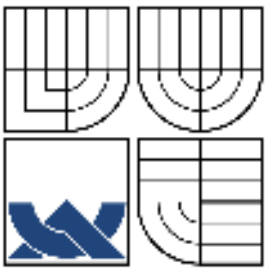
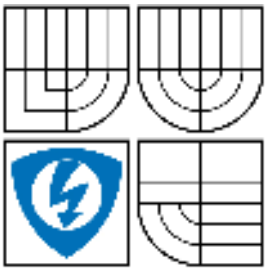


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMUNICATIONS

KOMUNIKAČNÍ PROTOKOL PRO VESTAVNÁ ZAŘÍZENÍ

Communication protocol for built-in facilities

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — Petr Dolák
AUTHOR

VEDOUCÍ PRÁCE — Ing. Ivo Herman, CSc.
SUPERVISOR

BRNO 2008

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení:
Bytem:
Narozen/a (datum a místo):
(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií
se sídlem Údolní 244/53, 602 00, Brno
jejímž jménem jedná na základě písemného pověření děkanem fakulty:
.....
(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
□ disertační práce
□ diplomová práce
□ bakalářská práce
□ jiná práce, jejíž druh je specifikován jako .....
(dále jen VŠKP nebo dílo)

Název VŠKP: .....

Vedoucí/ školitel VŠKP: .....

Ústav: .....

Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v*:

□ tištěné formě – počet exemplářů ……..
□ elektronické formě – počet exemplářů ……..

Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
Dílo je chráněno jako dílo dle autorského zákona v platném znění.
Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2

* hodící se zaškrtněte

Udělení licenčního oprávnění

Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
□ ihned po uzavření této smlouvy
□ 1 rok po uzavření této smlouvy
□ 3 roky po uzavření této smlouvy
□ 5 let po uzavření této smlouvy
□ 10 let po uzavření této smlouvy
(z důvodu utajení v něm obsažených informací)
Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: …….

……..	……
Nabyvatel	Autor

Prohlášení
Prohlašuji, že jsem bakalářskou práci na téma Komunikační protokoly pro vestavná zařízení vypracoval samostatně pod vedením vedoucího bakalářské práce. S použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citované v práci a uvedené v seznamu literatury na konci práce.

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

V Brně dne ……. ….…….podpis autora

Poděkování

Tímto bych chtěl poděkovat vedoucímu semestrální práce Ing. Ivu Hermanovi, CSc., za velmi užitečnou metodickou pomoc, cenné rady a návody při zpracování bakalářské práce.

Abstrakt

Problematika komunikačních technologií je v dnešním světě velmi závažnou otázkou, a proto se následující práce zaměřuje právě na tuto sféru informatiky. Konkrétně je práce zaměřena na komunikační protokoly, které jsou jedním ze základních stavebních kamenů jakéhokoliv přenosu dat, neboť vytváří elementární podmínky pro jakýkoliv datový tok, jelikož komunikační protokoly jsou pravidly pro správný datový transfer mezi účastníky.

V první části této práce jsou blíže probrána stávající řešení, bohužel však rozsah bakalářské práce neumožňuje podrobný rozbor všech, již používaných řešení, a proto se tato práce zaměřuje pouze na řešení, která jsou užívána na třech nejnižších vrstvách OSI modelu, jelikož zadání této práce jasně říká, že je nutno se zaměřit právě na trojvrstvá řešení komunikace, což vede ke dvěma výsledkům.

V druhé a třetí části této práce jsou právě tyto dva výsledky řešeny návrhem dvou vlastních komunikačních protokolů, přičemž první z nich vychází z podstaty tří nižších vrstev OSI modelu a je zaměřen zejména na bezchybný přenos dat a práci s nimi. Tím se myslí jejich ukládání do paměti vestavného zařízení, následné četní a další služby zahrnující práci s daty. Protokol vyšších vrstev také zabezpečuje kvalitní komunikační služby, nicméně se více zaměřuje na služby realizované zařízeními pracujícími s těmito protokoly.

V poslední části tohoto materiálu jsou přiloženy vývojové diagramy a simulace realizované v jazyku SDL.

Abstract

Questions connected with communication technologies are really serious problem worldwide and this Bachelor's thesis deals with this topic. Concretely is aim of this thesis Communication protocols. They are one of the basic keys in any data transfer, because they creates the basic environment for communication between users.

First part of this thesis specifies nowadays used communication technologies, however range of Bachelor's thesis do not give enough space for discussion all used technologies. The main aim of this part is to discuss used technologies on first three levels OSI model. It has been given to made a three layer solution and it has two possible results.

In the second and third part has been this two results discussed, by realizing two different communication protocols. The first one deals with three lower levels of OSI model, and it is connected to non-error transfer and working with data. It means uploading and downloading data. Protocol build on higher levels of OSI model deals with good communication, however is more specified for services used by in-built units.

The last part of this thesis includes diagrams and simulations performed in SDL language.

Obsah

Seznam použitých zkratek

A-vstup do kruhu příjezdů
AAM-signalizace příchodu
ADCCP- Advanced Data Communication Control Procedure
AK-potvrzení
ANSI- American National Standard Institute
BSC- bojary synchronous communication
CC-potvrzení spojení
CR-žádost o spojení
CRC-cyclic redundancy check
CSMA/CD-carrier sense with multiple access and collision detection
DC-potvrzení rozpojení
DGPS-diferenční GPS, jedná se o síť stanic zpřesňující polohu
DLE-1.znak konce rámce
DR-žádost o rozpojení
DSLC- Data Link Control
DT-data
EA-zrychlené potvrzení
ED-zrychlená data
ER-chyba
EXT-2.znak konce rámce
FCS-frame sequence check
FTP-file transfer protocol
GP-identifikace volajícího
GPRS-general packet radio service
GPS-celosvětový systém pro zjišťování polohy
HDLC-high level data link control procedure
ID DGPS-identifikační číslo stanice z DGPS
IPX-internet packet exchange
KZ-koncové zařízení
LAN-místní síť
MAC-media access control
MAN-metropolitní síť
NACK-záporné potvrzení
NDIS-network driver interface specification
NIC-network interface cards
NM-námořní míle
NMEA-národní asociace námořní elektroniky
OSI-open system interconnection reference model
PACK-kladné potvrzení
PDOP-rozptyl v udávání přesnosti polohy
RJ-odmítnutí
SDLC- Synchronous Data Link Control Procedure
SNMP-simple network management protocol
SPX-sequenced packet exchange
SYN-počáteční znak rámce
TCP-transmission control protocol
UDP-user datagram protocol
WPTNME-jméno cílového bodu

ÚVOD

Komunikační protokoly

Jsou to v podstatě specifikace, které definují postupy a parametry, které se používají při vysílání a příjmu dat, např. definice formátů dat, chybové kontroly atd.

Formát dat – veškeré prvky sítě mezi sebou komunikují pomocí speciálního druhu zpráv, jejichž obsah může být velmi různorodý. Od datových souborů až po řídící informace. Tyto zprávy jsou po kratších úsecích a jsou předem rozděleny počítačem do přesně stanovené délky. Dlouhé zprávy bývají rozděleny a kratší zprávy bývají do minimálních délek doplněny. Této činnosti se říká PADDING. Jednotlivé úseky zpráv nazýváme pakety (packet). Packet, který ve své hlavičce obsahuje informace o zdroji a cíli je před odesláním doplněn o informace typu: cílová a zdrojová adresa, posloupnosti a kontrolní součet správnosti dat. Takto doplněným paketům říkáme rámce (frame.). Po dosažení cílové stanice jsou pakety převedeny do původní podoby – souboru.

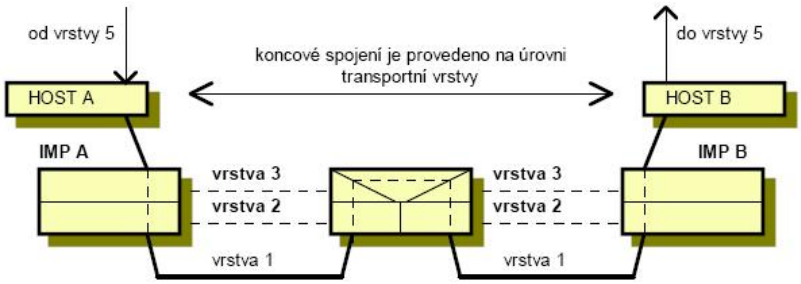
Dle OSI modelu se na různých vrstvách používají různé protokoly, proto bych se chtěl dále ve své práci zaměřit pouze na první tři vrstvy. A navrhovaný protokol aplikovat tak, aby respektoval třívrstvý model.

1. Fyzická vrstva

Je první vrstvou síťové architektury (OSI modelu). V originále se nazývá physical layer. Podporuje fyzickou komunikaci. Aktivuje a udržuje spojení (např. komutované spoje). Toto spojení může být dvojího druhu – 1. dvoubodové (sériová linka) 2. mnohobodové(Ethernet). Poskytuje spíše prostředky pro přenos bitů než pro přenos celých dat přes síťové uzly. Fyzická vrstva poskytne elektrické a mechanické vlastnosti přenosovému mediu.

2. Linková vrstva (spojová)

Jedná se o druhou vrstvu OSI modelu. V originále nese označení Data Link Layer. A poskytuje spojení mezi dvěma sousedními systémy (switch – PC). Seřazuje také přenášené rámce, stará se o nastavení parametrů přenosu linky a oznamuje též neopravitelné chyby. Formátuje fyzické rámce, opatřuje je fyzickou adresou (MAC adresou). O přenos fyzických rámců na konkrétní médium se stará LLC (Logical Link Control)



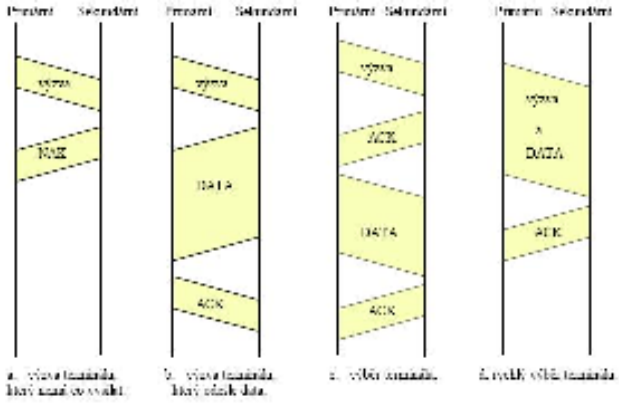
Obrázek 2.48: Umístění spojové vrstvy v OSI systému

2.1. Efektivní komunikace

Rámcová synchronizace – data jsou vysílána v blocích nazývaných rámce. Začátek a konec takovéhoto rámce musí být snadno identifikovatelný
Snadné řízení toku dat – vysílací stanice nesmí vysílat data rychleji než je přijímací stanice schopna přijímat
Kontrola chyb – chyby vzniklé v přenosovém řetězci musí být detekovány a opraveny
Adresování – má význam na mnohabodovém spoji, kdy musí být identifikována cílová stanice
Multiplexovaný provoz dat a řídících signálů – neboť dva druhy dat procházejí stejnou linkou. Přijímač musí umět rozlišit, která data jsou řídící a která uživatelská
Řízení spoje – tj. sestavení, udržování v chodu a ukončení spojení mezi stanicemi

2.2 Pracovní režimy

Režim výzva (polling) – používá se k přenosu dat z podřízených stanic do řídicí. Tato stanice vyzývá jednotlivé stanice, které odpoví odesláním dat, případně hlášením, že žádná data k odeslání nemají. Pořadí vyzívání podřízených stanice určuje hlavní stanice. Může být cyklické, založené na prioritě podřízených stanic apod.
Režim výběr - se používá pro přenos dat z řídicí stanice do podřízených. Řídicí stanice vybírá podřízené stanice, kterým po ohlášení jejich připravenosti posílá zprávy.



