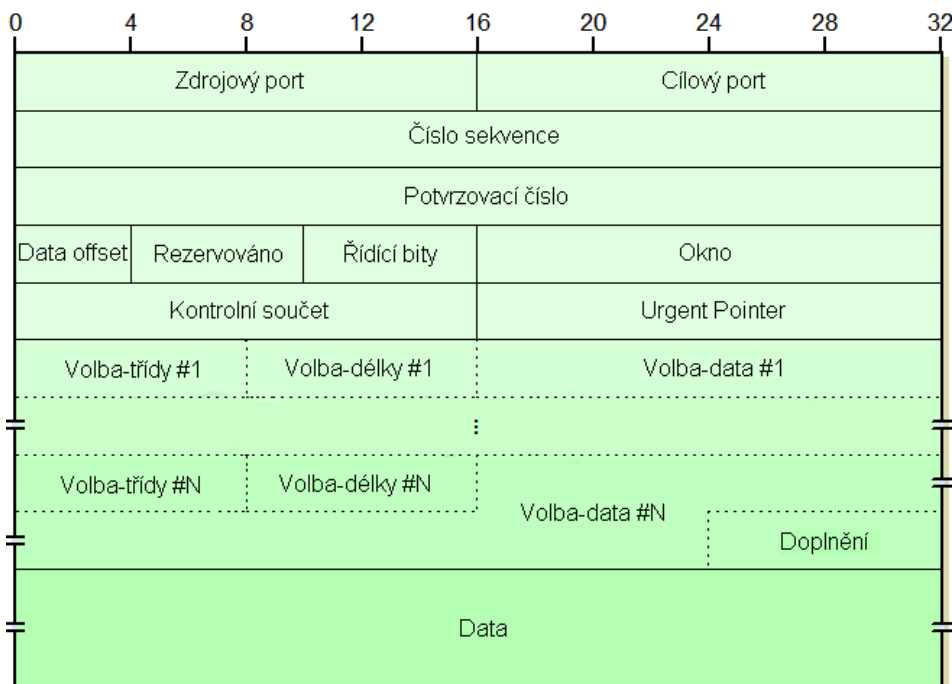
Při přijetí paketu se provádí opačný postup, tedy rozbalování. Je potřeba od dat oddělit hlavičky jednotlivých vrstev a předat data aplikaci.

## 5.1 TCP

Protokol TCP je tzv. transportní protokol, který využívá přenosových služeb síťového protokolu IP. Zatímco IP protokol spojuje dva počítače v síti, TCP spojuje konkrétní aplikace na těchto počítačích.

TCP protokol je určen pro přenos toku bajtů na transportní vrstvě. Jedná se o spolehlivý protokol, TCP rozdělí přichází data na segmenty a přidá TCP hlavičku a tak vytvoří pakety, které předá IP protokolu k přepravě po síti. TCP ověří, že se pakety neztratily tak, že každému paketu přidělil číslo sekvence. Toto číslo se pak použije k ověření, zda data byla přijata ve správném pořadí.

TCP protokol ověřuje, zda přenesená data nebyla poškozena šumem tak, že před odesláním spočítá kontrolní součet, uloží jej do odesílaného paketu a příjemce kontrolní součet vypočítá znovu a ověří, zda se shodují.



**Obr. 8: TCP hlavička [5]**

K rozlišení komunikujících aplikací používá TCP protokol *čísla portů*. Každá strana TCP spojení má přidruženo 16bitové bezznaménkové číslo portu (existuje 65535 portů) přidělené aplikaci. Porty jsou rozčleněny do třech skupin: dobře známé, registrované a dynamické/privátní. Seznam dobře známých portů je přiřazován organizací Internet Assigned Numbers Authority (IANA) a jsou typicky používané systémovými procesy.

**Tabulka 3: Dobře známé porty**

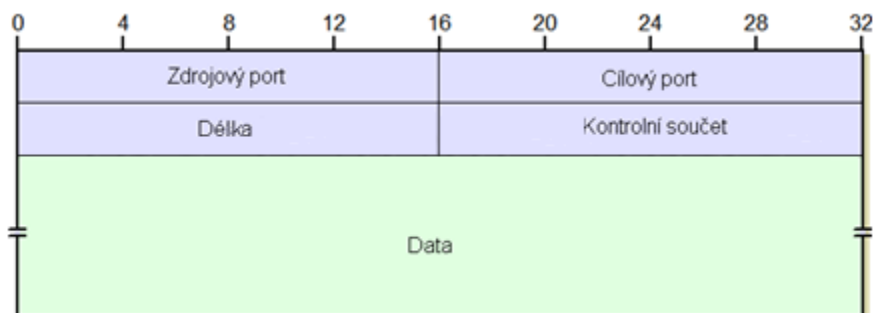
Číslo portu	Běžící Aplikace
7	Echo protokol
20/21	File Transfer Protocol (FTP - data/příkazy)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name Server (DNS)
80	HTTP Server

Registrované porty jsou typicky používané aplikacemi koncových uživatelů při otevírání spojení k serverům jako libovolná čísla zdrojových portů, ale také mohou identifikovat služby. Dynamické/privátní porty mohou být také používány koncovými aplikacemi, ale není to obvyklé.

## 5.2 UDP

V sadě transportních protokolů poskytuje UDP jednoduché rozhraní mezi sít'ovou a aplikační vrstvou. Tento protokol neposkytuje žádné záruky doručení a odesílatelova UDP vrstva si o už jednou odeslaných datagramech neudrží žádné informace. Datagramy mohou přijít vícekrát, v nahodilém pořadí, nebo se mohou vyskytnout další chyby.

UDP hlavička se skládá jen ze 4 políček, z nichž 2 jsou volitelná. Políčka zdrojového a cílového portu jsou 16bitová a identifikují odesílající a přijímající proces. Protože UDP je bezstavový a odesílatel nemusí vyžadovat odpověď, zdrojový port je volitelný. Pokud se nepoužije, měl by být zdrojový port nastaven na nulu. Po číslech portů následuje povinná délka UDP paketu včetně dat, v bytech. Minimální hodnota je 8 bytů. Zbývající políčko hlavičky je 16bitový kontrolní součet pokrývající hlavičku i data. Tento součet lze také vynechat, ale v praxi se téměř vždy používá. UDP stejně jako TCP používá čísla portů a platí pro něj stejný seznam portů jako pro TCP.



Obr. 9: UDP hlavička [5]

## 5.3 TCP VS. UDP

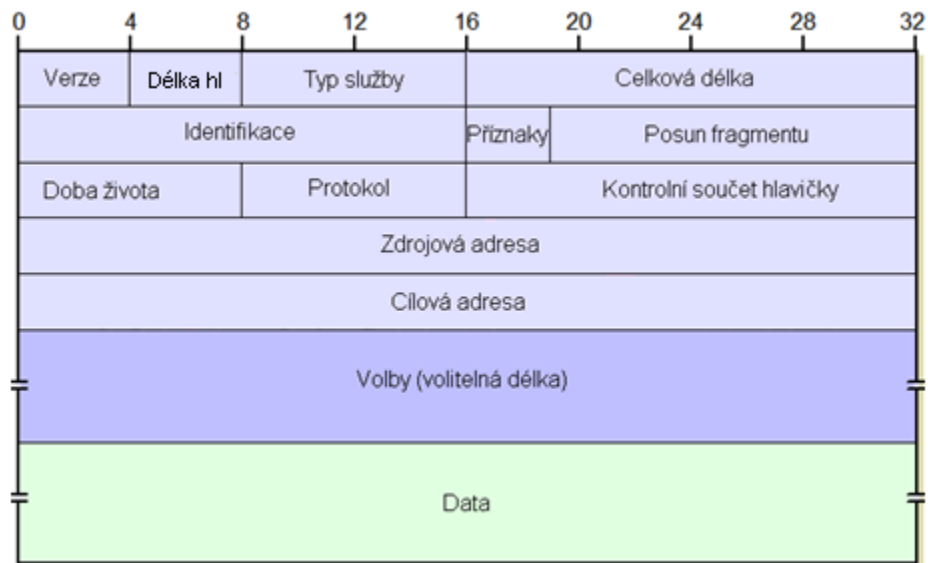
Oba tyto protokoly pracují na transportní vrstvě. TCP protokol garantuje spolehlivé doručování a doručování ve správném pořadí, také rozlišuje data pro

vícenásobné, současně běžící aplikace (například webový server a emailový server) běžící na stejném počítači. Protokol TCP využívá služby IP protokolu opakovaným odesíláním nespolehlivých paketů. Při ztrátě paketu zajišťuje spolehlivost přeuspořádáním přijatých paketů a tím zajišťuje jejich správné pořadí. Přesto je pro mnoho aplikací TCP nevhodné. Problém je nejen ve složitosti tohoto protokolu, ale také v tom, že při ztrátě paketu nemůže příjemce dostat paket následující, ale musí počkat na znovu zaslání a přijetí paketu ztraceného. To způsobuje problém v run-time aplikacích jako jsou internetová rádia, multiplayerové hry a VoIP (přenos digitalizovaného hlasu po síti). V těchto aplikacích je lepší dostávat data včas, než ve správném pořadí a kompletní, proto zde bude vhodnější dát přednost UDP protokolu před TCP.

