**ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE**
Fakulta elektrotechnická
Katedra telekomunikační techniky

# DIPLOMOVÁ PRÁCE

**2016** **Bc. Vítězslav Kříž**

**ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE**
Fakulta elektrotechnická
Katedra telekomunikační techniky

# Systém komplexního síťového dohledu a správy

Školní rok 2015 - 2016

Vypracoval: Bc. Vítězslav Kříž
Vedoucí práce: Ing. Pavel Troller, CSc.

## Čestné prohlášení

Prohlašuji, že jsem svou práci na téma „Systém komplexního síťového dohledu a správy“ vypracoval samostatně a uvedl jsem všechny použité zdroje a literaturu.

Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé práce nebo jejích částí se souhlasem katedry. V případě publikace práce nebo její významné části budu uveden jako spoluautor.

V Praze dne _____ _____

Podpis

České vysoké učení technické v Praze
Fakulta elektrotechnická

katedra telekomunikační techniky

# ZADÁNÍ DIPLOMOVÉ PRÁCE

Student: **Bc. Vítězslav Kříž**

Studijní program: Komunikace, multimédia a elektronika
Obor: Sítě elektronických komunikací

Název tématu: **Systém komplexního síťového dohledu a správy**

Pokyny pro vypracování:

Navrhněte systém, který bude proaktivně monitorovat a analyzovat provozní údaje ze síťových komponent společnosti 2N, distribuovaných u zákazníků, upozorňovat na závady, provádět pravidelné zálohy konfiguračních a provozních dat, distribuovat programové korekce a updaty a provádět další správní činnosti dle potřeby. Naprogramujte ve vybraném jazyce/vývojovém prostředí a implementujte webové rozhraní využívající otevřených standardů. Doporučeno řešit na platformě Linux.

Seznam odborné literatury:

[1] Nagios Enterprises, LLC.: *Monitoring Architecture Solutions For Managed Service Providers. Nagios - The Industry Standard in IT Infrastructure Monitoring*. 9/2011. [on-line].
[2] Levi, D. et al.: *Simple Network Management Protocol (SNMP) Applications*. 12/2002. Dostupné na http://www.ietf.org. [on-line].

Vedoucí: Ing. Pavel Troller, CSc.

Platnost zadání: do konce letního semestru 2015/2016


prof. Ing. Boris Šimák, CSc.
vedoucí katedry

prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 3. 12. 2015

**Anotace:**

Tato diplomová práce se zabývá popisem RM/OSI vrstev, protokolem M-Bus, Wireless M-Bus, SNMP, produkty 2N Telekomunikace a rozborem Raspberry Pi 2 či webovým serveren Apache. Cílem práce je naprogramovat webový konfigurátor s python skripty pro správu daných produktů.

**Klíčová slova:**

RM/OSI, TCP/IP, SNMP, M-Bus, WM-Bus, Python, HTML, jQuery

**Summary:**

This master thesis deals with RM/OSI layers, protocols M-Bus, Wireless M-Bus, SNMP, products 2N Telecomunication and Raspberry Pi 2 with Apache Web server. The goal of the master thesis is to make a web troubleshooting tool with python scripts.

**Index terms:**

RM/OSI, TCP/IP, SNMP, M-Bus, WM-Bus, Python, HTML, jQuery

## Poděkování:

Touto cestou bych chtěl poděkovat vedoucímu práce Ing. Pavlu Trollerovi, CSc., za jeho čas při pravidelných schůzkách. Dále bych mu chtěl poděkovat, za vedení při psaní práce a za zpětnou vazbu při realizaci praktické části.

## Obsah:

# 1 Úvod

Diplomová práce by měla obsahem navazovat na individuální projekt, který jsem absolvoval u mého vedoucího práce. Obsahem individuálního projektu bylo seznámení se s protokoly pro monitoring sítě, síťovou infrastrukturou a nástroji pro dohled prvků v síti, zejména program Nagios, který byl implementová v programu GNS3 a měl dohlížet na virtuální prvky v síti. Původním záměrem bylo pokračovat v implementaci různých python „plugynů“ do Nagiosu a měření různého chování prvků v prostředí GNS3. Bohužel jsem se potýkal s výpočetními problémy způsobenými prostředím GNS3 a také Virtualizací již zvirtualizovaného stroje v prostředí VirtualBoxu.