Obrázek 2.50: Příklad režimů výzva a výběr

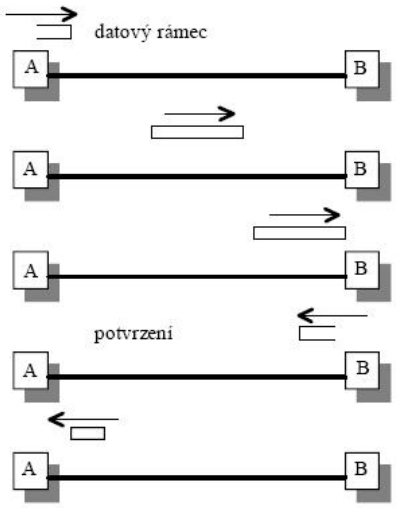
Režimy výzva a výběr se střídají. Většinou se zahajuje výzvou, po převzetí dat z podřízené stanice se jí předají data. Konverzace může být zrychlená, kdy přenos dat probíhá v obou směrech střídavě (s výjimkou záporného potvrzení)

Režim konkurence – kdy je podřízené stanici umožněno, aby z vlastní iniciativy požádala o přenos dat. Taková stanice je pak z cyklu výzev vyjmuta, čili nezdržuje konverzaci s ostatními podřízenými stanicemi.

Na této vrstvě se vyskytují následující protokoly:

2.3. Stop-and-wait

Tento protokol je nejjednodušší protokol. Zdrojová entita vyšle rámec. Cílová jej přijme a odešle kladné potvrzení o jeho příjmu. Na toto čeká vysílací stanice. Teprve po přijetí tohoto potvrzení může vysílací stanice opět vysílat. Pro tento režim jsou nejčastěji velké rámce segmentovány do menších z důvodu možnosti:
napadení chybou, neboť menší blok má menší pravděpodobnost napadení
na mnohabodových spojích by velký rámec dlouho zatěžoval společnou linku
velikost přijímací vyrovnávací paměti je omezena

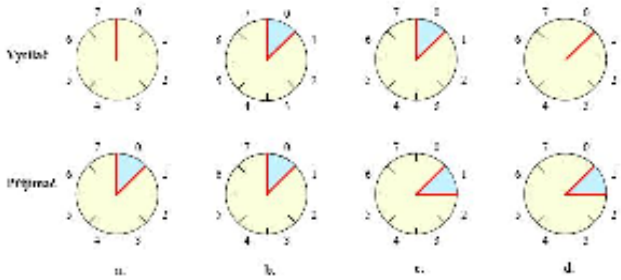


Obrázek 2.51: Účinnost protokolu STOP_AND_WAIT.

Pro použití protokolu STOP-AND-WAIT je nutno vzít v úvahu, že právě jeden paket může být v jednom čase na vedení. Proto jako velmi důležité parametry vystupují časy od vyslání rámce do jeho převzetí. Jedná se o:
přenosovou rychlost použitou na vedení
rychlost zpracování odezvy na koncovém zařízení
rychlost šíření přenášené zprávy

2.4. Protokol posuvného okénka

Tento protokol obsahuje každý rámec posloupnost čísel v rozsahu od 0 do maxima (obvykle 8 nebo 128), které určuje číslo vyslaného rámce (okénko vysílače) a číslo přijímaného rámce (okénko přijímače)
Číslo uvnitř okénka vysílače představuje číslo vysílaného a dosud nepotvrzeného rámce. Okénko je rozdíl mezi množstvím vyslaných a potvrzených rámců. Proto, přijde-li nový rámec, zvětší se okénko nepotvrzených rámců o jedna.Přijde-li potvrzení o přijetí rámce okénko se o jedna sníží. Vysílač si musí zapamatovat všechny vadné rámce, aby je mohl později opakovat (v případě nutnosti).


a. výchozí stav.
b. stav po vyslání prvního rámce.
c. stav po přijetí prvního rámce.
d. stav po potvrzení prvního rámce.

Obrázek 2.53: Protokol posuvného okénka o velikosti 1.

2.5. Techniky detekce chyb

Jsou-li data přenášena, existují tři třídy pravděpodobnosti, které mohou být definovány na straně přijímače:
1. třída rámec přijde bez chyb (běžná tel. Linka 10^{-4})
2. třída rámec přijde s jednou nebo více nedetekovanými chybami (resudial error rate)
3. třída rámec přijde s jednou nebo více detekovanými chybami, přičemž nedetekované neexistují

2.5.1. Základní techniky

paritní bit
Jedná se o nejjednodušší zabezpečovací schéma.
Používá se tzv.
-příčná parita – kdy se přidá ke každému slovu 1 bit v závislosti na tom, zda přenášený znak má lichý nebo sudý počet 1
podélná parita – kdy jsou sčítány operací modulo 2 po sobě jdoucí bity
křížová parita – která počítá současně podélnou i příčnou paritu
Zabezpečení paritou nevykazuje přílišnou spolehlivost, neboť se může s velkou pravděpodobností stát, že výsledek bude odpovídat paritnímu bitu

kontrolní součet
Provádí se obvykle jako podélný součet vysílaného rámce. Zabezpečení rámce je vyšší než i použití parity. Lze použít pro jednoduché případy.
cyklické zabezpečení
Jedná se o velmi výkonnou techniku pro zabezpečení dat používajících cyklického zabezpečení dat. (Cyclic Redundancy Check - CRC). Tato technika doplní každý přenášený rámec o zbytek po dělení polynomem. (Frame Check Sequence - FCS), přičemž zabezpečován je celý rámec včetně znaku na začátku rámce.
Úspěšnost detekce závisí na délce přenášeného rámce
- 100% detekce chyb sudých rámců
- 100% detekce chyb do 16 bitové délky
- 99,997% detekce chyb do 17 bitové délky
- 99,998% detekce chyb 18 bitové délky a delší

Existují nejen detekční, ale i cyklické kódy, které umí chyby opravit. Vyžadují však asi 50% nadbytečnost, čímž výrazně snižují průchodnost dat linkou a tím narůstá pravděpodobnost chyby.

2.6.Vývoj protokolů Linkové vrstvy

Protokoly lze rozčlenit do 3. generací. První generaci tvoří jednoúčelové bitové protokoly vytvářené v době, kdy normalizační činnost v oblasti přenosu dat nepřesáhla fyzickou úroveň. Společnou vlastností těchto protokolů je nemožnost spolupráce zařízení různých typů i stejného výrobce. První systémy přenosu dat byly realizovány většinou pomocí dvoubodových okruhů, pracovaly v nezpraženém režimu (off-line). Přenos se uskutečňoval většinou pouze mezi dvěma terminály (KZ), většinou pouze v jednom směru (sběr dat), kdy před přenosem a po něm se používala pomocná média, zejména děrná páska. Funkce potřebné k zajištění přenosu byly realizovány technickými prostředky. Za takovýchto podmínek nebylo podstatné, jakým způsobem spolu jednotlivé dvojice terminálů komunikují. Tento způsob přenosu byl vhodný pro dálkové dávkové zpracování dat.

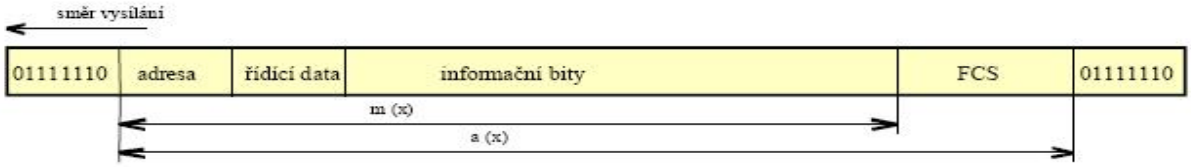
Se vznikem konverzačních systémů obsahujících velké množství terminálů je spojeno se zaváděním nových protokolů, které jsou vhodné pro konverzační režim, a které je možné standardizovat. Jsou to protokoly druhé generace, založené na použití řídicích znaků, mezinárodně normalizovaných abeced – zejména ISO (CCITT 5). Proto se jim říká znakové protokoly.
Třetí generací linkových protokolů jsou moderní bitové protokoly využívající výhod obou minulých generací, čímž je dovršen vývoj.

2.6.1. Znakový protokol ISO (BSC)

Znakový protokol BSC (bojary synchronous communication) byl vypracován firmou IBM a dále převzat v rámci ANSI (American National Standard Institute) pod názvem DSLC (Data Link Control) v roce 1968. V současné době se používají původní protokoly BSC a ISO, oba v různých variantách. Jsou založeny na speciálním použití řídicích znaků. ISO je založen na abecedě ISO 7, protokol BSC a USASCII a EBCDUC. Řídicí znaky jsou však definovány v šestibitových abecedách, případně je lze nahradit určitými kombinacemi znaků pětibitových abeced. Protokol ISO je určený pro poloduplexní znakový přenos dat mezi jednou řídicí a jednou nebo více podřízenými stanicemi. Přenos může být synchronní nebo asynchronní. Sériový nebo paralelní.

2.6.2. Protokol HDLC

Prvopočátkem tohoto protokolu byl SDLC (Synchronous Data Link Control Procedure), který byl později rozpracován v rámci ANSI skupinou X3S34. Ta připravila v roce 1971 americkou normu protokolu pod označením ADCCP (Advanced Data Communication Control Procedure). V rámci ICO je protokol označován zkratkou HDLC (High Level Data Link Control Procedure).
Tento rámec je určený pro duplexní nebo poloduplexní sériový provoz na okruzích libovolné technologie, které však musí být synchronní. Při použití HDLC se veškeré údaje přenáší v rámcích jednotného formátu.



Obrázek 2.64: Formát rámce HDLC.

HDLC definuje dva stavy kanálu:
Klidový stav - (Idle Link State) je charakterizován trvalým stavem 1. Je rozpoznán po příjmu minimálně 15 jedniček za sebou. Sled zrušení rámce proto můžeme mít délku 7 až 14 jedniček.
Aktivní stav – je přenos rámce, sledu zrušení rámce nebo mezirámcové výplně

Typy rámců HDLC
Informační – obsahují dvě čísla (proto dvojí/nezávislé číslování). Vysílací číslo rámce N(S) je číslo právě vysílaného rámce.. V HDLC protokolu je definován tzv. modul (8 pro základní, 128 pro rozšířený formát). Rámce jsou číslovány
0,1,2, …, MODUL. V určitém okamžiku může být odvysíláno a nepotvrzeno až MODUL – 1 rámců.