Kvůli chybějící spolehlivosti se UDP aplikace musí smířit s nějakými ztrátami, chybami nebo duplikacemi. Pokud aplikace vyžaduje vysoký stupeň spolehlivosti, může se místo něj použít TCP. Ačkoliv celkové množství UDP v provozu na typické síti je jen v řádu několika procent, UDP používá řada klíčových služeb (např. DNS).

#### **5.4 INTERNET PROTOKOL (IP)**

Vykonává to, co je hlavním úkolem síťové vrstvy: dopravovat data až na místo jejich určení, a to i přes eventuelní mezilehlé ("přestupní") uzly, neboli přes tzv. směrovače. Aby to protokol IP dokázal, musí hledat vhodné směry (cesty) v soustavě vzájemně propojených směrovačů, vedoucí až k požadovanému cíli - neboli zajišťovat to, čemu se říká směrování (routing). K tomu protokol IP potřebuje vhodné informace o topologii celé sítě, na kterou se snaží dívat jako na soustavu dílčích sítí, vzájemně propojených právě prostřednictvím směrovačů.



Obr. 10: IP hlavička [5]

- **Verze** - verze IP protokolu
- **Délka hlavičky** - ve čtyřbytových slovech
- **Typ služby** - nese značku pro mechanismy zajišťující služby s definovanou kvalitou
- **Celková délka** - délka datagramu v bytech
- **Identifikace** - odesílatel přidělí každému odeslanému paketu jednoznačný identifikátor. Pokud byl datagram při přepravě fragmentován, pozná se podle této položky, které fragmenty patří k sobě (mají stejný identifikátor).
- **Příznaky** - slouží pro řízení fragmentace. Definovány jsou dva: *More fragments* ve významu „nejsem poslední, za mnou následuje další fragment původního datagramu“ a *Don't fragment* zakazující tento datagram fragmentovat.
- **Posun fragmentu** - udává, na jaké pozici v původním datagramu začíná tento fragment
- **Životnost (TTL)** – slouží jako ochrana proti zacyklení, každý směrovač odečte jedničku (případně odečte počet sekund, které datagram čeká na směrovači), jestliže tato hodnota klesne na nulu, je datagram zahozen
- **Protokol** – určuje, kterému protokolu vyšší vrstvy se mají data předat při doručení

- **Kontrolní součet hlavičky** – zjišťuje, zda nebyla data poškozena, součet se provádí pouze z hlavičky. Jestliže byla data poškozena, datagram bude zahozen
- **Adresa odesílatele** - IP adresa odesílatele
- **Cílová adresa** - IP adresa příjemce
- **Volby** - různé rozšiřující informace či požadavky. Například lze předepsat sérii adres, kterými má datagram projít.
- **Data** – po hlavičce následují samotná data

## 5.5 ARP

ARP (Address Resolution Protocol) je protokol, který přiřazuje k IP adrese fyzickou adresu (MAC adresu). Když se tak děje, mohou nastat dva stavy. Prvním takovýmto stavem je, že při komunikaci dvou zařízení spolu tato zařízení již komunikovala a MAC adresa příjemce je uložena v ARP cash paměti. Tato možnost se prověřuje jako první. V cash paměti se uchovávají tyto adresy po omezenou dobu. ARP cash paměť je implementována, aby snižovala počet dotazů na zjišťování MAC adresy.

Druhý stav je takový, že cash paměť cílovou MAC adresu neobsahuje, a je tedy potřeba ji zjistit. To se děje následovně:

1. V prvním kroku stanice odesílá **ARP Request**, zdrojovou adresou je vlastní MAC adresa a cílovou adresou je adresa broadcastu. Protože požadavek byl zaslán na broadcast, dojde k rozeslání tohoto požadavku do všech stanic v síti.
2. V druhém kroku se všechny stanice musí zabývat tímto požadavkem. Porovnají svoji IP adresu s IP adresou příjemce, kterou obdržely v požadavku na zjištění MAC adresy. Když stanice zjistí rovnost IP adres, pošle tzv. **ARP Response**, tedy odpověď se svojí MAC adresou. Ostatní stanice tento požadavek ignorují a nereagují na něj.
3. Další komunikace už probíhá pouze mezi těmito dvěma stanicemi, nikoli přes broadcast.

Reverzní ARP (RARP), zjišťuje IP adresu z MAC adresy. To bývá využíváno na bezdiskových stanicích, kde zařízení zná pouze svoji MAC adresu a potřebuje zjistit svou IP adresu. V síti kde jsou připojeny tyto bezdiskové stanice, musí být přítomný

RARP – server. V praxi se jinak tento protokol téměř nevyužívá a bývá nahrazen protokolem DHCP, který je komplexnější.

## 5.6 DHCP

Jedná se o další protokol z rodiny TCP/IP. Používá se pro automatické přidělení IP adresy pro zařízení v síti. V praxi bývá v síti připojen DHCP server, který umí zařízením pracujících s protokoly TCP/IP přiřadit síťové nastavení. Nejčastěji IP adresu, masku sítě, výchozí bránu a DNS server, ale i další. [8]

Po připojení do sítě, klient vyšle požadavek na UDP portu č. 68, server naslouchá na portu č. 67. Server pak nabídne klientovi několik možných IP adres a klient si jednu vybere a odešle ji DHCP serveru zpět. Od serveru pak obdrží potvrzení a od této chvíle může klient používat IP adresu a další síťové nastavení, které mu DHCP server přiřadí. Toto nastavení je DHCP serverem zapůjčeno pouze na omezenou dobu, před uplynutím této doby, musí klient odeslat požadavek o prodloužení platnosti IP adresy. Pokud se tak nestane, klient tuto adresu nesmí dále používat. [8]

Síťové nastavení může DHCP server nastavovat **staticky**, to znamená, že server obsahuje tabulku MAC adres a k nim odpovídající IP adresy. To zajistí, že klient dostane pokaždé stejnou IP adresu. Druhou možností je přidělení IP adresy **dynamicky**, kdy server vymezí rozsah adres, které může klient dostat. Časové omezení pronájmu IP adresy dovoluje DHCP serveru již nepoužívané adresy přidělovat jiným stanicím. Registrace dříve pronajatých IP adres umožňuje DHCP serveru při příštím pronájmu přidělit stejnou IP adresu. [8]

## 6. BEZDRÁTOVÉ SÍTĚ

Jak už napovídá název, jedná se o takové sítě, kde jednotliví členové sítě nejsou fyzicky propojeni, ale přenos dat je bezdrátový. Jejich výhodou je cena, která je nižší o cenu kabeláže. Absence kabelů, ať už napájecích nebo datových, je největší výhodou bezdrátových sítí. Zařízení proto mohou být umístěna i tam, kde nelze natáhnout kabely. Toto je využíváno především u snímačů, které je pak možné umístit prakticky kamkoli.

Nevýhodou bezdrátových sítí je možnost snadného rušení signálu. Signál ruší například elektromotory, rozvody vysokého napětí, ale třeba i tlusté zdi. Protože je dnes v provozu mnoho bezdrátových zařízení, může nám také vznikat problém s překrýváním frekvencí.

### 6.1 IEEE 802.15.4

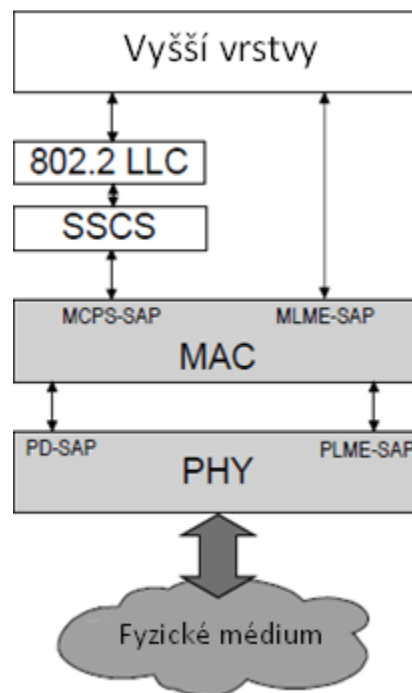
Informace o tomto standardu byly čerpány výhradně ze stránek IEEE, kde je uložen elektronický text, který je tomuto protokolu věnován. Text je kompletně v angličtině. V žádném případě se však nejedná o doslovný překlad tohoto více jak šesti set stránkového dokumentu, ale pouze o jakýsi výtah informací o které by měli objasnit základní fungování tohoto protokolu.

Standart IEEE 802.15.4 patří do osobních sítí (PAN), stejně jako například dobře známý bezdrátový standart Bluetooth, nebo ZigBee. Právě ZigBee má základy vystavěné právě na tomto protokolu. Zařízení pracující na úrovni protokolu IEEE 802.15.4 mohou pracovat v režimu nízkého odběru elektrické energie. Tyto zařízení jsou navržena tak, aby mohla na jednu baterii fungovat měsíce, nebo i roky. Existuje zde možnost přejít do úsporného režimu. V tomto stavu takovéto zařízení pouze naslouchá a tím se ještě více sníží energetické nároky na jeho provoz.