Díky mému působení ve firmě 2N jsem získal možnost pozměnit téma mé diplomové práce a místo vytvoření „umbrella“ řešení pro kontrolu prvků v síti bych rád vytvořil webovou stránku, která bude mapovat část portfolia 2N produktů. Daná stránka navazuje na můj projekt v tom smyslu, že bude sbírat informace, provádět restarty a stahovat informace z GSM bran a SmartCom Pro produktu určený pro M2M trh. Bude se jednat o jednoduchou stránku, kde si zákazník vybere produkt, který má připojený v síti, a následně skript, který by rád na jednou či více zařízení provedl. Tento jednotný design by měl být dále rozšiřitelný, což je výhodné pří přidávání dalších funkcí. Samotné výpočetní úkony by měly být programované v prostředí programovacího jazyka python.

V teoretické části bych se rád věnoval seznámení čtenáře s technologií internetu. Síťová technologie je nezbytnou součástí většiny moderních businessů, proto použiji již napsanou část z mého projektu k diplomové práci. Další důležitou částí bude popis jednotlivých technologií, které dané produkty použité v mojí webové aplikaci nabízejí. Pro brány je velmi důležitá VoIP technologie spojená se SIP protokolem a také PRI port využívající DSS1 signalizaci. Na druhou stranu SmartCom PRO podporuje M-Bus, Wireless M-Bus a další technologie. Za zmínku bude stát i SNMP protokol, který v dnešní době slouží pro monitoring sítě. Daný protokol nebude použit v praktické části, v oblasti monitoringu je ale velmi důležitý. Považuji tedy za velmi důležité čtenáře s danou problematikou seznámit. V mém projektu – příprava pro diplomovou práci jsem se seznámil například s programem Nagios, který daný monitoring protokol velmi využívá.

V dipolomové práci bych také rád rozebral použité jednotky. Každý ze zařízení 2N Telekomunikace funguje trochu jinak a čtenář by měl možnost dozvědět se něco o produktech. V praktické části by měla být naprogramovaná i „Help“ stránka. Tato pomocná stránka by měla uživateli lépe vysvětlit funkci, kterou si vybral, případně obsahovat odkazy, které uživatele budou přesměrovávat na dané stránky s podrobně popsanou problematikou.

Toto téma by mělo sloužit jako dočasné řešení pro firmu 2N Telekomunikace, než se dovyvine řešení pro M2M, která bude řešit právě online demonstrační sběr dat. V současnosti chybí demonstrační stránka v případě, že by zákazník provozoval například

více GSM bran a chtěl by se občas přihlásit na tento testovací polygon a získat informace z více bran najednou. To dnes není možné a můj projekt se pokusí tuto problematiku vyřešit.

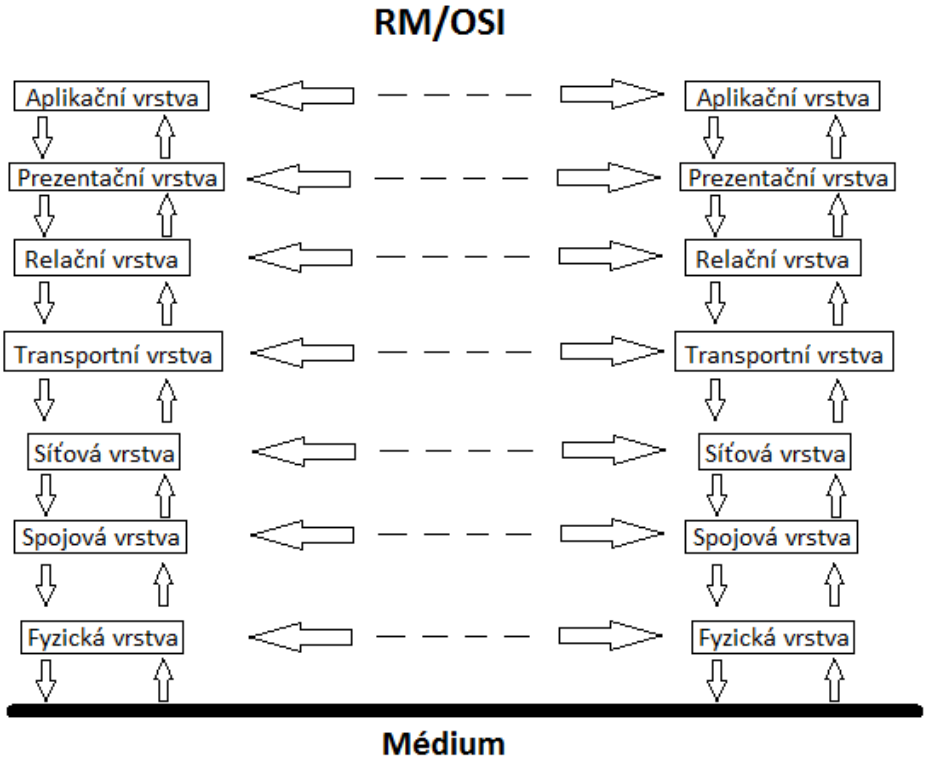
Toto téma diplomové práce považuji za velkou výzvu. V dnešní době se veškeré síťové projekty stávají více automatické a je tedy velkou výhodou naučit se některý skriptovací jazyk, který bude v dané práci použit.