Dohlížecí – slouží k řízení přenosu. Všechny mohou potvrzovat informační rámce číslem N(R) a využít bity Poll/Final. Jsou definovány 4 dohlížecí rámce.

Nečíslované – slouží k pomocným funkcím, zejména k zahájení a ukončení přenosu, nastavení linky do provozního stavu, řešení výjimečných situací apod.. Jsou definovány rámce typu příkaz (dohromady 12) a rámce typu odpověď (celkem 7), zbylé kombinace do 32 tvoří rezervu do 32 nebo je lze použít pro další funkce.

Konfigurace okruhu a typu stanic
Pro protokol HDLC bylo definováno několik režimů. Jedná se o:

Nevyváženou (unbalanced) konfigurací
Naznačenou na obrázku. Jedná se o původní definici protokolu HDLC. Je definována jedna řídicí (Primary) a jedna nebo více podřízených (Secondary) stanic. Okruh tedy může být dvoubodový nebo mnohobodový. Rámce vysílané z P stanice se nazývají příkazy, rámce z S stanic odpovědi. Adresa v tomto případě vždy značí adresu S stanice.

Symetrická konfigurace
se používá na dvoubodových okruzích, na nichž komunikují rovnocenné stanice. Protokol HDLC se tímto požadavkem vypořádal s konfigurací naznačenou na obrázku. Symetrie bylo dosaženo dvěma dvojicemi P,S stanic.

Vyvážená (balanced) konfigurace
Je na obrázku. Stanice se nazývají kombinované, obě mohou současně vysílat i přijímat příkazy i odpovědi. Rozlišení je opět dáno adresami. Příkaz obsahuje protější adresu, odpověď místní adresu. Data jsou přenášena jako příkazy v režimu výběr. Režim výzva se používá k vyžádání potvrzení nebo ohlášení o stavu protější stanice.

2.6.3. ODI
Open Data-link Interface je celý název tohoto softwarového vybavení, které umožňuje různým protokolům na různých vrstvách sdílet tentýž ovladač nebo adaptér v počítači. ODI bylo poprvé užito Novellem a ku příkladu, při použití ODI, mohou TCP/IP a IPX/SPX sdílet jeden a tentýž adaptér.

2.6.4. NDIS

Network Driver Interface Specification je programovatelné rozhraní pro síťové karty. Bylo vyvinuto firmami Microsoft a 3Com Corporation a k dnešnímu dni je převážně využíváno operačním systémem Windows. Avšak nejrůznějšími projekty se docílilo toho, aby tato varianta byla aplikovatelná i na Linux.

NDIS je logický kontrolér linky, který tvoří podvrstvu pro linkovou vrstvu OSI modelu a funguje nebo chová se jako rozhraní mezi vrstvami 2 a 3 (Síťová vrstva). Nižší podvrstva je Media Access Control (MAC).

NDIS je knihovna funkcí, která bývá často označována jako „balič“, což skrývá komplexnost NIC(Network interface cards = síťové karty).

2.6.5. MAC

Media Access Control tento datový komunikační protokol je též známý jako Medium Access Control, je částí linkové vrstvy. Zajišťuje adresování a přístup kontrolním mechanizmům přístup na kanál, což umožňuje několika terminálům komunikovat uvnitř mnohobodové sítě, obvykle LAN(local area network = místní síť) nebo MAN(metropolitan area network = metropolitní síť). MAC protokol je nutný pro plný duplex směrového(point-to-point) spojení.

MAC též funguje jako podvrstva mezi Logickou linkovou podvrstvou a síťovou fyzickou vrstvou. MAC také zabezpečuje adresovací mechanizmus, který se nazývá fyzická nebo MAC adresa. Toto je unikátní sériové číslo, které je přiřazeno patřičnému síťovému adaptéru, což ho zeschopňuje k přenosu datových paketů uvnitř podsítě.

MAC se velmi často používá jako synonymum pro několika násobný přístupový protokol, MAC podvrstva též zabezpečuje protokol a kontrolní mechanizmy, které jsou požadovány pro určitou metodu kanálového přístupu. Toto umožňuje několika stanicím se připojit na jediné fyzické médium a sdílet ho. Příkladem takovéhoto systému jsou BUS sítě, Ring sítě, Hub sítě, bezdrátové sítě nebo polo-duplexované přímo propojené linky.

2.6.6. SANA II

Jedná se o jediné softwarové rozhraní mezi AmiTCP (AmiTCP je jediné volně dostupné TCP/IP pro Amigu) a naším síťovým rozhraním.

2.6.7. Ethernet

Jedná se o jeden z typů lokálních sítí, který realizuje vrstvu síťového rozhraní. V LANech se Ethernet prosadil v 80% všech instalací. Jeho popularita spočívá v jednoduchosti protokolu a tím i snadné implementaci i instalaci. Původní protokol s přenosovou rychlostí 10 Mbit/s byl vyvinut firmami DEC, Intel a Xerox pro potřeby kancelářských aplikací. Poté však byl v poměrně pozměněné podobě normalizován institutem IEEE jako norma IEEE 802.3. Tato norma byla převzata jako ISO 8802-3, autoři původního Ethernet vytvořili upravenou verzi Ethernet II, která změnila některé časové konstanty s cílem dosáhnout vyšší kompatibility se standardem 802.3. Mezi oběma specifikacemi je však rozdíl ve formátu rámce.

Klasický Ethernet používal sběrnicovou technologii. Jednotlivé stanice jsou na něm identifikovány svými hardwarovými adresami (MAC adresa). Když stanice obdrží paket s jinou než vlastní adresou, zahodí jej. Pro přístup ke sdílenému přenosovému médiu (sběrnici) se používá CSMA/CD(Carrier Sense with Multiple Access and Collision Detection). Česky to znamená: Metoda mnohonásobného přístupu s nasloucháním nosné a detekcí kolizí.

Stanice, která potřebuje vysílat, naslouchá co se odehrává na síti (přenosovém médiu). Pokud je v klidu, začne stanice vysílat. Může se stát, že dvě stanice začnou vysílat přibližně ve stejnou dobu. Jejich signály se pochopitelně smíchají dohromady. Tuto situaci nazýváme kolizí a vysílací stanice ji poznají podle toho, že během svého vysílání zároveň zjistí příchod cizího signálu. Stanice, která detekuje tento stav, vyšle krátký signál (jam o 32 bitech). Poté se všechny vysílající stanice odmlčí a po uplynutí nějaké doby se pokusí o nové vyslání. Mezi

opakovanými pokusy o vysílání stanice počká vždy náhodnou dobu. Interval, ze kterého se čekací doba náhodně vybírá se během prvních deseti pokusů vždy zdvojnásobuje. Stanice tak při opakovaných neúspěších „ředí“ své pokusy o vysílání a zvyšuje tak pravděpodobnost, že o sdílené médium úspěšně podělí s ostatními. Pokud během šestnácti pokusů neobdrží rámec odvysílat, stanice své snažení ukončí a ohlásí nadřízené vrstvě neúspěch.

Ke kolizi může dojít jen v době, která uplyne od začátku vysílání do okamžiku, kdy signál vysílaný stanicí obsadí celé médium (poté další zájemci o vysílání zjistí, že médium je obsazené a počkají na jeho uvolnění). Tento interval se nazývá kolizní okénko a musí být kratší, než je doba vysílání nejkratšího rámce. Jinak by mohlo docházet k nezjištěným kolizím (dvě vzdálené stanice odvysílají krátké rámce, které se na kabelu zkomolí, ale obě stanice ukončí vysílání dříve, než k nim dorazí kolidující signál).

Tato metoda je velmi efektivní při nižším zatížení sítě (cca 30% šířky pásma). Její efektivita klesá při větším počtu zájemců o vysílání, kdy může dojít k exponenciálnímu nárůstu kolizí. Efektivita CSMA/CD je vyšší pro delší rámce, protože při jejich přenosu je výhodnější poměr mezi trváním kolizního okénka a vysílání dat.

Formáty rámce

Formát rámců sítě Ethernet II a IEEE 802.3 se skládá z následujících polí:

Preambule: Skládá se z 8 byte, střídavě binární 0 a1. Poslední byte má tvar 10101011 a označuje začátek vlastního rámce. Preambule slouží k synchronizaci. Poslední byte se někdy nazývá omezovač počátku rámce(Starting Frame Delimiter SFD)
Cílová adresa: Fyzická MAC adresa o délce 48 bitů (v rámci LAN pro všechny stanice stejné délky). Adresa může být individuální (unicast), skupinová (multicast) a všeobecná (broadcast)
Zdrojová adresa: Fyzická adresa stejného typu jako cílová, ale je to vždy individuální adresa konkrétní stanice (rozhraní)
Typ protokolu nebo délka:

Pro Ethernet II je to pole určující typ vyššího protokolu
Pro IEEE 802.3 udává toto pole délku pole dat

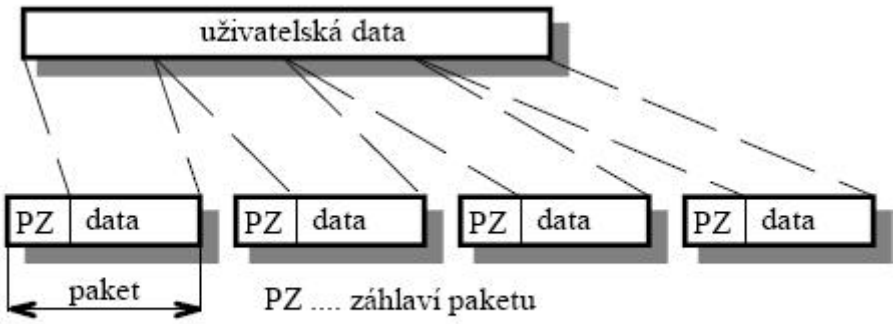
Data: Pole dlouhé minimálně 46 oktetů a maximálně 1500 oktetů. Minimální délka je nutná pro správnou detekci kolizí
Kontrolní součet: (Frame Check Sequence, FCS) jedná se o dvaatřiceti bitový cyklický kontrolní kód, který se počítá ze všech polí s výjimkou preambule a FCS. Slouží ke kontrole správnosti dat, tzn. příjemce si jej vypočítá z obdrženého rámce a pokud výsledek nesouhlasí s hodnotou pole, rámec je zahozen jako vadný.