Přenosové rychlosti se pohybují maximálně ve stovkách kilobitů za sekundu. Jako maximální teoretická rychlost je udávána rychlost 250kb/s. Oproti Ethernetu se tedy jedná o velmi malé rychlosti přenosu dat.

### 6.1.1 Architektura

Zařízení pracující na protokolu IEEE 802.15.4 mají dvě vrstvy. A to vrstvu Fyzickou (PHY), která obsahuje transceiver a jeho kontrolní mechanismy. A podvrstvu MAC, která má za úkol zprostředkovávat přístup k fyzické vrstvě ostatním přenosům a zastupuje v této architektuře tedy linkovou vrstvu modelu ISO/OSI.



Obr. 11: Architektura zařízení WPAN[3]

Vyšší vrstvy zobrazené v obr. 15 poskytují manipulaci a směrování a také vrstvy aplikační. Definice těchto vrstev je ovšem mimo rozsah normy IEEE 802.15.4. Zařízení může být postaveno jako embedded zařízení, nebo jako zařízení vyžadující podporu externího zařízení, například PC.

## 6.2 FYZICKÁ VRSTVA IEEE 802.15.4

Fyzická vrstva je odpovědná za následující úkoly:

- aktivace a deaktivace transceiveru
- odesílání a přijímání dat

- výběr frekvence kanálu
- indikuje kvalitu pro příjem paketu
- zabraňuje kolizím (CSMA – CA)
- energetická detekce v rámci aktuálního kanálu

### 6.2.1 Frekvenční rozsahy

Výhodou protokolu je kromě jeho jednoduchosti také fakt, že IEEE 802.15.4 funguje v pásmu nelicencovaných frekvencí.

- 868 - 868,6 MHz (např. Evropa)
- 902 - 928 MHz (např. Severní Amerika)
- 2400 - 2483,5 MHz (celosvětově)

To může být ovšem také nevýhoda, protože v okolí, kde chceme používat bezdrátové zařízení na určité frekvenci, může už na této frekvenci vysílat někdo jiný. Pak je potřeba nelézt novou frekvenci, která je volná.

Používá také několik druhů kódování signálu, to má za následek různé přenosové rychlosti. Přesněji se používají tyto tři způsoby kódování:

- ASK – amplitude shift keying
- BPSK – binary phase-shift keying
- O-QPSK – offset quadrature phase-shift keying

Na frekvenci 2,4GHz se používá pouze kódování O-QPSK, které všeobecně umožňuje vyšší datový tok. Na frekvenci 2,4GHz to je 250kbps.

### 6.2.2 Rozdělení kanálů

Celkem 27 kanálů číslovaných od 0 do 26. V pásmu 2450MHz je k dispozici 16 kanálů, 10 kanálů v pásmu do 915MHz a jediný kanál v pásmu 868MHz.

Tyto kanály jsou definovány takto:

$$F_c = 868.3 \text{ MHz, pro } k = 0$$

$F_c = 906 + 2(k - 1)$  MHz, pro  $k = 1, 2, \dots, 10$

$F_c = 2405 + 5(k - 11)$  MHz, pro  $k = 11, 12, \dots, 26$

kde  $k$ , je číslo kanálu.

### 6.2.3 Rámec fyzické vrstvy

Protokol je navržen tak, že nejprve jsou předávána pole, která jsou nejvíce vlevo, pak se v předávání pokračuje dále doprava. Pokud pole obsahuje více oktětů, předává se nejprve nejméně významný oktět, z tohoto oktetu zase nejméně významný bit.

Každý rámec normy IEEE 802.15.4 se skládá z těchto komponent:

- Synchronizační hlavička (SHR)
- Hlavička fyzické vrstvy (PHR)
- Užitečný „náklad“ (PHY payload) – obsahuje rám podvrstvy MAC

		Oktetů		
		1		proměnné
Preamble	SFD	Délka rámu (7bitů)	Rezervováno (1bit)	PSDU
SHR		PHR		PHY payload

**Obr. 12: Rámec fyzické vrstvy [3]**

#### Preamble

Toto pole slouží pro synchronizaci a skládá se z 32 binárních nul.

#### SFD

Osmibitové pole označuje konec synchronizace a odděluje jej od začátku paketové části. Musí mít následující podobu: 11100101. Vlevo je nejméně významný bit, vpravo pak nejvíce významný bit.

### Frame length

Pole velké sedm bitů může nabývat hodnot od 0 do 127. Hodnoty od nuly do sedmi, kromě pětky, která označuje potvrzující paket, jsou rezervovány. Od hodnoty 8 výše, se jedná o velikost paketu v bytech.

### **6.3 PODVRSTVA MAC**

Obecný rám podvrstvy MAC musí být ve formátu, v jakém je zobrazen na obrázku č. 13. Obsahuje MAC hlavičku, užitečný „náklad“ a zápatí.

Oktetů: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/ 14	proměnlivé	2
Ovládání rámu	Číslo sekvence	Cílový PAN identifikátor	Cílová adresa	Zdrojový PAN identifikátor	Zdrojová adresa	Pomocná bezpečnostní hlavička	Užitečné zatížení rámu	FCS
		Adresové pole						
MHR							MAC Payload	MFR

**Obr. 13: Rámec podvrstvy MAC [3]**

Zápatí (na obrázku označeno jako MFR) obsahuje pouze kontrolní sekvenci. MAC Payload pak zase jen užitečná data. Nejzajímavější je tedy hlavička MAC, která obsahuje více polí různých velikostí, především pak adresační pole.

#### **6.3.1 Hlavička podvrstvy MAC (MHR)**

Skládá se ze sedmi polí, obsahuje adresační prostor, tedy oblast dat rámu, kde jsou uloženy zdrojové a cílové adresy, nejen zařízení, ale také sítě. Dále obsahuje velice důležité pole „Ovládání rámu“, které určuje vlastnosti rámu.

#### **Ovládání rámu**

Jedná se o důležité pole velké 16bitů. Těchto 16bitů nám řekne mnoho o typu rámce a jeho možnostech. Na toto pole je odkazováno i dále v tomto textu. Musí mít stejný formát, jako je zobrazen na obrázku č. 14.

Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Typ rámu	Možnost zabez.	Blížící se rám	Pož. odpověď	PAN ID komprimovaný	Rezerva	Cílový adresový mód	Verze rámu	Zdrojový adresový mód

Obr. 14: Formát pole Ovládání rámu [3]

### Typ rámu

Tříbitové pole, které určuje typ rámu (např.: 001 – Data, 101 – Potvrzení, 011 – příkaz MAC).

### Možnost zabezpečení

Toto jednobitové pole říká, zda je rám pod nějakou ochranou. Když obsahuje jedničku, musí být přítomná „Pomocná bezpečnostní hlavička“.

### Blížící se rám

Pole o velikosti jednoho bitu. Musí být nastaveno do jedné, když má odesílatel více dat pro příjemce. V opačném případě je nastaveno na nulu.

### Požadovat odpověď

Pole nastavuje odesílatel rámu tehdy, když má zájem o zaslání potvrzujícího rámu o přijetí. Pokud je nastaveno na nulu, příjemce dat potvrzení nikdy neodesílá.

### PAN ID komprimovaný

Jednobitové pole, které říká, jestli má MAC rámeček obsahovat PAN identifikátor, ze kterého byl odeslán. Pokud je pole nastaveno do jedné a rám obsahuje pouze cílovou adresu, předpokládá se, že rám přichází ze stejné sítě. Pokud rám obsahuje zdrojovou a cílovou adresu a toto pole obsahuje nulu, jsou vyžadovány identifikátory obou sítí, tedy zdrojové a cílové sítě.

### Cílový adresový mód

Dvoubitové pole, které musí mít jednu z hodnot zobrazených na obrázku č. 15. Pokud je toto pole rovno 0 a nejedná se o majákový rám, nebo o potvrzující rám, musí být pole „Zdrojový adresový mód“ nenulové. To znamená, že rám je zaměřen na koordinátora sítě uvedeného v poli „Zdrojový PAN identifikátor“.

### Verze rámu

Délka pole je dva bity. Když je nastaveno na 0x00 indikuje, že rám je kompatibilní s verzí IEEE 802.15.4 – 2003. Při nastavení 0x01 zase říká, že se jedná o verzi IEEE 802.15.4, tedy o verzi která prošla v roce 2006 aktualizací. Ostatní hodnoty jsou vyhrazeny pro budoucí použití.

### Zdrojový adresový mód

Dvoubitové pole, které musí mít jednu z hodnot zobrazených na obrázku č. 15. Pokud je pole nulové a nejedná se o majákový rám a ani o potvrzující rám, musí být pole „Cílový adresový mód“ nenulové. To znamená, že rám vznikl u koordinátora sítě uvedeného v poli „Cílový PAN identifikátor“.

Hodnota Adresových módů $b_1 b_0$	Popis
00	PAN identifikátor a adresové pole nejsou přítomna
01	Rezervováno
10	Adresové pole obsahuje 16 bitovou krátkou adresu.
11	Adresové pole obsahuje 64 bitovou rozšířenou adresu.

**Obr. 15: Hodnoty pole PAN ID komprimovaný [3]**

### **Číslo sekvence**

Zde je schováno číslo, které určuje pořadí rámu. Velikost tohoto pole je 8bitů.