# 2 Modely RM/OSI model a TCP/IP

Základní úlohou RM/OSI modelu je vytvoření norem pro propojování systémů. Norma žádným způsobem neříká, jaká bude realizace systémů, pouze je v ní uveden a definován princip síťové architektury. Tato architektura se skládá ze sedmi vrstev a každá vrstva plní určité funkce a služby, obsahuje základní typy protokolů pro možnou komunikaci mezi vrstvami a mezi systémy. V reálném provozu je však komunikace mezi vrstvami spojována do ucelených celků. Takový příklad je třeba TCP/IP, který má pouze čtyři vrstvy pro snadnější komunikaci mezi nimi.

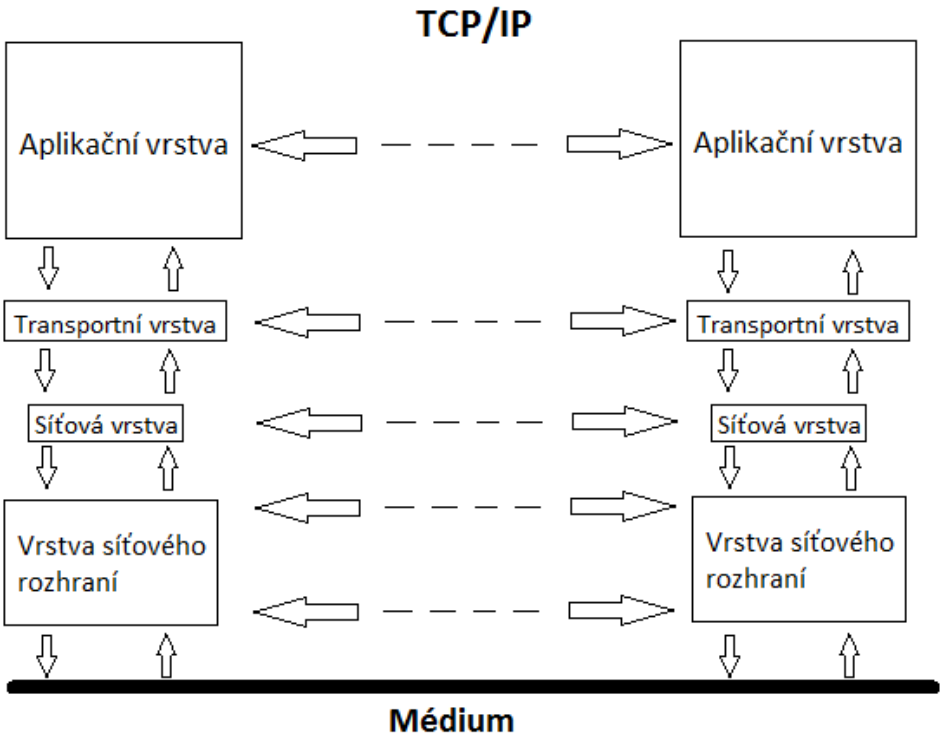
Vrstvy mohou komunikovat pouze se sousedními vrstvami. Žádná se nesmí přeskočit, ale může být neaktivní. Každá vrstva má přesně definované funkce při komunikaci. Dá se říct, že vrstva pro správnou komunikaci využívá vždy své nižší vrstvy a nabízí své funkce pro vrstvy vyšší. Druhou možností je komunikace mezi stejnými vrstvami různých systémů.

Komunikace je vždy vyvolána nejvyšší vrstvou a poté prochází všemi vrstvami až k nejnižší. V první fázi vznikne určitý funkční požadavek v aplikační vrstvě, která chce komunikovat s druhým systémem. Vznikne jisté množství dat, které je třeba přenést do druhého systému. Data propadají po vrstvách až k vrstvě fyzické, kde se přenesou pomocí signálu. V každé vrstvě se k datům přidávají užitečné informace (hlavička) a spolu s nimi se zabalují do specifického bloku dat. U příjemce se stejným způsobem data rozbalují až do nejvyšší vrstvy.