3.Síťová vrstva

3.1. Principy spínání paketů

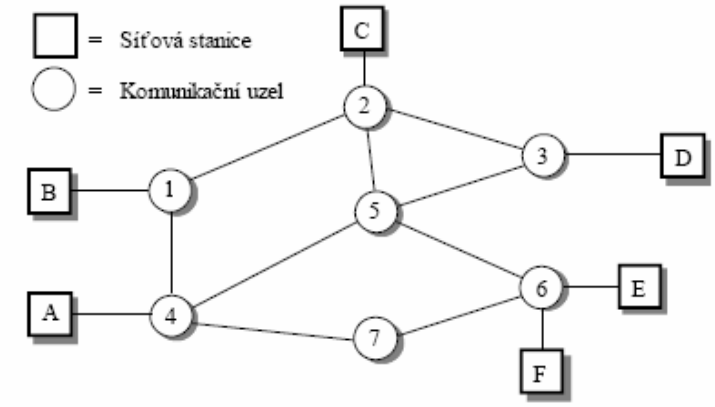
Síťová vrstva musí být použita všude tam, kde spolu chtějí komunikovat dva nesousedící účastnící spojení, tj. existuje-li mezi nimi nepřímé spojení. V tomto případě je nutné mezi nimi najít vhodnou cestu jdoucí přes mezilehlé uzly od jednoho koncového uzlu ke druhému. Možných cest může být samozřejmě více, ale vybrána může být pouze jedna, po které je poté zajištěno správné předání dat.

Obecně existuje více druhů sítí. Základní dělení je na spínání okruhů a přepojování paketů. Pro další výklad budeme předpokládat sítě s přepojováním paketů. Ty se obvykle použijí tam, kde není trvalá potřeba přenosu dat mezi zdrojem a cílem dat. Princip je vysvětlen na obrázku.



Obrázek 2.76: Způsob vzniku paketů

Typická horní hranice pro délku paketů je 1000 oktetů (byte). Jelikož uživatelská data jsou delší, musí být zpráva pro přenos rozdělena do čtyř paketů. Každý paket pak obsahuje své záhlaví (řídicí informaci paketu) a určitou část uživatelských dat. Na základě svého záhlaví je pak paket směrován sítí do uzlu dle následujícího příkladu:



Obrázek 2.77: Obecná struktura sítě (neúplný polygon)

Uvažujme jednoduchou síť z obrázku výše. Nechť je paket vyslán ze stanice A do stanice E. Bude mít v řídicím poli adresu cílové stanice tj. E. Vlastní paket je vyslán ze stanice A do uzlu 4. V tomto uzlu je uchován, je zde určen následující uzel a poté je paket předán do fronty paketů na lince mezi uzly 4-5.

3.2. Protokolové sady síťové vrstvy

Sada protokolů IPX/SPX
Tato sada protokolů byla vyvinuta firmou Novell pro její síťový software NetWare. Pozdější verze tohoto programu však již umí pracovat s lepším TCP/IP a dokonce verze 6 NetWare IPX/SPX ani neumí. Tato sada obsahuje mnoho různých protokolů, nejdůležitějšími jsou protokoly IPX a SPX.

IPX (Internet Packet Exchange) – je protokolem nespojově orientovaným, je určen k přenosu dat mezi jednotlivými síťovými stanicemi, avšak nekontroluje správnost přenosu. Pracuje právě na úrovni síťové vrstvy.
SPX (Sequenced Packet Exchange) – jde o protokol spojově orientovaný, pracuje na úrovni transportní vrstvy, a proto se pro naše účely nehodí, protože však je v balíku s IPX musela zde o něm být zmínka.

Adresace v sítích IPX/SPX
Adresa každého PC v síti je generována automaticky a skládá se ze tří čísel. Prvním je osmimístné hexadecimální číslo externí sítě IPX (external network number), toto číslo využívají především směrovače a jsou vždy stejné pro počítače, které leží v jednom segmentu sítě. Následně je přidáno dvanáctimístné číslo síťové karty (node number), někdy též označované jako MAC adresa (Media Access Control adress). Tímto číslem je označena každá síťová karta od svého výrobce, přičemž na světě existuje vždy jedna karta s jednou MAC adresou. Posledním číslem, z kterého ose vytváří adresa v síti je čtyřmístné hexadecimální číslo interní sítě(IPX internal network number). Tímto číslem je identifikován server.

Sada protokolů TCP/IP

Je dnes nejpoužívanějším a nejnovějším protokolem proto jsme si nemohli dovolit jej vynechat.. Jeho použití je velice univerzální – může být nasazen v sítích internetu, domácích sítích založených na platformě Novellu i Microsoft, nebo třeba v Linuxu, Jedná se o soustavu protokolů.
Avšak jejich koncept je natolik obsáhlý a složitý, že jiné práce se jimi zabývají dopodrobna, a proto je vynecháme.

Síťové komunikační protokoly Poseidon

Jednotky Poseidon jednotlivých modulů tvoří rozhraní mezi sítí Ethernet na jedné straně a různými čidly pro měření teplot, vlhkosti, kontaktních vstupů a dalších veličin. Naměřené hodnoty jsou sdíleny pomocí dále uvedených protokolů, které přibližně popisuje tato stránka. Naměřená data z Poseidonu lze získat různými způsoby, které odpovídají různým typům aplikací. Pro průmysl a v něm používanou vizualizaci je určen Modbus/TCP, pro telekomunikace a vzdálenou zprávu je určeno SNMP.

WEB řešení

Stav čidel Poseidonu je zobrazován na jednoduché WWW stránce, která volá jako první při přístupu na Poseidon pomocí WWW prohlížeče. Stránka se automaticky periodicky obnovuje s intervalem 5-30 sekund. Je-li některá hodnota z proměnných nastavena jako ALARM a hodnota se dostane do této oblasti, je tento binární vstup podsvícen červenou barvou.
Dále existují ještě realizace pomocí XML tagů nebo Modbus. Lze také užít SNMP.

4. Komunikační protokol nižších vrstev – vlastní návrh

Komunikační protokoly jsou množiny pravidel, která definují, jak úspěšně přenášet data mezi jednotlivými stanicemi či servery. Jsou to pravidla definující jak přenos vést, řídit a také ukončit. Podle typu hardwaru, softwaru a dat jsou jich různé sady, přičemž povinností výrobce je uvést, které protokoly jejich zařízení podporuje. Jedná se o protokol, který musí respektovat třívrstvý model a je i takto definován:

vrstva 1 – jedná se o fyzickou vrstvu, která řeší elektrické rozhraní
vrstva 2 – jedná se o spojovou vrstvu, jejíž první polovina zabezpečuje strukturu rámce a druhá polovina této vrstvy zabezpečuje adresaci síti
vrstva 3 - jedná se již o aplikační vrstvu, která řeší konečnou výměnu informací

4.1. Fyzická realizace

Tato vrstva se zabývá převodem signálu na přístupový bod. Jako přístupové body je možno použít přístroje od nejrůznějších firem. Například PlanetWsAP, Linksys nebo Aerocomm

4.2. Realizace spojení na spojové vrstvě

Rámec této vrstvy má mezi vestavným zařízením a přístupovým bodem následující strukturu

Tab. 4.2.1. vzhled rámce na spojové vrstvě

SYN	DLE	EXT	END
16	10	3	0

Pro ohraničení rámce se používají následující znaky:
SYN – značí počátek rámce
DLE – první znak konce rámce
EXT – druhý znak konce rámce

4.2.1 Řešení transparence

Zabezpečení je realizováno pomocí generačního polynomu:

$G(x)= x^{32}+ x^{31}+ x^{30}+ x^{29}+\ldots+ x^{3}+ x^{2}+1$

Pomocí tohoto polynomu tak dosáhneme dostatečného stupně zabezpečení dat ve smyslu ochrany proti chybovosti.

4.3. Síťová realizace

4.3.1 Obecná struktura síťové vrstvy

Na síťové vrstvě mají standardně protokoly osmi bajtovou hlavičku doplněnou o typ služby, jak ukazuje následující tabulka:

Tab. 4.3.1 Vzhled hlavičky síťové vrstvy

Adresa cíle	Adresa odesilatele	Typ protokolu	Klíčové slovo protokolu	Typ služby	Charakteristika služby

Základní funkce

- očekávání odpovědi na vyslaná data
- ve vestavném zařízení se dohledávají služby dle příchozích dat, v případě neexistence služby dle parametru v příchozích datech, vestavné zařízení patřičně odpoví
- po vykonání služby následuje náležitá odpověď PACK (positive acknowledgement = kladná odpověď) nebo NACK (negative acknowledgement = záporná odpověď)

Adresa cíle

- nabývá hodnot 1 až 9999 a je dána číslem vestavného zařízení, toto číslo se zadává hexadecimálně

Adresa odesilatele

- obsahuje adresu přístupového bodu, taktéž se zadává hexadecimálně

Typ a řídící slovo protokolu

Typy jsou následující
0000 – volné pakety pro libovolné využití
0001 – vzdálené spouštění funkcí
0002 – typ protokolu určující směr přenosu

Typ služby a její parametr

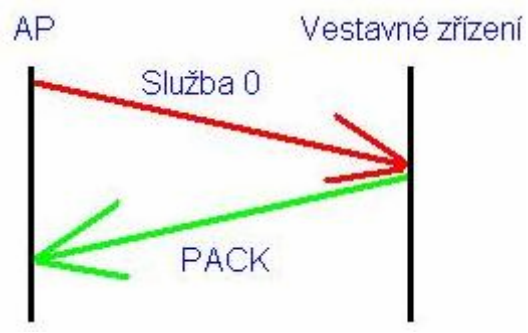
Paket volání služby – jeho první bajt musí vždy obsahovat typ číslo požadované služby, další bajty pak obsahují parametry

4.3.2. Obecné funkce

- Dotaz žije

  Služba typu 0, data jdou na vestavné zařízení z přístupového bodu, přičemž vestavné zařízení vrací pouze Acknowledgement

Obr. 4.3.1. schéma dotazu „žije“



- Funkce RESET

  Tato funkce resetuje vestavné zařízení. Při volání této funkce se zastaví smyčka nulování časovače a poté je tento příkaz proveden. Následně je nutný krátký časový úsek cca 2s pro aktivaci vestavného zařízení

- Zápis dat do paměti

  Tato služba zapíše obsah rámce (jednoho či více bajtů) do konfigurační paměti vestavného zařízení

  Příklad zápisu dat
  -číslo zařízení
  -odkud (adresa počítače či sloupu)
  -typ protokolu
  -řídící slovo protokolu (určuje směr komunikace)
  -typ služby (zde se jedná o zápis dat)
  -počet zapisovaných dat

- Čtení dat z paměti

  Tato služba přečte data, která obsahuje paměť zvolené adresy. Přičemž je možno zvolit různou délku dat

- Zjištění údajů o vestavném zařízení

  Tato služba slouží k zjištění základních informací. Například poloha zařízení, stav, verze softwaru. Následně je možno do této funkce zakomponovat další volitelné funkce
  Odpovědí na takováto volání mohou být například:
  <Integer> poloha(zjistí podle GPS)
  <Word> stav(tzn. připraven, zaneprázdněn, aj.)