### **Cílový PAN identifikátor**

Velikost je 16bitů a specifikuje unikátní osobní síť. Toto pole se vyplňuje pouze v případě, že „Cílový adresový mód“ v poli „Ovládání rámu“ má nenulovou hodnotu.

### **Cílová adresa**

Jedná se o pole s cílovou adresou. Jeho délka je proměnná a to buď 16, nebo 64bitů. Jak velké bude, určuje hodnota v kolonce „Cílový adresový mód“ ta je umístěná

v poli „Ovládání rámu“. Tato část rámu obsahuje tedy cílovou adresu. Pokud je v šestnáctibitové podobě vložena adresa 0xFFFF jedná se o adresu broadcastu.

### **Zdrojový PAN identifikátor**

Jeho velikost je 16bitů, jedinečně identifikuje osobní síť, odkud byl rám odeslán. Toto pole musí být zahrnuto do rámu MAC pouze v případě, že „Zdrojový adresový mód“ je nenulový a „PAN ID komprimovaný“ je roven nule. Obě tyto proměnné se nacházejí v poli „Ovládání rámu“.

### **Zdrojová adresa**

Velikost pole závisí na hodnotě uložené v poli „Ovládání rámu“ přesněji pak v dvoubitovém poli s názvem „Zdrojový adresový mód“, může být 16, nebo 64bitů. Toto pole určuje adresu, která je původcem rámu. Musí být zahrnuto v MAC rámu jen tehdy, je-li proměnná „Zdrojový adresový mód“ v poli „Ovládání rámu“ nenulová.

### **Pomocná bezpečnostní hlavička**

Pole s proměnou délkou, které má za úkol upřesnit informace pro požadované zabezpečení včetně toho, jak je rám skutečně chráněn. Je vkládáno pouze, pokud je „Možnost zabezpečení“ v poli „Ovládání rámu“ nastaveno na jedničku.

### **6.3.2 Zápatí MAC (MFR)**

Zápatí obsahuje pouze kontrolní sekvence (FCS). Pro výpočet se používá techniky CRC (Cyclic Redundancy Check).

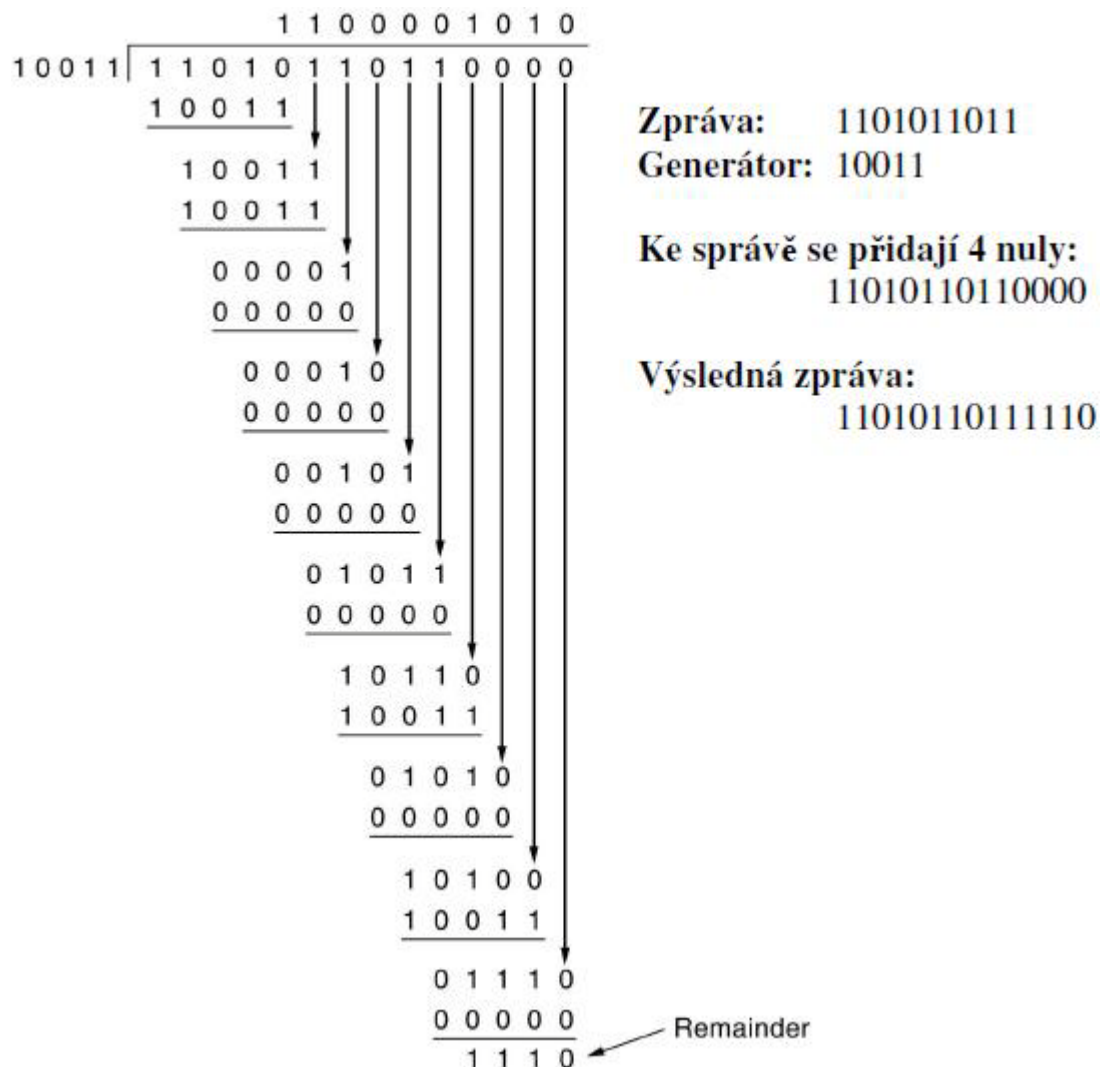
### **CRC**

CRC se používá pro detekci chyb. A to nejen při přenosu dat v síti, ale například i v ukládání dat na disk. Před odesláním dat je proveden odesílatelem výpočet CRC a výsledek je obsažen v posledních 16b bezdrátového rámu. Příjemce když přijme data, provede podle stejného algoritmu opět výpočet CRC a porovná ho s tím, který vypočítal odesílatel a připojil ho na konec rámu.

Existuje několik možných algoritmů pro výpočet CRC, který bývá nejčastěji 16bitový, nebo 32bitový. Ty se dále ještě liší ve tvaru polynomů, pomocí kterých je CRC počítáno. V protokolu IEEE 802.15.4 je kontrolní součet šestnáctibitový s následujícím polynomem:

$$C_{16}(x) = x^{16} + x^{12} + x^5 + 1$$

Takovýto CRC součet, se nazývá ITU-T, nebo také CCITT. V protokolu IEEE 802.15.4 je CRC počítáno z MAC hlavičky a samozřejmě, také ze samotných dat.



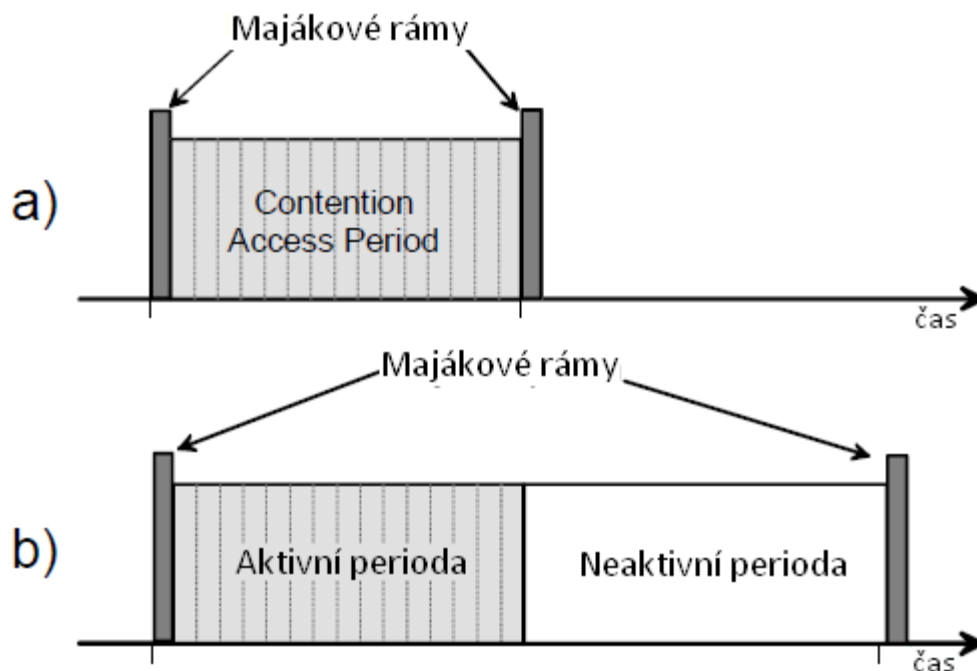
Obr. 16: Příklad výpočtu Remainderu [10]