*Obr. 1: RM/OSI*

Model RM/OSI dobře znázorňuje demonstraci fungování komunikace mezi koncovými systémy. Jak bylo zmíněno výše, v reálném provozu se používá systém TCP/IP z důvodu větší efektivity. Má méně vrstev, protože jednotlivé vrstvy jsou sloučeny do jedné. Tak se děje v aplikační vrstvě, která v sobě obsahuje všechny tři vrstvy, tedy Aplikační, Prezentační a Relační vrstvu. Dále pak vrstva Síťového připojení spojuje jak vrstvu Spojovací, tak vrstvu Fyzickou.




*Obr. 2: TCP/IP*

## 2.1 Fyzická vrstva

Hlavní úloha fyzické vrstvy spočívá ve vytvoření, udržení a ukončení fyzického spojení mezi sousedícími systémy. Mezi nejznámější typy spojení patří point – to – point (dvoubodové spojení) a ethernet (mnohabodové spojení). Fyzická vrstva hlavně definuje všechny elektrické a fyzikální vlastnosti zařízení. Rozlišují se různé připojovací standardy, napěťové třídy, specifikace kabeláže. Fyzická vrstva má za úkol rozhodnout o způsobu přenosu datového toku – způsobu modulace a konverze digitálního signálu pro použité médium. Navazuje a ukončuje spojení s médiem.

Zařízení pracující na fyzické vrstvě jsou například huby, opakovače či síťové adaptéry, jejichž úkolem je pouze přeposílání a regenerace obdrženého signálu, potlačení šumu a další funkce.

## 2.2 Linková (spojová) vrstva

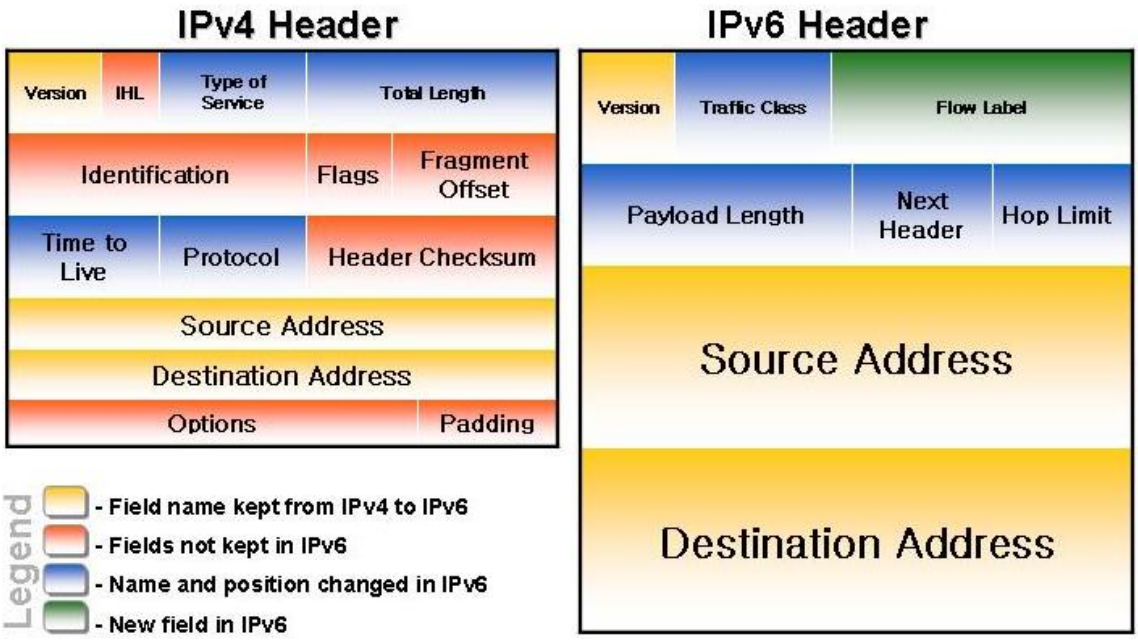
Oproti síťové vrstvě poskytuje spojová vrstva spojení mezi tzv. sousedícími systémy, převádí pakety do tzv. framů – rámců a umožnuje přístup k fyzickému médiu. V různých sítích je možné použít různé protokoly. Rozděluje se na dvě podvrstvy, MAC pro lepší komunikaci s fyzickou vrstvou, LLC pro přenos dat.