4.3.3. Práce s FLASH pamětí ve vestavném zařízení

-Zásady pro přenos souborů a práci s nimi

a) formátování FLASH disku, mazání souborů a uvolnění jimi zabíraného místa
b) otevření a uzavření souboru na vestavném zařízení
c) čtení ze souboru, zápis do souboru

-Formátování FLASH disku

Tato služba se provádí před nahráváním souborů, zejména při nové instalaci vestavného zařízení

-Příprava souborů pro přenos

Příprava souborů pro příjem na vestavném zařízení probíhá tak, že soubor se otevře pro zápis v blokovém módu, což značí, že se na disku vytvoří fyzicky prázdný soubor

-Přenos souborů do zařízení

Vlastní odeslání připraveného souboru je realizováno protokolem síťové vrstvy, jež je určen pro hromadný přenos dat. Díky tomuto protokolu je možné libovolná data opakovat v libovolném pořadí. Zjednodušeně řečeno vestavné zařízení zapisuje do předem připraveného volného místa přijatá data ve správném pořadí

-Služba ke zjištění nepřijatých bloků

Díky této speciální službě je možno si od vestavného zařízení vyžádat tzv. BLOCK LIST, díky němuž lze zjistit, které bloky jsou správně nahrány, a které nikoliv. Bohužel však v jedné zprávě lze získat pouze data o max. délce 200 slov.

-Ukončení přenosu souboru

Po úspěšném přenesení souboru je nutno tato data uzavřít. Pokud není tato operace provedena dálkově je provedena automaticky vestavným zařízením díky časovači, který přenášená data uzavře v případě, že se s nimi déle jak 10 minut nepracuje.

4.3.4. Měření kvality přenosu

Princip měření kvality přenosu

Díky zjišťování kvality přenosu dat se vytváří přibližně stejný datový tok, jako u přenosu na jednotlivá zařízení či hromadnými přenosy na několik dostupných jednotek

Z vysílajícího počítače je tudíž nutno zadat tyto parametry:

a) Počet testovacích paketů
b) Délka FTP paketu (standardně je to 125 slov)
c) Číslo testovací sekvence
d) Číslo příjemce (buďto konkrétní adresa, nebo všesměrové)

Návratová hodnota musí být potvrzení o odvysílání celé zadané sekvence

Testování kvality přenosu

Funkce odešle zadaný počet paketů s libovolným obsahem (lze též odesílat libovolné části dat již dříve odeslaných) a ukončí svoji činnost. PACK se vyšle až po odeslání všech paketů. Na voze(ch) se správným příjmem paketů se navýší čítač, avšak pouze v případě, že čísla dvou testovacích sekvencí dvou po sobě příchozích paketů se shodují, v opačném případě se čítač nastaví na hodnotu 1

Pro odesílání testovací sekvence se odesílání realizuje pomocí jiného protokolu, a proto je nutno změnit i záhlaví síťové vrstvy dle následující tabulky

Tab. 4.3.2. Pozměněné testovací záhlaví

Adresa cíle	Adresa odesilatele	Typ protokolu	Testovací sekvence

Tab. 4.3.3. Demonstrace paketu testovací sekvence

Adresa cíle	Adresa odesilatele	Typ protokolu	Testovací sekvence	Počet náhodně vybraných slov

Adresování cíle je standardní jako u síťové vrstvy tzn., že je možno použít všesměrové vysílání na adrese 0x0000

Čtení hodnoty čítače sekvence

Tato služba se volá na vestavná zařízení vždy po odvysílání testovací sekvence. Na straně příjmu se hodnota čítačů získaných z jednotlivých zařízení porovná s odeslaným počtem paketů a tím se zjistí kvalita přenosové cesty.

Parametry volání služby

a) identifikátor vzdálené proměnné
b) hodnota čítače z vestavného zařízení
c) hodnota testovací sekvence

Finální výsledek testu je pak přístupný v globální proměnné TEST_DATA, jež je umístěna ve vestavném zařízení, kde horní bajt je počet správně přijatých paketů a poslední bajt je číslo testovací sekvence posledně přijatého paketu

5. Komunikační protokol vyšších vrstev-vlastní návrh

5.1 Využitelné vrstvy

-Transportní vrstva

Hlavním úkolem této vrstvy je poskytnout efektivní přenosové služby své bezprostředně vyšší vrstvě(Tzn. relační). Jedná se o poslední vrstvu OSI modelu, která slouží pro vlastní přenos dat, ostatní vrstvy jsou již od přenosu jako takového izolovány.

-Relačně – prezentační vrstva

Úkolem této dvojvrstvy, jež se obvykle sdružuje do jedné, je udržení dialogu, i když dojde ke ztrátě dat v oblasti transportní vrstvy a také synchronizace spolupracujících procesů. Dle doporučení by měla poskytovat následující služby:

a)koordinace kooperace mezi procesy
b)příznak oprávnění
c)simplex, duplex
d)request, relay

Ve spojení s prezentační vrstvou zajišťují dále překlenutí rozdílů v reprezentaci dat a také překlenutí rozdílů činnosti jednotlivých entit. Jedná se tedy o změnu syntaxe při zachování sémantiky.

Aplikační vrstva

Zahrnuje všechny funkce a aplikace, jež se vyznačují dvojicí aplikačních procesů. Tyto funkce závisí na aplikaci, pod kterou se obecně chápe skupina aplikačních procesů. Touto vrstvou mohou být například realizovány tyto funkce:

a)Identifikace účastníků komunikace
b)Zjištění dostupnosti účastníka komunikace
c)Rozhodování o povolení komunikace žadatelům
d)umožnění přístupu k požadovaným zdrojům
e)Stanovení metod pro opravu chyb, potvrzování

Aplikační vrstva je okno do OSI systému pro uživatelské procesy

5.2. Vlastní protokol

Jelikož se jedná o přenos dat pomocí GPRS, je nutné zde do protokolu zařadit UDP datagramy, proto bude daná služba nespojovaná a nespolehlivá. Systém však musí umožňovat komunikovat i na úrovni zabezpečené a spolehlivé, neboť první varianta je vhodná pouze k jednoduchým operacím jako je kupříkladu zjišťování polohy zařízení, či jeho stav. Avšak pro složitější operace jakými jsou přenos souborů, či vzdálená konfigurace vestavného zařízení musí být služba spolehlivá. Tuto spolehlivost nám ve výsledku zaručí aplikační vrstva. Dále je nutno doplnit, že protokol pro jednoduchost navrhneme na principu Master -Slave

5.2.1. Transportní řešení

Na této vrstvě bude probíhat samotná výměna dat, konkrétně pomocí již zmíněných UDP datagramů, jejichž struktura je zobrazena v následující tabulce, na doplnění uvedu, že v této vrstvě se budou ukládat odeslané a dosud nepotvrzené zprávy

Tab. 5.2.1 Vzhled UDP datagramu

16bitů	32bitů
Zdrojový port	Cílový port
Délka	Kontrolní součet
Data	

Zdrojový port – doplňková položka, nemusí být vždy obsažena, je-li implementována vypovídá hodnotu portu, jež odesílá data

Cílový port – určuje adresu portu, na který mají být data zaslána

Délka – určuje délku celého datagramu v oktetech. Zahrnuje jak hlavičku tak data a její minimální hodnota je osm oktetů.

Kontrolní součet – jedná se o pole, jež doplňuje hlavičku na potřebných 32 bitů. Jedná se o libovolné pole, které j možno vynechat, avšak v praxi se takřka vždy využívá.

Předpokládaný způsob výměny dat

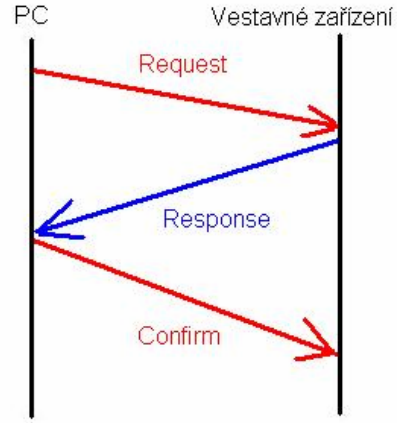
Teoretický průběh navázání spojení

Connect – request – jedná se o zprávu, kterou bude vysílat vysílající strana, v našem případě Master

Connect – response – jedná se o zprávu, jež potvrzuje přijetí předchozí zprávy. Jedná se de facto o požadovanou odpověď na volaní Master, vysílá ji Slave

Connect – confirm – zpráva, která je odesílána volající stranou jako potvrzení navázání spojení

Obr. 5.2.1. Průběh navázání spojení



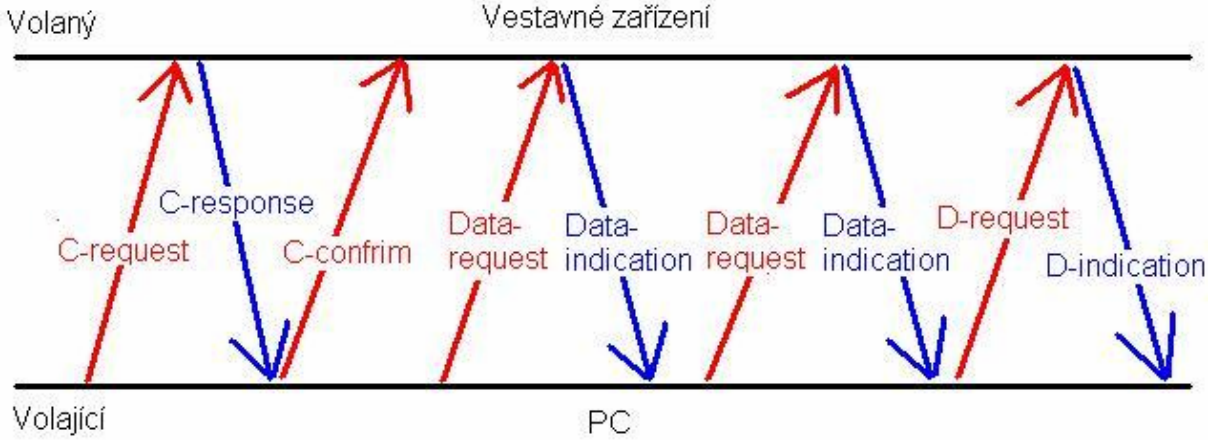
Dále je nutno do této fáze zahrnout dva poměrně důležité programy, kterými jsou:
Connect – tento program umožňuje řídit spojení a v případě zjištění chyby vrací zápornou hodnotu. Je na straně volajícího
Listen – indikuje volanému, že transportní vrstva vyslala požadavek na navázání spojení, záleží na volaném jak se zachová.