Výpočet Cyclic Redundancy Check se provádí postupným dělením kontrolované zprávy generátorem a to pomocí xor algebry. Při výpočtu uvažujeme

dva případy, prvním je kontrola přijaté zprávy, kde se dělí přijatá zpráva s přijatým generátorem. Zbytek při je buď nulový – zpráva byla přijatá bez chyby nebo nenulový – to nám říká, že v průběhu přenosu došlo k narušení zprávy. Druhý případ je příprava zprávy před transportem v síti. V tomhle případě se počítá tzv.: reminder – zbytek při dělení zprávy a generátoru. Spolu se zprávou se pak musí poslat generátor, aby se mohl provést kontrolní výpočet. [10]

### 6.3.3 Struktura super-rámu

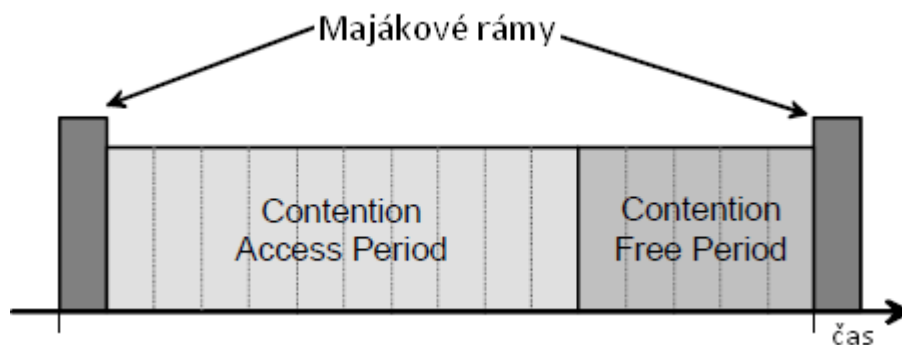
Tento standart podporuje volitelnou strukturu super-rámu. Takovýto super-rám je rozdělen na 16 stejně velkých bloků. V prvním bloku se odesílá tzv. maják, je to rámec, který slouží pro synchronizaci připojených zařízení. Volitelně může být tato struktura rozdělena na aktivní a neaktivní část. To ukazuje obrázek č. 17. V neaktivní části může zařízení přejít do stavu, kdy odebírá méně energie.



Obr. 17: Struktura super-rámu [3]

Z obrázku je patrné, že každý takovýto super-rám je ohraničen majákovými rámy na obrázku a) je vidět super-rám bez neaktivní periody. Obrázek b) nám ukazuje použití i neaktivní části.

Pro aplikace s nízkou odezvou, nebo aplikace vyžadující přesné informace o šířce pásma může koordinátor osobní sítě vyhradit úsek aktivní části v super-rámu pro tyto aplikace. Této části super-rámu se pak říká „garantovaný časový slot“ označovaný jako GTS (z anglického: „Guaranteed Time Slot“).



**Obr. 18: Struktura super-rámu s GTSs [3]**

Koordinátor osobní sítě může rozdělit až sedm těchto GTS a ty mohou zabírat více než jen jeden slot periody. V GTS na konci rámu se nachází sloty CFP (Contention Free Period) ihned po CAP (Contention Access Period), jak ukazuje obrázek č. 18.

### 6.3.4 Formát majákového rámu

Takový rámeček je velice podobný klasickému rámu, ale obsahuje některá rozšiřující pole oproti klasickému rámu. Formát takového rámu musí být stejný, jako je zobrazen na obrázku č. 19.

Oktetů: 2	1	4/10	0/5/6/10/14	2	proměnné	proměnné	proměnné	2
Ovládání rámu	Číslo sekvence	Adresové pole	Pomocná bezpečnostní hlavička	Specifikace superrámu	GTS pole (obr. 20)	Pole očekávaných adres (obr. 21)	Užitečná data	FCS
MHR				MAC užitečná data				MFR

**Obr. 19: Formát majákového rámu [3]**

V dalším textu budou objasněna jednotlivá pole. Některé pole Superrámu, byla v tomto textu zmiňována již dříve v kapitole 6.3.1, a proto nebudou dále zmiňovány.

### Specifikace superrámu

Pole o velikosti 16bitů musí mít formát zobrazený na obrázku č. 19.

Bitů: 0–3	4–7	8–11	12	13	14	15
Uspořádání majáku	Uspořádání superrámu	Konečný CAP slot	Prodloužení života baterie	Rezerva	PAN koordinátor	Povolení sdružení

**Obr. 20: Formát Superframe Specification field [3]**

#### **Uspořádání majáku**

Pole velké 4bity, které určuje interval mezi majákovými rámy.

#### **Uspořádání superrámu**

Pole velké 4bity, které určuje po jakou dobu je super-rám aktivní. A to včetně času kdy se přenáší majákový rám.

#### **Konečný CAP slot**

Další čtyřbitové pole, které určuje konečný slot využívající CAP.

#### **PAN koordinátor**

Jednabitové pole, musí být nastaveno na jedničku v případě, že majákový rám je předán koordinátorem. Jinak musí být nastaven na nulu.

#### **Povolení sdružení**

Další jednabitové pole. Musí být nastavené do jedné, pokud koordinátor akceptuje sdružení v PAN. Pokud koordinátor ve své síti toto sdružení neakceptuje, musí být pole nastaveno na nulu.

### GTS pole

Oktetů: 1	0/1	proměnné
Specifikace GTS	Směry GTS	GTS list

**Obr. 21: Formát GTS pole [3]**

### **Specifikace GTS**

Osmibitové pole, kde první tři bity určují „Počet GTS deskriptorů“, pokud je toto pole rovné nule nejsou přítomna pole „Specifikace GTS“ a „Směry GTS“. Čtvrtý až sedmý bit je rezervován. Posledním bitem tohoto pole, je bit s názvem „Povolení GTS“. Pokud je nastaveno do jedné, koordinátor sítě tak říká, že přijímá žádosti GTS.

### **Směry GTS**

Osmibitové pole, kde poslední bit je rezervován. Prvních sedm bitů obsahuje masku identifikaci pokynů GTS v super-rámu. Nejnižší bit v masce odpovídá směrování první GTS v „GTS list“. Zbytek je uveden v pořadí, v jakém jsou uvedeny v tomto seznamu.

### **GTS list**

Jedná se o 24 bitů velké pole. Prvních 16 bitů obsahuje adresu zařízení, pro kterou je GTS určeno. Další pole o velikosti čtyři, které určuje slot, na němž GTS začíná. Poslední, taktéž čtyřbitové pole, nám říká, po kolik slotů je GTS aktivní.

### **Pole očekávaných adres**

Toto pole má formát takový, jaký je uveden na obrázku č. 22. Obsahuje dvě pole, jedno osmibitové a jedno s proměnnou délkou.

Oktetů: 1	proměnné
Očekávané upřesnění adres	Seznam adres

**Obr. 22: Formát Pole očekávaných adres [3]**

### **Očekávané upřesnění adres**

V tomto osmibitovém poli jsou opět rezervovány bity. Jsou to bity číslo 3 a 7. Formát celého pole je zobrazen na obrázku č. 23.

**Počet očekávaných krátkých adres**

Udává počet 16ti bitových adres, obsažených v „Pole seznamu adres“  
v majákovém rámu.

**Počet očekávaných rozšířených adres**

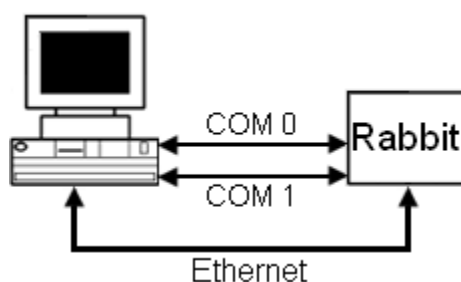
Udává počet 64ti bitových adres, obsažených v „Pole seznamu adres“  
v majákovém rámu.

Bitů: 0-2	3	4-6	7
Počet očekávaných krátkých adres	Rezervováno	Počet očekávaných rozšířených adres	Rezervováno

Obr. 23: Formát Pending address Specification [3]

## 7. NÁVRH PŘEVODNÍKU

Před návrhem samotného převodníku sestavíme podle zadání blokové schéma. V něm nemůže chybět osobní počítač a vývojový kit Rabbit. Modul je propojen s počítačem pomocí dvou sériových kabelů. První slouží pro obsluhu procesoru a druhý je určen pro simulaci bezdrátového rozhraní. Modul je dále s počítačem spojen přes Ethernet.



**Obr. 24: Blokové schéma**

Sériový port COM0 je použit jako programovací a můžeme říct, že slouží i pro sledování dění na převodníku. Port COM1 slouží k simulaci bezdrátové sítě. Po tomto kabelu „proudí“ do modulu rámy ve formátu IEEE 802.15.4. Převodník je převede na Ethernetové rámy a pošle je zpět do PC přes Ethernetové rozhraní. Data mohou proudit také v opačném směru. Tedy převodník přijme data z Ethernetu a odešle je zpět do PC přes sériovou linku, která simuluje bezdrátové rozhraní.