Jednou z hlavních funkcí MAC podvrstvy je přidělování fyzické adresy zařízením, seřazování rámců a synchronizování se s vrstvou fyzickou. LLC podvrstva detekuje a opravuje chyby, jež vznikly na fyzické vrstvě. Nejlepším příkladem je Ethernet, na lokálních sítích založených na IEEE 802 a některých na IEEE 802 sítích jako je FDDI.

Na této vrstvě pracují všechny switche a bridge.

## 2.3 Síťová vrstva

Síťová vrstva se stará o směrování a adresování sítí, zároveň zajišťuje komunikaci mezi nesousedícími systémy. Komunikace probíhá přeposíláním paketů. Obsahuje funkce pro přenos dat různé délky skrz několik vzájemně propojených sítí nebo funkce pro report. Na 3. vrstvě RM/OSI či 2. vrstvě TCP/IP modelu pracují dnes všechny směrovače - routery. Většina provozu je prováděna pomocí protokolu IP. V současné době je stále nejvíce využíván IP protokol verze 4 – IPv4, jehož adresa má 32 bitů. Do budoucna se počítá s verzí 6 – IPv6, která bude mít adresní rozsah 128 bitů, což představuje $3{,}4.10^{38}$ adres.




*Obr. 3: IPv4 vs IPv6*

IPv4 disponuje oproti IPv6 velkým množstvím polí, z nich jsou pro komunikaci nejdůležitější pole velikosti 32 bitů, a to Source, Destination Address. Každá IPv4 adresa se skládá ze 4 bloků velikosti 8 bitů, tedy 0 – 255. IP adresy rozdělujeme na adresy lokální, adresy multicast, a také se dříve vytvořil rozsah adres pro vědecké účely.

| Class | Leading bits | Size of *network number* bit field | Size of *rest* bit field | Number of networks | Addresses per network | Start address | End address |
|---|---|---|---|---|---|---|---|
| Class A | 0 | 8 | 24 | 128 ($2^7$) | 16,777,216 ($2^{24}$) | 0.0.0.0 | 127.255.255.255 |
| Class B | 10 | 16 | 16 | 16,384 ($2^{14}$) | 65,536 ($2^{16}$) | 128.0.0.0 | 191.255.255.255 |
| Class C | 110 | 24 | 8 | 2,097,152 ($2^{21}$) | 256 ($2^8$) | 192.0.0.0 | 223.255.255.255 |
| Class D (multicast) | 1110 | not defined | not defined | not defined | not defined | 224.0.0.0 | 239.255.255.255 |
| Class E (reserved) | 1111 | not defined | not defined | not defined | not defined | 240.0.0.0 | 255.255.255.255 |

Tab. 1: *IPv4 adresace*

Vše je shrnuto v tabulce 1, která ukazuje rozsah multicast adres, rozsah adres pro vědecké účely a také rozsah tříd A, B, C při dříve používaném třídním (classfull) adresování. Z důvodu nedostatku adres se začalo používat adresování beztřídní (classless), které šetří zejména adresy.

Veřejné adresy bohužel došly, a tak se začalo pracovat na ustavení nového standardu pro budoucí účely – IPv6. IPv6 přináší:

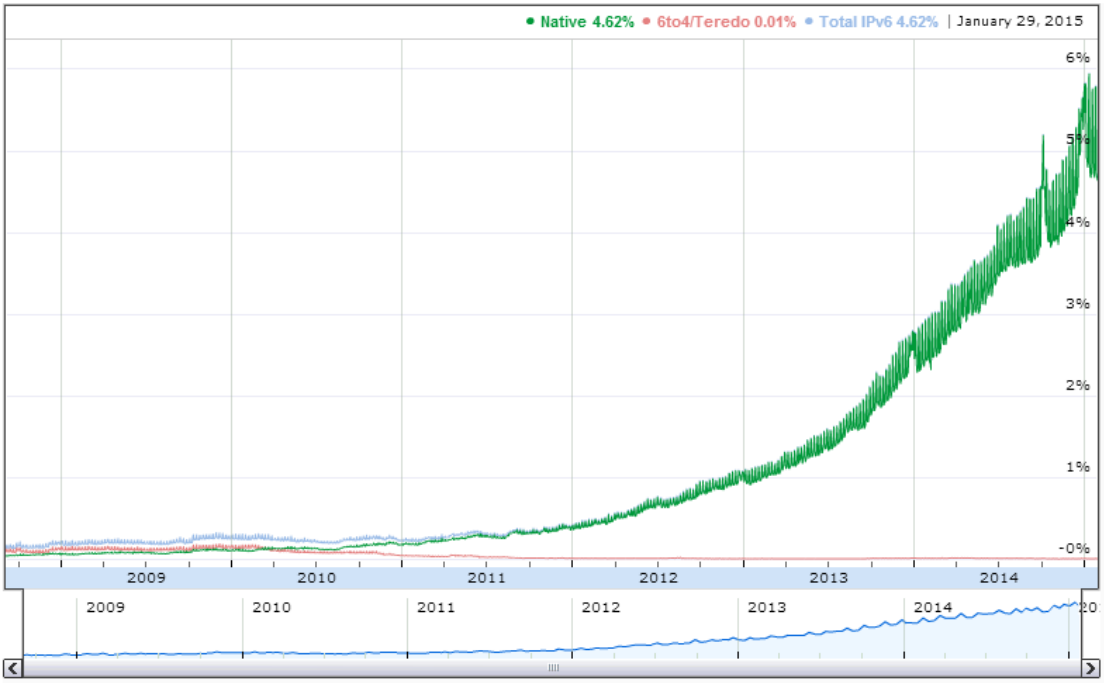
1) Nový rozsah, a to adresy o velikosti 128 bitů, a s nimi zavádí tzv. Anycast adresy, ULAs (*Unique Local IPv6 Unicast Addresses*) a CGAs (*Cryptographically Generated Address*).,

2) Zefektivnění a zjednodušení hlavičky – viz. Obr. 3, a díky tomu rychlé zpracování datových toků ve směrovačích. S tím je spojena i zákaz Hop – by - hop fragmentace, ale pouze End – to – end fragmentace + Path MTU – Discovery.

3) Další důležitou částí je ICMPv6, které nyní integruje všechny protokoly, jež dříve nebyly součástí ICMP, například ARP, IGMP. ICMPv6 zavádí Neighbor discovery pro automatickou konfiguraci IP adresy pro dané zařízení.

4) Podpora rozšiřujících hlaviček pro AH (Authentication header) a ESP (Encapsulation security payload) a další.

Nevýhoda IPv6 spočívá především ve větších režijních datech pro přenos informací a ty se mohou negativně podepsat například při přenášeních VoIP služeb. Na Obr. 5 je možné vidět datový tok v Internetu v dnešní době používající IPv6 hlavičky. Data jsou stažená z Google, dnešní datový provoz v Internetu tvoří IPv6 zhruba ze 4%.




*Obr. 4: IPv6 statistika*

## 2.4 Transportní vrstva

Transportní vrstva byla vytvořena pro přenos dat mezi koncovými uzly. Hlavním cílem je poskytnutí co možná nejlepší kvalita přenosu. Nejznámější protokoly na transportní vrstvě představují TCP a UDP protokoly.

TCP (Transmission Control Protocol) protokol je určen pro bezpečný, bezztrátový přenos. Jedná se o nejpoužívanější protokol využívaný v Internetu. TCP je považován za spojově orientovaný protokol, s důrazem na spolehlivost doručování jednotlivých datových prostředků. Využit je při sledování www stránek, přenosu souborů nebo čtení E-Mailů. Zejména tedy tyto protokoly HTTP, HTTPS, SNMP, POP3, IMAP, SSH, FTP či Telnet a mnohé další jsou enkapsulovány do TCP hlavičky. TCP pracuje s porty, což je jakási obdoba IP adres z třetí vrsty. Každá aplikace pracuje na určitém portu a daný požadavek určený port v TCP hlavičce obsahuje. Pokud chce klient A vytvořit TCP spojení s klientem B, který poskytuje webové služby, inicializije klient A TCP spojení s destination port 80 či 443, což odpovídá službám HTTP, HTTPS.