Teoretický průběh přenosu dat
Data – request – zpráva jež volanému přináší již vlastní data, jedná se o zprávu od vysílajícího
Data – indication – zpráva, která je vysílána volaným účastníkem komunikace, indikuje o přijetí dat

Programové vybavení nutné k realizaci přenosu dat
Send – dovoluje odeslat požadovaná data, při chybě vrací stav na počátek děje
Recieve – na straně volaného umožňuje bezpečné přijetí dat. V případě, že je paměť plná, nebo dojde k chybnému přijetí. Odešle zprávu s požadavkem návratu stavu na počátek

Teoretický průběh ukončení spojení
Disconnect – request – vysílá volající. Tato zpráva obsahuje požadavek na uzavření spojení a také důvody proč se tak děje. (např. ukončený přenos dat)
Disconnect – indication – odpověď na předchozí zprávu, je odesílána volanou stranou. Obsahuje obdobná data jako předchozí zpráva

Obr. 5.2.2 Předpokládaný průběh výměny dat mezi PC a vestavným zařízením



Takto navržený komunikační protokol bude ve finále ke komunikaci používat 10 transportních protokolárních datových jednotek. Zde je jejich výpis:

a)žádost o navázání spojení (Connection request - CR)
b)potvrzení o navázání spojení (Connection confrim - CC)
c)žádost o rozpojení spojení (Disconnect request -DR)
d)potvrzení žádosti o rozpojení spojení (Disconnect confrim - DC)
e)data (Data - DT)
f)zrychlená data (Expedited data - ED)
g)potvrzení (Acknowledgement - AK)
h)zrychlené potvrzení (Expedited Acknowledgement - EA)
i)odmítnutí (ReJect - RJ)
j)chyba (Error - ER)

Všechny tyto datové jednotky je však nutno zakomponovat do patřičného komunikačního záhlaví, jež bude vypadat následovně:

Tab. 5.2.2. komunikační záhlaví

bajty	bity							
	7	6	5	4	3	2	1	0
1	NACK / PACK			S	V	verze protokolu		
2-254	ověřovač transportní vrstvy							
255	příznak funkce							
256	priorita spojení							

NACK / PACK – toto pole nese informaci po přijetí respektive nepřijetí příkazu, záměrně je pro toto potvrzení vyhrazeno místo tří bitů, aby byla zajištěna dostatečná přehlednost této důležité informace. Nese hodnotu 000 = NACK, nebo 111 značící PACK

S bit – pole indikující směr komunikace. Obsahuje-li hodnotu 1 jedná se o směr komunikace Master-Slave, v opačném případě se jedná o komunikaci Slave-Master

V bit – jedná se o pole, jehož hodnota vypovídá o nutnosti potvrzení obsluhou. Má-li hodnotu 1, je toto potvrzení požadováno v opačném případě nikoliv

Ověřovač – jeho funkce bude podrobněji vysvětlena dále v textu

Příznak funkce – soubor všech těchto parametrů je vypsán nad strukturou záhlaví. Toto pole obsahuje zkratku funkce jež bude protokolem realizována.

Priorita spojení – jedná se o parametr, určující důležitost funkce. Nabývá hodnot od –7 do +7 přičemž -7 značí proces s největší důležitostí

Ověřovač transportní vrstvy

Pomocí tohoto pole lze velmi jednoduše zajistit službu, která je po protokolu vyžadována. Touto službou je možnost zjištění kvality signálu z důvodu výběru nejlepšího přístupového bodu na zařízení. Postup výběru nyní v několika krocích nastíním.

Krok číslo 1

Obsluha u PC si přeje zaslat data na vestavné zařízení, které je umístěno například v policejním voze. Jelikož obsluhující předem neví, kde momentálně se vůz nachází přiřadí do tohoto pole libovolnou hodnotu v rozsahu (2 – 254)a vyšle požadavek na spojení pomocí multicastu, což zaručí že se všechny dostupné přístupové body pokusí o navázání spojení, do pole V zadá požadavek na potvrzení, čímž zajistí, že protokol bude posílat data zpět na přístupový bod. Tímto příkazem zabezpečí zpětné odeslání záhlaví, které bude obsahovat menší počet dat v poli ověřovače.

Krok číslo 2

PC na straně vysílajícího s pomocí softwarového vybavení vyhodnotí, který přístupový bod je nejvhodnější. Takto zvolený bod bude následně výhradně využíván pro komunikaci s vestavným zařízením. Samotné vyhodnocení proběhne velmi prostým způsobem tak, že PC odečte přijatou hodnotu ověřovače od hodnoty předem nastavené a výsledek rozdělí na polovinu. V případě lichého výsledku se zaokrouhlí nahoru, neboť PC bude předpokládat vždy horší variantu.

Krok číslo 3

Tímto krokem je spouštění časovače ihned po výběru vhodného přístupového bodu, neboť vestavné zařízení může být v pohybu, což může vést k postupnému zhoršování přenosových podmínek jednou zvoleného přístupového bodu, proto je nutné, po určité době „otestovat“ i ostatní možnosti spojení. Tím je myšleno, že po vypršení časovače se opět rozešle záhlaví s novou hodnotou, díky čemuž se vybere (případně zachová) nový přístupový bod. Pakliže od vestavného zařízení přijde údaj „budu stát“ není nutné časovač spouštět, tedy konkrétně až do té doby, dokud nepřijde údaj „jsem v pohybu“

Krok číslo 4

Bude-li vypnuto vestavné zařízení je možné ukončit relaci časovače i výběru přístupových bodů. Což tvoři závěrečný krok. Konkrétně je tím myšleno, obdrží-li obsluha PC údaj „konec“ vypne časovač a tím ukončí režim výběru a uvolní tím výpočetní kapacitu pro další vozy.

Tímto lze ukončit veškeré děje, které se dějí na transportní vrstvě, jelikož tato úroveň má za hlavní úkol přenášet data. Další služby a zajištění obstarávají vyšší vrstvy OSI modelu, a proto si dovoluji ukončit rozbor a návrh na transportní vrstvě a přikročit k vyšším vrstvám.

5.2.2. Relační a prezentační řešení

Tato „dvojvrstva“ musí zajistit, aby přenos dat probíhal zcela v pořádku a hladce. Služby zde popsané se postarají o bezchybný přenos a úspěšné doručení dat, následně zaručí dostatečnou kompresi dat a případné kódování přenášených dat.

- Realizované služby

Řízení spojení – jedná se nadstavbu k transportní vrstvě a je předpokládáno, že nižší vrstva dokáže spojení vést v pořádku. Proto není nutno tuto službu využívat vždy

Uvolnění spojení – jedná se o službu, jež zajišťuje uvolnění přenosové cesty pro procesy s vyšší prioritou, přičemž se nejedná o zrušení spojení ale o jeho pozastavení po dobu nezbytně nutnou, čímž nedochází ke ztrátě dat. Ke ztrátě dojde pouze v případě požadavku na zrušení spojení.

Přenos dat – zde je myšlen spíše dohled nad správným průběhem relace a také předcházení zahlcení spojení.

Garantovaná služba – zadržení dat do doby, než dojde k jejich celé kompletaci a v případě požadavku je odeslat (jako celek) nebo je zničit.

Hlášení vyjímek – umožňuje řešit vyjímečné situace

Komprese dat – na této vrstvě je též zajištěna patřičná komprese dat. Užívá se k tomu několik principů zde je jejich výpis:

a)Hoffmanovo kódování
b)Aritmetické kódování
c)Kontextově orientované kódování
d)LZW kódování

Kódování dat – slouží k ochraně informací, v našem případě nebude nutné

Autentizace zpráv – pomocí této služby se bude ověřovat pravost přenášených dat a tím také pravost klienta

5.2.3. Služby realizované protokolem

Služba „Žije“

Jedná se o službu, která zjišťuje připravenost vestavného zařízení, respektive jeho aktivitu. Očekává se pouze pozitivní Acknowledgement (PACK). Není možná jiná odpověď

Služba „Stav“

Tato služba zajišťuje okamžité zjištění stavu vestavného zařízení. To značí, že lze díky ní operativně posílat data v průběhu činnosti zařízení, měnit nastavení či jinak reagovat na vyskytující se změny.

Služba „Příkaz“

Pomocí této služby může obsluha z dispečinku bezpečně kontrolovat pohyb vozidla v terénu nebo lze prostřednictvím této služby jednoduše zadávat příkazy na vestavné zařízení, tím je myšleno například vnitřní nastavení zařízení, mazání patřičných souborů či jiné příkazy dle požadavků operátora.

Příklad služby „Příkaz“

a) Navázání spojení

Connection Request – parametry: kdo volá, za jakým účelem, nutnost potvrzení

Connection Confrim – potvrzení navázání spojení

b)Přenos dat příkazu

Data – parametry: velikost => požadované místo v paměti

Data Confirm – potvrzení správnosti přenosu

c)Ukončení spojení

Disconnect request – požadavek na ukončení spojení

Disconnect confirm – potvrzení rozpojení

Služba „Výstraha“

Tato služba s velmi vysokou prioritou informuje osádku vozidla o hrozícím nebezpečí na cestě. Služba tohoto typu je přednostně posílána datovým tokem před ostatními službami, ze zcela pochopitelného důvodu.

Služba „Poloha“

Jedná se o službu umožňující okamžité zjištění polohy zařízení pomocí GPS, což ve výsledku umožňuje volbu optimální cesty, či novou selekci přístupového bodu, neboť může dojít k situaci, kdy vozidlo rychle urazí určitý úsek cesty, což může mít za důsledek zhoršení přenosové cesty.

Způsob zjišťování polohy pomocí GPS

Tato funkce bude realizována na vestavném zařízeni následujícím způsobem, do zařízení bude implementován speciální protokol, který je celosvětově využíván ke snímání polohy pomocí GPS (Global Positioning System). Jedná se o protokol NMEA (National Marine Electronics Association), přičemž standart NMEA 0183 je standardem protokolu, který definuje způsob přenosu dat ve větách, kde každá věta začíná $ a končí CR a LF, které jsou přenášeny od jednoho volajícího k několika volaným. Přičemž NMEA 0183 používá sériového přenosu dat, což je sice pomalé, ale pro tento druh spojení dostačující, neboť linka využívá přenos 4800b/s, 8 bitů, bez parity, jeden stop bit. Některé GPS neposílají všechna pole a Cyclic Redundancy Check bývá přidáváno volitelně.

Elektrické zapojení je doporučeno pomocí STP (stíněná kroucená dvojlinka) se stíněním uzemněným pouze na straně vysílače. Standard nijak zvláště nespecifikuje použití zvláštního konektoru.