Pro přenos paketů po Ethernetu lze využít služeb protokolu TCP nebo UDP. Protože protokol IEEE 802.15.4 má předpoklady pro využití v průmyslu (např.: ZigBee). Lze předpokládat menší datovou náročnost aplikací, které na tomto protokolu budou pracovat. Vhodnější tedy bude dát přednost protokolu UDP, který je „rychlejší“ než protokol TCP a také jeho jednoduchost ho zvyhodňuje před protokolem TCP.

### **Rabbitcore RCM3365**

Ještě stručně o hardwaru, který byl použit při řešení úlohy. Jedná se o vývojový modul určený pro síťové aplikace. Tento modul může být doplněn také paměťovou

kartou až do velikosti 128MB. Protože se jedná o modul určený pro práci v síti, nechybí samozřejmě ani rozhraní pro Ethernet (RJ45).



**Obr. 25: Modul RCM3365 [2]**

Napájení zajišťuje síťový adaptér s výstupem stejnosměrného napětí o velikosti 12V a maximálním dodávaným proudem 1A. Tento zdroj dodává dostatečný výkon pro bezchybnou funkci převodníku.

**Tabulka 4: Vlastnosti modulu RCM3365**

Specifikace	
Microprocessor	Rabbit 3000 44.2MHz
Ethernet port	10/100Base-T, RJ-45
Flash	512K
SRAM	512K program + 512K data
Rozšířená paměť	32 MB NAND Flash ... max. 128 MB
Watchdog	Ano
Hodiny reálného času	Ano
Časovače	deset 8 - bitových(kaskádových) a jeden 10 - bitový s 2 registry
Napájení	3.15 - 3.45 V DC, 250 mA
Pracovní teplota	0°C až 70°C
Vlhkost	5 - 95%, bez kondenzace

### **Rabbit 3000 PROCESOR**

Modul RCM3365 je osazen právě tímto typem procesoru. Jedná se procesor, který je navržen speciálně pro komunikační a Ethernetová připojení. Maximální frekvence procesoru je 55,5MHz a napájení se pohybuje od 1.8V – 3,6V stejnosměrného napětí. Procesor má 20bitovou adresovou a 8bitovou datovou sběrnici.

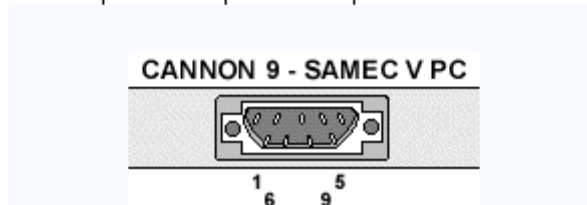


Obr. 26: Rabbit 3000 Processor [2]

Procesor má 1MB paměti pro kód a prostor dat. Může se pochlubit šesti sériovými porty a systémem „Watchdog“, který chrání procesor proti zacyklení.

Aby bylo možné simulovat bezdrátové rozhraní, je nutné připojit další sériový kabel. Tentokrát ne přímo na síťový modul, ale na základní desku. Tato deska je na rozdíl od síťového modulu vybavena převodníkem napěťových úrovní RS232/TTL. Deska nabízí dvě sériová rozhraní označená jako porty E a F.

Cannon 9			
PIN	NÁZEV	SMĚR	POPIS
1	CD	<--	Carrier Detect
2	RXD	<--	Receive Data
3	TXD	-->	Transmit Data
4	DTR	-->	Data Terminal Ready
5	GND	---	System Ground
6	DSR	<--	Data Set Ready
7	RTS	-->	Request to Send
8	CTS	<--	Clear to Send
9	RI	<--	Ring Indicator

Obr. 27: Popis pinů konektoru CANNON9 [4]

Na obrázku č. 27 je zapojení konektoru CANNON 9. Protože se jedná o tří vodičové zapojení sériové linky, stačí připojit pouze piny RXD, TXD a samozřejmě také zemnicí pin.

## 7.1 PŘIPOJENÍ PŘEVODNÍKU DO SÍTĚ

Protože každé zařízení připojené v síti musí být jednoznačně identifikovatelné, je nutné, aby i tento převodník měl své vlastní síťové nastavení. Pokud by se tak nestalo, nebylo by možné převodník adresovat a posílat mu tak jakákoliv data. Proto je v prvním kroku praktické realizace převodník připojen do sítě s PC a je mu přiděleno jeho síťové nastavení. Konkrétně se jedná o IP adresu, masku sítě a o výchozí bránu (hraniční router). Tyto hodnoty jsou pro začátek napevno nastaveny na následující hodnoty:

- IP adresa: 192.168.1.150
- Maska podsítě: 255.255.255.0
- Výchozí brána: 192.168.1.255

Hodnoty je možné měnit pomocí webového prohlížeče na příslušné IP adrese. Nejprve je ale nutné zprovoznit webový server na převodníku. Toho lze jednoduše dosáhnout voláním funkce `http_init()` na začátku funkce `main` a vyhrazením portu číslo 80. V dalším kroku jsou na převodník nahrány jednoduché webové stránky, které umožňují měnit síťové nastavení z internetového prohlížeče umístěného na osobním počítači. Zde pouze stačí převodníku označit, jaké typy souborů se budou nahrávat a kde jsou tyto soubory umístěny a kompilátor je sám vloží do převodníku při nahrávání programu.

### 7.1.1 Možnosti přidělení IP adresy

V prostředí Dynamic C se IP adresa dá přidělit několika způsoby. Jako nejvhodnější a nejuniverzálnější se jeví funkce „`ifconfig`“. Jedná se o funkci s velkým počtem volitelných parametrů, tyto parametry pak ovlivňují síťové nastavení. Další možností je použití příslušných předdefinovaných maker. V tomto případě ale vzniká problém, pokud bude chtít uživatel změnit síťové nastavení převodníku. I když Dynamic C nabízí funkci pro změnu makra IP adresy, dále už nenabízí funkce pro změnu maker masky sítě a výchozí brány.

## Manuálně

Uživatel si sám nastaví všechny síťové proměnné (IP adresa, masku sítě, výchozí brána) přes internetový prohlížeč nainstalovaný na PC. Při tomto nastavení má funkce „ifconfig“ následující parametry:

- IF\_ETH0, - říká že se jedná o rozhraní Ethernet
- IFS\_DOWN, - „shodí“ rozhraní
- IFS\_DHCP, NULL, - zakáže použití DHCP serveru
- IFS\_IPADDR, aton(myIP), - nastaví IP adresu, její hodnota je ukryta v „myIP“
- IFS\_NETMASK, aton(myNETMASK), - síťová maska uložena v „myNETMASK“
- IFS\_ROUTER\_SET, aton(myGATEWAY), - výchozí brána v „myGATEWAY“
- IFS\_UP, - „nahodí“ rozhraní

Samotné proměnné jsou ještě předány funkci aton(), která je vyžadována funkcí „ifconfig“ a která zajišťuje správný formát dat předávaných právě funkcí „ifconfig“.

## Automatické nastavení

Probíhá pomocí DHCP serveru, tento server má k dispozici omezený počet IP adres, které může přidělit. Tyto adresy jsou časově omezeny, a proto DHCP server může přidělovat již nepoužívané IP adresy. Parametry funkce „ifconfig“ jsou následující:

- IF\_ETH0,
- IFS\_DOWN,
- IFS\_DHCP, 1, - povolí pužití DHCP serveru pro síťové nastavení
- IFS\_DHCP\_FB\_IPADDR, aton("192.168.1.150"),
- IFS\_UP,


Jak je vidět, parametry jsou podobné jako u nastavení manuálního. Parametr IFS\_DHCP\_FB\_IPADDR nastaví IP adresu uvedenou v závorce v případě, že se to z nějakého důvodu nepodařilo DHCP serveru.

Nevýhodou této metody je fakt, že uživatel musí použít MAC adresu převodníku (je zobrazena na webu, který je spuštěn na převodníku) a s použitím příslušného programu zjistit, jakéže síťové nastavení to DHCP server převodníku vlastně přiřadil.

Pokud chce uživatel použít možnost automatického síťového nastavení, musí se ujistit, že je tento server v síti dostupný.

## 7.2 PŘENOS DAT VE SMĚRU ETHERNET – IEEE 802.15.4

Předtím než budou data posílána, musí být nějak vytvořena. K tomuto účelu je používán program „Colasoft Packet Builder 1.0“. S jeho pomocí je poměrně snadné vytvořit UDP pakety podobné tomu na obrázku č. 28.