Porty dělíme na:

1) známé – well known v rozsahu 0 – 1023 (vyhrazené pro nejběžnější služby)

2) registrované porty – v rozsahu 1024 – 49151

3) dynamické a soukromé porty – v rozsahu 49152 - 65535

**TCP Header**

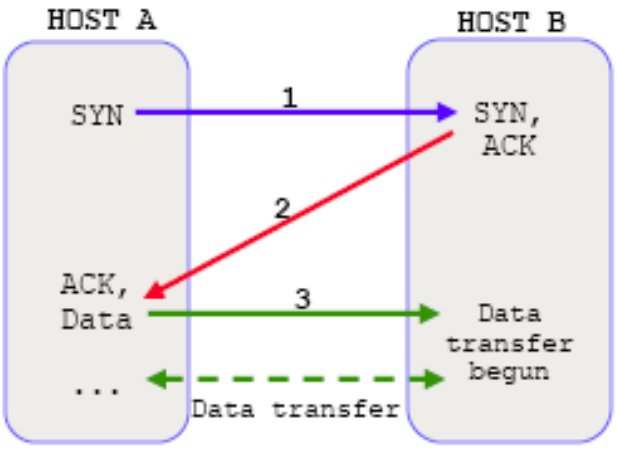
| Offsets | Octet | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Octet | Bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 0 | 0 | Source port | | | | | | | | | | | | | | | | Destination port | | | | | | | | | | | | | | |
| 4 | 32 | Sequence number | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | 64 | Acknowledgment number (if ACK set) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 12 | 96 | Data offset | | | | Reserved 0 0 0 | | | | NS | CWR | ECE | URG | ACK | PSH | RST | SYN | FIN | Window Size | | | | | | | | | | | | | | |
| 16 | 128 | Checksum | | | | | | | | | | | | | | | | Urgent pointer (if URG set) | | | | | | | | | | | | | | |
| 20 ... | 160 ... | Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

*Tab. 2: TCP hlavička*

Důležité vlastnosti, díky kterým se odlišuje TCP hlavička od UDP, jsou:

1) Uspořádaný datový přenos – datové rámce chodí ve správném pořadí (tato vlastnost je důležitá pro video a hlas)
2) Přeposlání ztracených paketů – při ztrátě rámců se TCP postará o jejich přeposlání. Důležité např. při prohlížení www stránek.
3) Flow control – používá se tzv. sliding window pro kontrolu. Díky window size se určí limit poslaných dat tak, aby došlo k největší efektivitě přenosu dat a jejich potvrzení pomocí ACK a nejmenší ztrátou dat.
4) Zajištění přeposlání dat bez chyb.

Známý je proces vytvoření spojení, kterému se také říká three – way handshake. Je to proces, kdy klient A žádá klienta B o utvoření TCP spojení. Tento proces zobrazuje obr. 5.




*Obr. 5: 3 – way handshake*

Klient A pošle SYN klientu B, ten pošle zpět ACK a zároveň pošle SYN klientu A, ten potvrdí ACK a může dojít k posílání dat.

Dříve to byl způsob, jakým se útočilo na veřejné servery, tomuto útoku se říká SYN flood attack. Infikovaná zařízení rozesílala na daný server požadavek na utvoření TCP spojení, server mu odpověděl SYN, ACK už se ale nedočkal zpětného potvrzení ze strany klienta. Pokud bylo těchto dotazů více, server již nebyl schopen odpovídat na nové požadavky a stal se nedostupným. Dnes se tento problém řeší například firewallem před daný server, který kontroluje provoz, který teče na daný server a pokud začína být server vytížen, začne TCP požadavky vyřizovat za server. Server po určité době nedokončené TCP dotazy smaže a stane se znovu plně dostupným.

Druhý protokol je UDP. Oproti TCP zajišťuje přenos dat bez zpětné záruky. Pokud vývojář použije pro svou aplikaci protokol UDP, musí počítat s tím, že se některá data mohou ztratit v přenosových sítích. Výhodou oproti TCP je však výrazné zrychlení. Toho se využívá hlavně při přenosu internetových rádií či pro streamovaná videa. V tabulce 3 je možno vidět UDP hlavičku, která oproti TCP obsahuje mnohem méně informací. Obsahuje pouze Source a Destination port, délku, která specifikuje v bytech UDP hlavičku a UDP data. Minimální délka je 8 bytů (délka hlavičky).

**UDP Header**

| *Offsets* Octet | | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Octet | 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 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 0 | 0 | Source port | | | | | | | | | | | | | | | | Destination port | | | | | | | | | | | | | | |
| 4 | 32 | Length | | | | | | | | | | | | | | | | Checksum | | | | | | | | | | | | | | |

*Tab. 3: UDP hlavička*

## 2.5 Relační vrstva

Relační vrstva se snaží o organizaci a spolupráci relačních vrstev obou systémů. Vytváří, udržuje a ukončuje relační spojení. Synchronizuje a obnovuje spojení. Mezi známé služby poskytované touto vrstvou mohou být zařazeny například AppleTalk, RPC, SSL.