Příklad věty

$GPAAM,A, 0.10,NM,WPTNME*32<CR><LF>

Význam jednolitých údajů věty:
GP – identifikace volajícího
AAM – signalizace příchodu(arrival alarm)
A – vstup do kruhu příchodů
0.10 – rozsah, okruh, rozptyl
NM – námořní míle (Nautical miles)
WPTNME – jméno zastávky
*32 – data kontrolního součtu

Tab. 5.2.3 Popis znaků vyskytujících se v NMEA zápisu

Popis	Forma	Pole
Úvodní znak	"$"	1
UTC pozice (6 místný časový údaj)	ZDA,hhmmss.ssss,dd,mm,yyyy	2
Zeměpisná šířka (stupně,minuty)	IIII.IIIII	3
Směr zeměpisné šířky	Sever nebo jih	4
Zeměpisná délka (stupně, minuty)	yyyy.yyyyy	5
Směr zeměpisné délky	Východ nebo západ	6
Počet SV	NSV	7
Satelitní identifikační číslo	NSV,n,…	
Počet „n“ opakování		
Zakončovaní značka	“&”	

Převod dat do binární podoby

Vyjádření času a polohy

Tab. 5.2.4. Datový údaj vyjadřující čas

1.bajt	2.bajt	3.bajt
Obsah bajtu viz níže	Čas v sekundách, v 12 hodinovém cyklu	

Obsah 1.bajtu

-1.bit – 0 reprezentuje hodnotu dopoledne, 1 značí hodnotu odpoledne
-2.,3, 4 – tato kombinace vyjadřuje způsob vyjádření časového formátu
000 značí středoevropský čas
-5.bit – 0 značí, že následuje platný údaj o poloze. 1 znamená, že nejnovější údaje nejsou správné a je nutno použít poslední známou platnou pozici vestavného zařízení

Vyjadřování polohy

Zeměpisná šířka – 3 bajty, hodnota nejvyššího bitu vyjadřuje sever=1, jih=0
přesnost vyjadřování této hodnoty v 1/100 000 minut
Zeměpisná délka – 3 bajty, hodnota nejvyššího bitu vyjadřuje východ=1, západ=0, přesnost vyjadřování této hodnoty v 1/100 000 minuty
Stupně 8 bitů, 6 bitů minuty a 10 bitů sekundy

Tab. 5.2.5. Datový údaj vyjadřující polohu

Bajt	První								Druhý								Třetí							
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Hodnota	Stupně								Minuty								Sekundy							

Přičemž první bit v poli stupňů udává sever nebo jih u zeměpisné šířky a u zeměpisné délky udává západ nebo východ

Ostatní parametry polohy

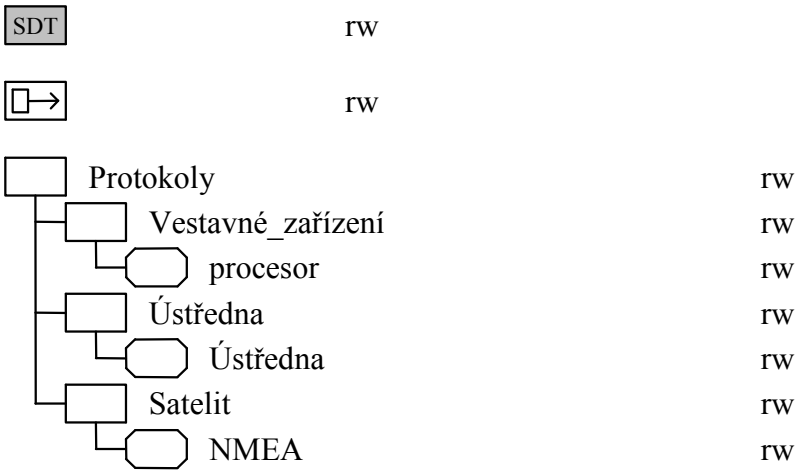
1bajt – síla GPS signálu(0-255)
2bajty – PDOP (Position dilution of precision) – značí rozptyl v přesnosti udávání polohy
1bajt – DGPS (Diferential GPS) – této bajt značí stáří korekce ze sítě DGPS v sekundách(0-255)
2bajty – ID DGPS stanice(0-1023), která provedla předešlou korekci
1bajt – azimut jízdy (upraveno do rozsahu 0-255)
1bajt – rychlost jízdy vozidla v km/h (0-255)

Tab. 5.2.5 Celkový vzhled datového údaje z NMEA

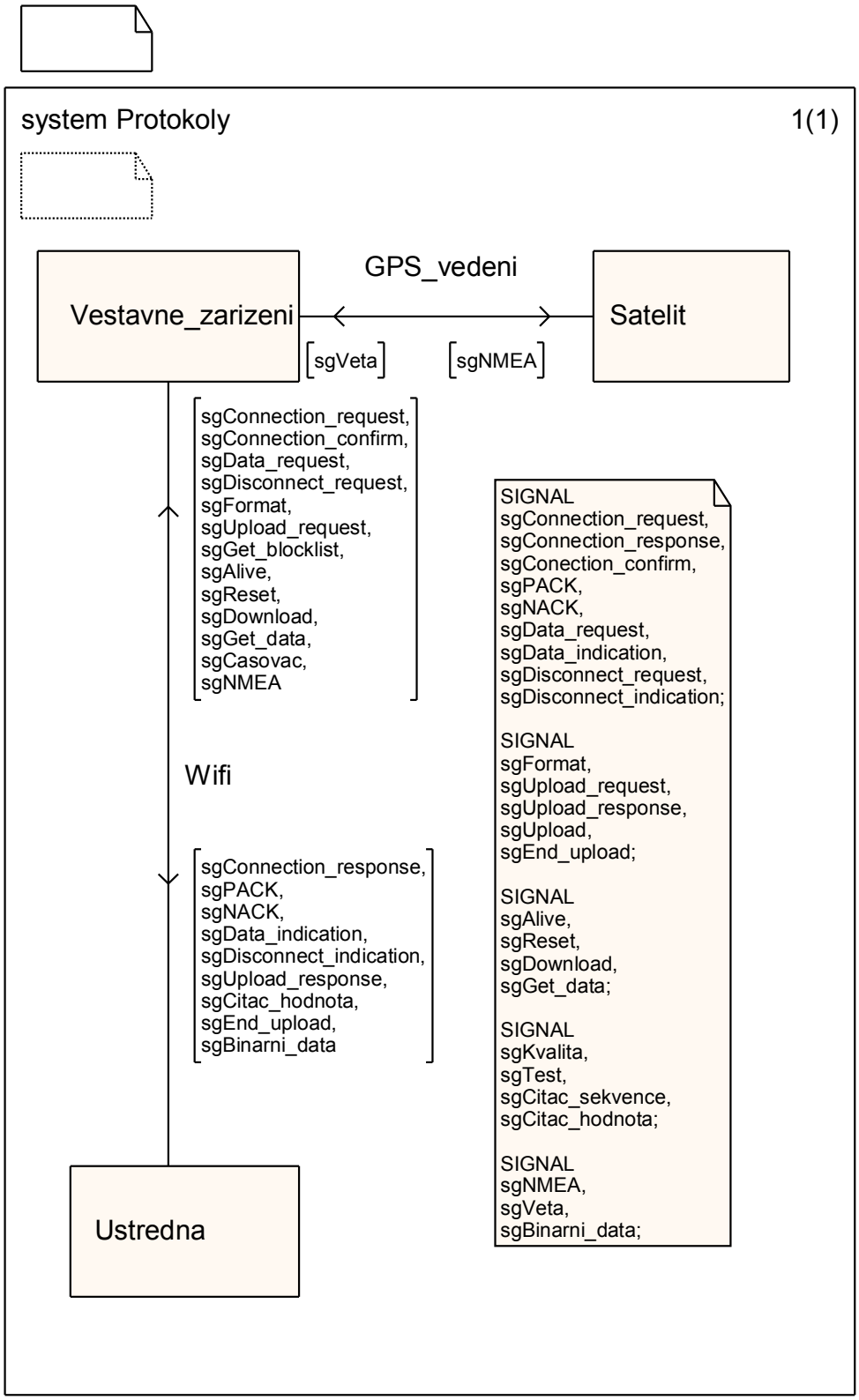
Bajty	1-3	4-6	7-9	10	11-12	13	14-15	16	17
Hodnota	Časový údaj	Zeměpisná délka	Zeměpisná šířka	Síla signálu	PDOP	DGPS	ID DGPS	Rychlost	Azimut