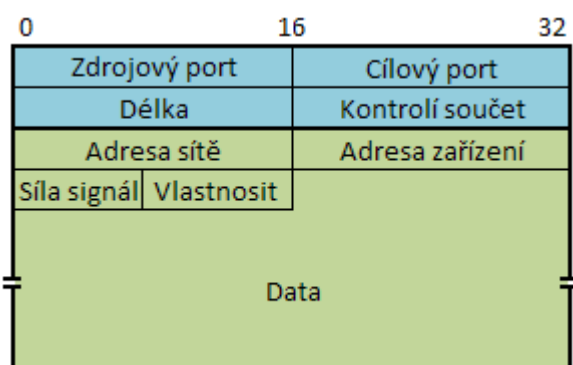


Field	Value	Length
<b>Packet Info:</b>		
Packet Number:	000001	
Packet Length:	64	
Capture Length:	60	
Delta Time	0.000000 Second	
<b>Ethernet II Header</b>		
Destination Address:	00:90:C2:D3:D2:F3	[0/6]
Source Address:	00:11:09:68:D6:A5	[6/6]
Protocol:	0x0800	[12/2]
<b>IP - Internet Protocol</b>		
Version:	4	[14/1] 0xF0
Header Length:	5	(20 Bytes) [14/1] 0x0F
Differentiated Services Field:	1111 0010	[15/1] 0xFF
Differentiated Services Codepoint:	1111 00..	[15/1] 0xFC
Transport Protocol will ignore the CE bit:	.... ..1.	(Availability) [15/1] 0x02
Congestion:	.... ..0	(No Congestion) [15/1] 0x01
Total Length:	34	(34 Bytes) [16/2]
Identification:	0x0003	(3) [18/2]
Fragment Flags:	000. ....	[20/1] 0xE0
Reserved:	0... ....	[20/1] 0x80
Fragment:	.0... ....	(May Fragment) [20/1] 0x40
More Fragment:	..0. ....	(Last Fragment) [20/1] 0x20
Fragment Offset:	0	[20/2] 0x1FFF
Time To Live:	243	[22/1]
Protocol:	17	(UDP) [23/1]
Checksum:	0x42EE	(Correct) [24/2]
Source IP:	192.168.1.1	[26/4]
Destination IP:	192.168.1.150	[30/4]
No IP Option		[34/0]
<b>UDP - User Datagram Protocol</b>		
Source port:	1234	[34/2]
Destination port:	1234	[36/2]
Length:	14	[38/2]
Checksum:	0x7246	(Correct) [40/2]
<b>Extra Data:</b>		
Number of Bytes:	18 bytes	[42/18]
<b>FCS - Frame Check Sequence:</b>		
FCS:	0xCCF1A8F	(Calculated)

**Obr. 28: Vytvořený rám**

Většina polí je volitelná, jen kontrolní součty jsou kalkulovány programem a nelze je ovlivnit.

Aby bylo možné takovýto rám převést na rám, který odpovídá standartu IEEE 802.15.4, je do něj nutné vložit některé informace o podobě bezdrátového rámu. Protože knihovny vývojového prostředí Dynamic C jsou dobře připraveny pro práci s Ethernetovými rámci a funkce samy zkontrolují kontrolní součet a vrací pouze užitečná data. Jako nejlepší volba se tedy jeví, vložit informace pro bezdrátový rám na začátek datové části UDP paketu. Je to vhodné především pro zpracování rámu na převodníku.



**Obr. 29: Upravený formát UDP**

Když přijde paket z PC na převodník, je datová část (na obrázku č. 29 bledě zelená barva) uložena do bufferu. Adresa sítě a adresa zařízení je vložena do bezdrátového paketu na místa odpovídající příslušným adresám. Síla signálu nemá další využití v reálné simulaci, ale v praxi by byla tato jednobytová hodnota předána vysílači. Pole „Vlastnosti“ obsahuje dva bity a zbytek je pouze doplněk do jednoho bytu. První bit určuje, zda mají být data vyslána do stejné sítě, v které je zapojený převodník a druhý bit říká, zda má odesílatel pro příjemce více dat. Podobu bezdrátového paketu nejvíce ovlivňuje právě pole „Vlastnosti“. Kombinací dvou bitů, nám vzniknou čtyři možnosti, které přehledně zobrazuje následující tabulka.

**Tabulka 5: Možné kombinace bitů a vlastnosti bezdrátového rámu**

Binárně	Hexadecimálně	Poznámka
0 0	0x00	Paket putuje do jiné sítě a odesílatel nemá více dat pro příjemce.
0 1	0x01	Paket putuje do jiné sítě a odesílatel má pro příjemce více dat.
1 0	0x02	Paket putuje do stejné sítě a odesílatel nemá více dat pro příjemce.
1 1	0x03	Paket putuje do stejné sítě a odesílatel má pro příjemce více dat.

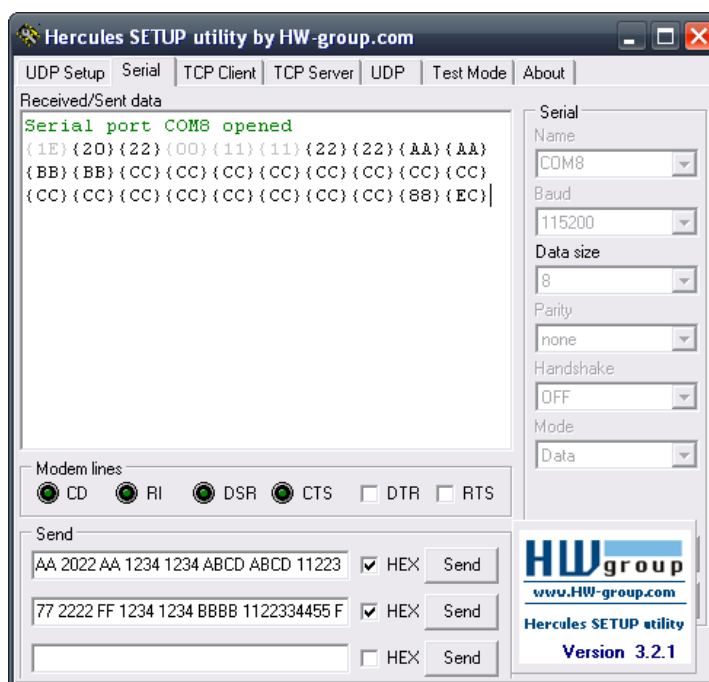


Když data doputují na převodník z Ethernetu, podle 6. bytu se rozhodne o vlastnostech bezdrátového rámu. Na obrázku č. 30 je vidět, že se tedy jedná o možnost nula, podle tabulky č. 5 jde o rám, který putuje do jiné sítě, než v které je zapojen převodník a odesílatel nemá pro příjemce více dat.

Z paketu je vyjmuta adresa cílové sítě a cílového zařízení spolu se silou signálu a celý paket je následně posunut o šest bytů a tak máme ve vstupním bufferu pouze užitečná data. Nyní může převodník sestavit hlavičku bezdrátového paketu a připojit i data, která mají být odeslána. Nakonec je spočítán ještě kontrolní součet, jehož výsledek je připojen na úplný konec paketu. Takovýto paket je následně odeslán po sériové lince, která má simulovat bezdrátový vysílač. Paket je pro kontrolu zobrazen v PC díky programu Hercules (obr. 31).

### 7.3 PŘENOS VE SMĚRU IEEE 802.15.4 – ETHERNET

Pro simulaci rámu přicházejících z bezdrátové sítě jsem opět použil program Hercules. Přichází i odchozí data jsou v programu zobrazována v hexadecimální podobě pro lepší přehlednost. Převodník umí zpracovat čtyři různé druhy přichozích paketů a to takové, které jsou popsány výše v kapitole 7.2.