6. Simulační schémata

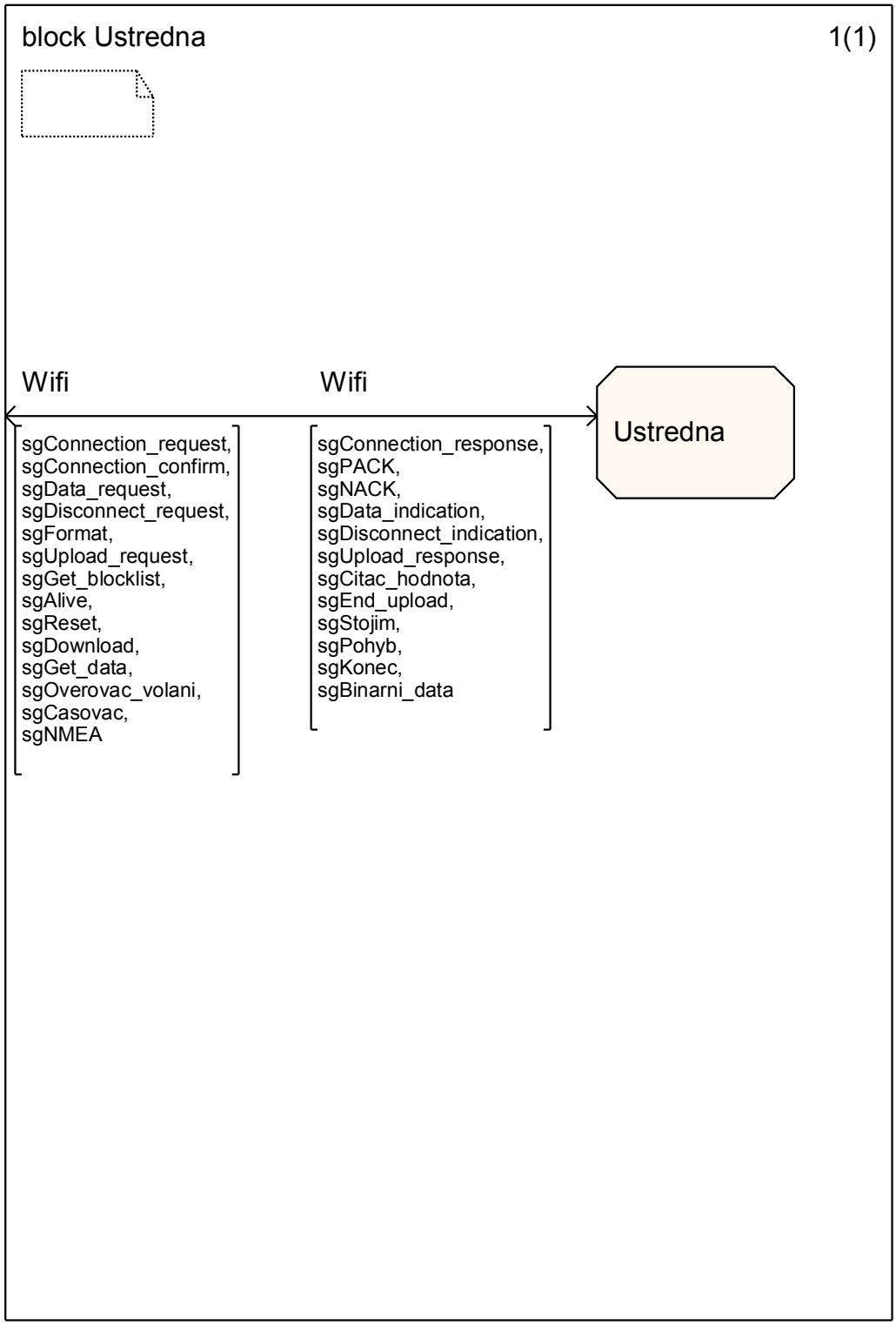
Obr. 6.1 Vzhled simulovaného systému



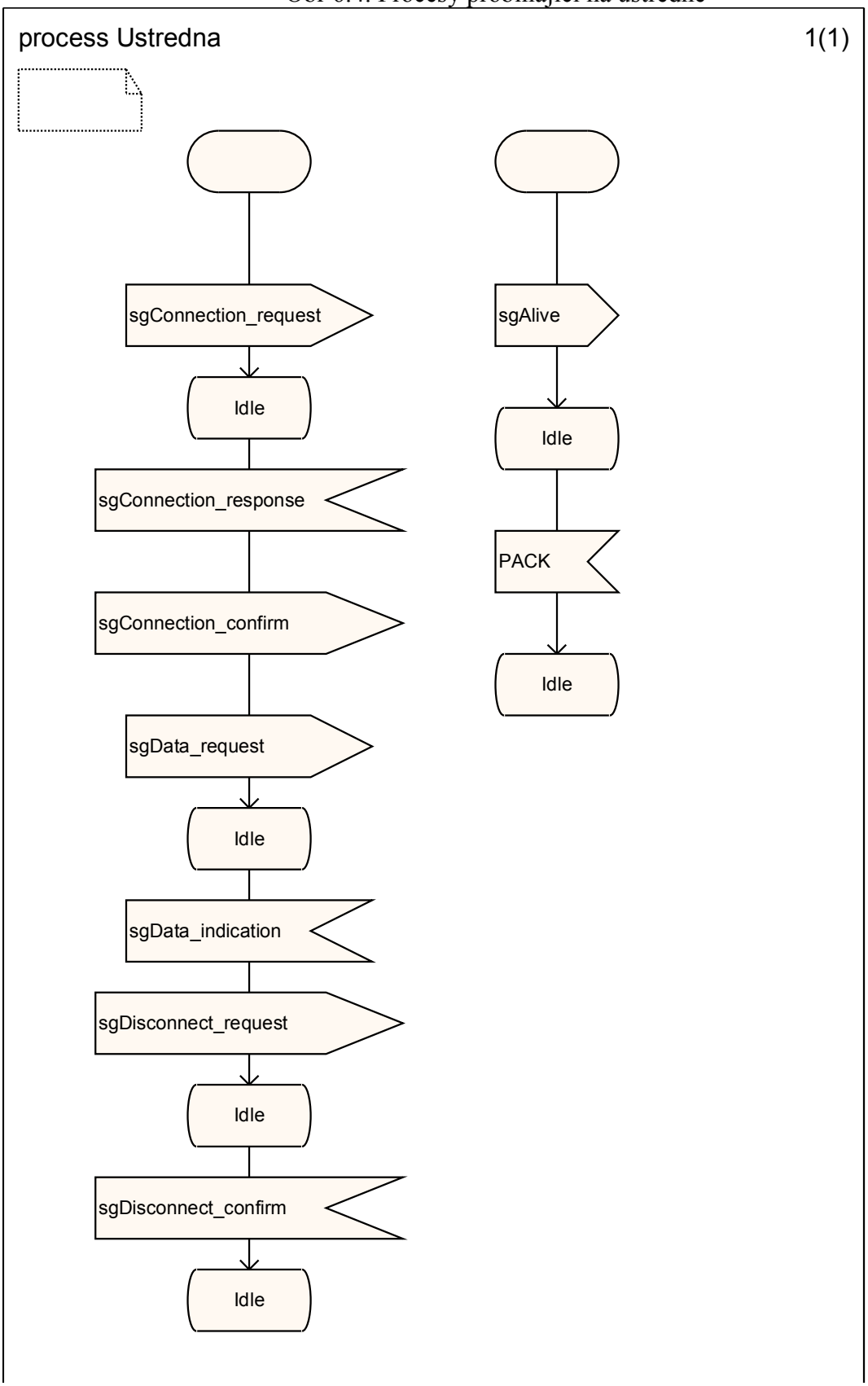
Obr 6.2. Vedení signálů simulovaným systémem



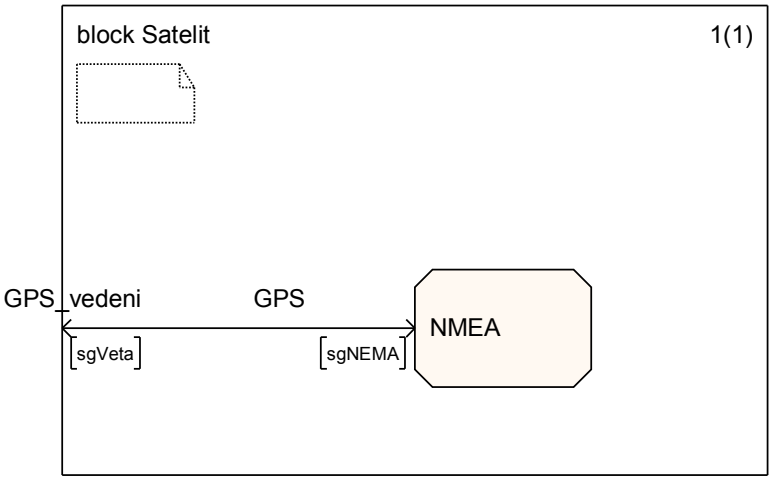
Obr. 6.3. Signály putující z ústředny a do ní



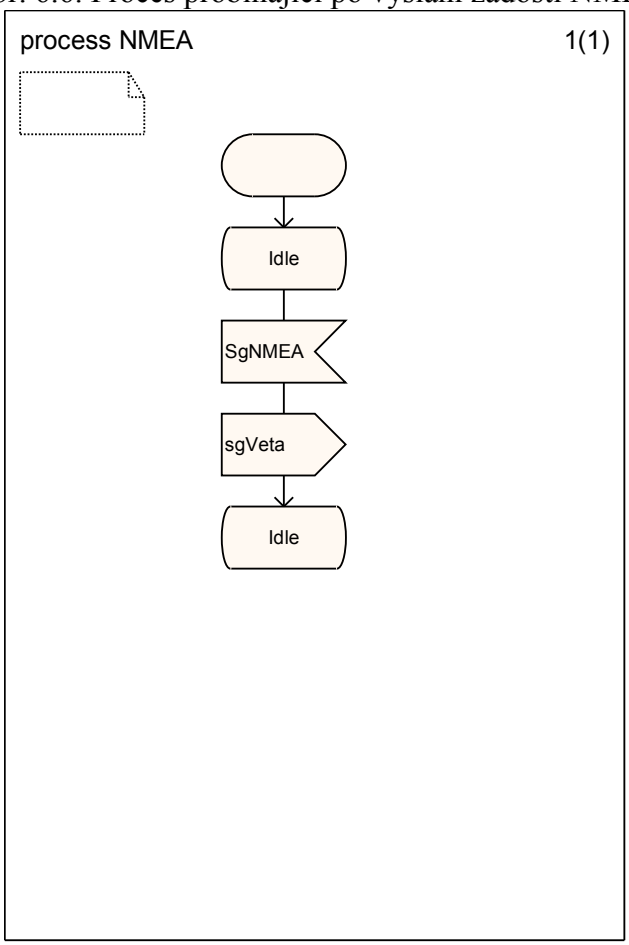
Obr 6.4. Procesy probíhající na ústředně



Obr. 6.5. Signály putující mezi zařízením a satelitem



Obr. 6.6. Proces probíhající po vyslání žádosti NMEA



Závěr

V první části této práce bylo objasněno několik stávajících řešení problematiky komunikačních protokolů, jež respektují třívrstvý model. Bohužel rozsah této práce neumožňuje rozebrat veškerá známá řešení. Z tohoto důvodu byl zvolen přehled těch méně známých řešení, neboť v případě volby protokolu IP by mohla být práce čistě jen o něm. Dále byly prodiskutovány jednotlivé funkce vrstev, jež je možno použít pro návrh komunikačního protokolu, čímž bylo zjištěno, že fyzická vrstva realizuje jen signálový přenos, linková vrstva se již stará o datovou komunikaci a síťová vrstva již přebírá funkci aplikační vrstvy.
V modelu vyšších vrstev bylo pro přenos dat zvoleno UDP datagramů. Čímž vznikla nutnost zabezpečení spojení, z hlediska spolehlivosti. Z tohoto důvodu byla vybrána vrstva relačně-prezentační, neboť poskytuje dostatečné služby právě pro tyto činnosti.

Návrh vlastního protokolu probíhal ve dvou částech, respektive byl pokus o realizování dvou komunikačních protokolů. Jedním je protokol nižších vrstev, kde po ustanovení několika základních parametrů je již možno komunikovat, avšak v omezené míře. Je zcela pochopitelné, že v případě detailního rozboru, by bylo možné služby tohoto protokolu rozšířit a obohatit.

Druhým řešením je komunikační protokol vyšších vrstev. Jedná se sice o složitější a rozsáhlejší strukturu, která však poskytuje již v základu mnohem více služeb, jež je však nutno definovat. Děje se tak z důvodu přímého napojení na aplikační vrstvu, která sama o sobě zaručuje velmi širokou paletu aplikací využitelných v komunikaci.

V poslední části této práce bylo zamýšleno simulovat navržené protokoly v jazyku SDL. Bohužel vzhledem k nezkušenosti autora s tímto jazykem simulace neproběhly dle očekávání, a proto není důvod sem neúspěšné simulace vkládat, jelikož jejich výsledky byly neuspokojivé. Nicméně teoretický výsledek této práce je jistě dostačující.

Seznam použitých zdrojů

http://books.google.sk/books?id=QHr_58UayXkC&dq=validation+of+communications+systems+with+sdl+the+art+of+sdl+simulation+and+reachability+analysis&pg=PP1&ots=iZLy9EVHbT&sig=Y4BFGqjRW-3JotXbqCOPVEpnV_0&hl=sk&prev=http://www.google.sk/search%3Fhl%3Dsk%26q%3D%2BValidation%2Bof%2BCommunications%2BSystems%2Bwith%2BSDL.%2BThe%2Bart%2Bof%2BSDl%2BSimulation%2Band%2BReachability%2BAnalysis.%2B&sa=X&oi=print&ct=title&cad=one-book-with-thumbnail#PPA9,M1

http://www.kh-gps.de/nmea.faq

http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/udp.html

http://www.protocols.com/pbook/tcpip1.htm

http://en.kioskea.net/internet/udp.php3

http://www.ardenstone.com/projects/seniorsem/reports/UDP_Protocol.html

http://www.syn-wiki.de/ban/HTML/P_ISO/Eng/P_iso68.html

http://cs.wikipedia.org/wiki/Hlavn%C3%AD_strana

http://en.wikipedia.org/wiki/Main_Page

Literární zdroje

Herman,I.: Komunikační technologie. Elektronické předlohy. FEKT VUT v Brně. 2006.

Doldi,L.: Validation of Communications Systems with SDL. The art of SDl Simulation and Reachability Analysis. John Wiley and Sons, England, 2003.

Lee A. Luft, Larry Anderson, Frank Cassidy: NMEA2000® A digital interface for the 21st Century