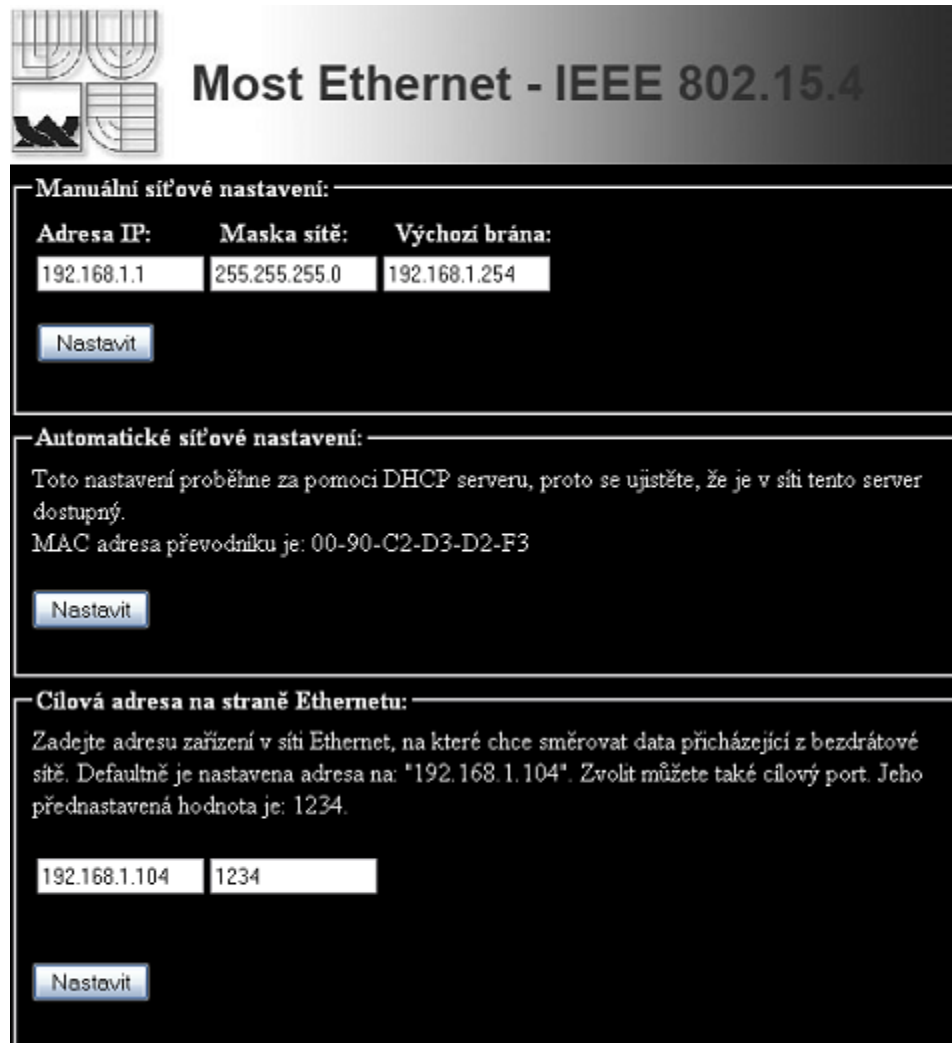


Obr. 31: program Hercules

Funkce převodu z bezdrátové strany na Ethernet je podobná jako v opačném směru. Z příchozího paketu je vyjmut kontrolní součet, který je v zápětí porovnán s kontrolním součtem vypočteným ze zbytku příchozích dat. Následně je podle druhého a třetího bytu v příchozím paketu rozhodnuto, o jaký typ příchozí rámu se jedná. Pokud převodník zná podobu příchozího rámu, je možné určit, kde jsou data a adresy odesílatele. Tyto informace jsou vloženy na začátek datové části UDP paketu, v pořadí jaké ukazuje obrázek č. 29.

Celý rám je pak odeslán na předem zvolenou adresu a předem zvolený port. Jak cílovou adresu, tak cílový port je možné změnit přes webový prohlížeč z PC.

Na obrázku č. 32 je vidět webové rozhraní spuštěné na převodníku. Lze z něj měnit síťové nastavení převodníku. Buď manuálně, nebo pomocí DHCP serveru. V neposlední řadě zde lze změnit adresu cílového zařízení a cílového portu.



**Most Ethernet - IEEE 802.15.4**

**Manuální síťové nastavení:**

Adresa IP:  Maska sítě:  Výchozí brána:

**Automatické síťové nastavení:**

Toto nastavení proběhne za pomoci DHCP serveru, proto se ujistěte, že je v síti tento server dostupný.  
MAC adresa převodníku je: 00-90-C2-D3-D2-F3

**Cílová adresa na straně Ethernetu:**

Zadejte adresu zařízení v síti Ethernet, na které chce směřovat data přicházející z bezdrátové sítě. Defaultně je nastavena adresa na: "192.168.1.104". Zvolit můžete také cílový port. Jeho přednastavená hodnota je: 1234.

Obr. 32: Webové rozhraní na převodníku

Stejně jako jsou kontrolována data přicházející z Ethernetu do „bezdrátové sítě“ pomocí programu Hercules, jsou kontrolována i data přicházející z převodníku po Ethernetu. Tuto službu zajišťuje program od firmy Microsoft s názvem Network Monitor 3.2.

## 8. ZÁVĚR

Na začátku práce jsou obsaženy informace nejen o obou protokolech, ale i o sítích všeobecně. Tyto informace nejsou příliš podrobné, ale měli by být dostačující pro pochopení fungování obou protokolů.

V další části textu je návrh převodníku. Nejprve bylo však potřeba připojit ho do sítě a přidělit mu IP adresu. Adresa převodníku je nastavena na 192.168.1.150. Záměrně je zvolena pozice někde uprostřed adresového rozsahu, protože na konci bývají například hraniční routery, DNS servery a jiná síťová zařízení. Na počátku pak mohou být již připojeny jiné síťové jednotky. Na převodníku je taktéž zprovozněn webový server, na který je možné se připojit pře internetový prohlížeč a změnit IP adresu dvěma způsoby. A to buď manuálně, nebo pomocí DHCP serveru. Bohužel při použití DHCP serveru jsem nenašel způsob jak uživateli sdělit jeho nové síťové nastavení a proto musí uživatel použít externí program pro zjištění své nové IP adresy. Na webovém serveru je zobrazena MAC adresa převodníku.

Převodník umí vytvořit a přijmout čtyři druhy rámu. Tyto rámy poznává podle kombinace bitů v poli „Ovládání rámu“ a podle toho zpracuje příchozí paket, respektive vytvoří paket odchozí. Převodník by mohl rozlišovat i více druhů rámu, například rámy, které přicházejí od koordinátora bezdrátové sítě, nebo naopak které mu jsou zasílány. Ale to by nepřineslo v návrhu převodníku nic nového, pouze delší zdrojový kód, a tak jsme se s vedoucím práce dohodli na tomto rozsahu. Převodník umí vypočítat a pracovat s CRC na straně „bezdrátové sítě“. Na straně Ethernetu je tato funkce automatická.

Aby bylo možné dokázat funkčnost převodníku, byly využity tři programy na straně PC. První dva sledují tok dat na Ethernetu (Microsoft Network Monitor) a na sériové lince (Hercules), třetí program pak slouží pro vytvoření a odeslání UDP paketu přes Ethernet (Colasoft Packet Builder 1.0).

## SEZNAM POUŽITÉ LITERATURY

- [1] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualiz. vyd. 2000. 435 s.
- [2] *Rabbit Semiconductor* [online]. c2009. Angličtina. [cit. 2010-05-01]. Dostupné z WWW: <<http://www.rabbit.com/>>.
- [3] *IEEE : Std 802.15.4*. [s.l.] : [s.n.], 2003. 679 s. Dostupný z WWW: <<http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf>>.
- [4] OLMER, Vít. *Hw.cz* [online]. c1997-2009. Angličtina.[cit. 2010-05-01]. Čeština. Dostupné z WWW: <<http://hw.cz/rs-232#konektory>>.
- [5] KOZIEROK, Charles M.. *The TCP/IP Guide* [online]. Version 3.0. c2001-2005 [cit. 2010-05-1]. Dostupné z WWW: <<http://www.TCPIPGuide.com>>.
- [6] *CC2520 DATASHEET : 2.4 GHZ IEEE 802.15.4/ZIGBEE® RF TRANSCEIVER* [online]. 2007 [cit. 2010-05-01]. Dostupné z WWW: <<http://www.datasheetarchive.com/pdf/Datasheet-064/DSA00204613.pdf>>.
- [7] *MC13192 Reference Manual : 2.4 GHz Low Power Transceiver for 802.15.4* [online]. 2004 [cit. 2010-05-01]. Dostupné z WWW: <<http://www.datasheetarchive.com/pdf-datasheets/Datasheets-12/DSA-220652.pdf>>.
- [8] DHCP. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 06.12.2006, last modified on 06.1.2006 [cit. 2010-05-20]. Dostupné z WWW: <<http://cs.wikipedia.org/wiki/DHCP>>.
- [9] ODVÁRKA, Petr. *Svět sítí* [online]. 19. 09. 2000 [cit. 2010-05-22]. Ethernet. Dostupné z WWW: <<http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=17>>.
- [10] MINÁŘ, Petr. *Interaktivní webové aplikace vytvořené pomocí technologie Adobe Flash : TEORIE KÓDOVÁNÍ* [online]. Brno, 2007. 42 s. Bakalářská práce. VUT Brno. Dostupné z WWW: <[http://autnt.fme.vutbr.cz/szz/2007/BP\\_Minar.pdf](http://autnt.fme.vutbr.cz/szz/2007/BP_Minar.pdf)>.

## SEZNAM POUŽITÝCH ZKRATEK

ISO	International Organization for Standardization	Mezinárodní organizace pro normalizace
OSI	Open Systems Interconnection,	Otevřený systém propojení
PAN	Personal area network	Osobní síť
LAN	Local area network	Místní síť
MAN	Metropolitan Area Network	Metropolitní síť
WAN	World Area Network	Celosvětová síť
IP	Internet Protocol	Internetový protokol
TCP	Transmission Control Protocol	Přenosový ovládací protokol
UDP	User Datagram Protocol	Uživatelský datagram protokol
ICMP	Internet Control Message Protocol	Internetový zprávy ovládající protokol
MAC	Media Access Control	Řízení přístupu média
ARP	Address Resolution Protocol	Protokol pro zjištění IP adresy
B/s	Byts per second	Bajty za sekundu
b/s	Bits per second	Bity za sekundu
IEEE	Institute of Electrical and Electronics Engineers	Institut pro elektroniku a elektronické inženýrství
ASK	Amplitude shift keying	Amplitudově posunuté klíčování
BPSK	Binary phase-shift keying	Binární fázově posunuté klíčování
O-QPSK	Offset quadrature phase-shift keying	Offsetové kvadratické fázově posunuté klíčování
GTS	Guaranteed Time Slot	Garantovaný časový slot
SHR	Synchronization header	Synchronizační hlavička
PHY	Physical layer	Fyzická vrstva
PHR	Physical header	Fyzická hlavička
MFR	MAC footer	MAC zápatí
MHR	MAC Control header	MAC řídicí hlavička
TX	Transnit data	Odeslaná data
RX	Receive data	Doručená data