## 2.6 Aplikační vrstva

Aplikační vrstva je označovaná jako 7. vrstva RM/OSI modelu. Hlavním úkolem této vrstvy je propojit aplikace a komunikační systémy, poskytnout aplikacím využití komunikačních systémů. Mezi hlavní protokoly v aplikační vrstvě dnes řadíme FTP, SSH, Telnet, POP3 a další.

# 3 Protokoly pro komunikaci

V této kapitole budou popsány nejpoužívanější protokoly, které naše produkty využívají v běžné komunikaci. V rámci dohledového systému je možno zvolit VoiceBlue Next, BlueTower/ Stargate či SmartCom. GSM brány umožňují komunikovat pomocí SIP aplikačního protokolu, BlueTower/ Stargate dále pak pomocí PRI portu využívající DSS1 komunikační protokol. SmartCom nabízí více rozhraní, pomocí kterých se dá připojit k periférii a vyčítat data. V této kapitole bude rozebrán M-Bus protokol a jeho bezdrátová varianta Wireless M-Bus, RS232, RS485 či ZigBee.

## 3.1 VoIP a SIP protokol

### 3.1.1 Představení VoIP, výhody a nevýhody VoIP

VoIP se považuje za velice perspektivní oblast telekomunikací současnosti a v současnosti je možné pozorovat rozšiřování VoIP technologie směrem k zákazníkům. Toto potvrzují i sítě NGN (Next Generation Network), které jsou právě na dané technologii postavené. Zkratka VoIP vychází z anglického názvu Voice over IP, tedy transport hlasového záznamu pomocí IP sítí.

Mezi velkou výhodu patří použití existující infrastruktury Internetu. Vzdálenost mezi jednotlivými stanicemi přestává mít smysl a uživatel A může komunikovat s uživatelem B na velkou vzdálenost za stejné náklady. Velkou výhodu také představuje tzv. autoprovisioning, tedy společná správa a konfigurace telefonů komunikujících po IP připojených do proxy PBX.

Jistou nevýhodou může být snaha poskytovatele Internetu upřednostňovat jiný datový provoz než hlas, protože z něj nemá žádný profit. Při vyšším datovém provozu se budou hlasové pakety zahazovat, a to vede k nižší kvalitě hlasu, nesrozumitelnosti atd., což je nevyhovující. V dnešní době lze za jistou nevýhodu považovat také vyšší cenu fyzických koncových IP telefonů, existuje však již spousta „softphonů“ či aplikací na smartphone.

### 3.1.2 SIP protokol

Session Initiation Protocol představuje signalizační protokol pro VoIP technologii, jehož úkolem je vyhledání volného účastníka, sestavení spojení (relace) mezi účastníky, vyjednání kodeků atd. S protokolem SIP je svázán RTP ( Real-time Transport Protocol) protokol zajišťující samotný přenos hlasu či videa. Obecně se dá říct, že protokol SIP se dá použít pro výměnu jakýchkoliv médií. Je definován pomocí IETF RFC a to konkrétně 3261 doplněný o další RFC definující další funkce. Konkrétně mezi nejznámější patří RFC 1889 pro RTP, RFC 2396 popisující URI adresu, RFC 2833 definující přenos DTMF značek a další.

Základním znakem SIP protokolu je to, že je textově orientovaný, komunikuje obvykle pomocí UDP protokolu a poslouchá na portu 5060. SIP signalizace umožňuje i

TCP spojení, která je doporučena při přenosu delších zpráv. Nejjednodušší případ komunikace je pomocí dvou SIP klientů, které spolu komunikují peer – to – peer. V tomto případě je jedno, jestli se jedná o fyzické či softwarové telefony. Stačí, aby jeden z nich znal IP adresu toho druhého a věděl, na jakém portu poslouchá. Pomocí tzv. URI ve tvaru sip: terminál@IP_adresa_terminálu je možné uskutečnit hovor. Klient A musí však znát IP adresu a číslo klienta B, což je dosti nepraktické. Díky tomu byla vyvinuta řešení s tzv. SIP registrary a SIP proxy servery. SIP registrar je server, který zajišťuje komunikaci bez nutnosti znát adresu volaného zařízení. Volá se pouze pomocí ID, což může být telefonní číslo, ale i registrační jméno klienta. SIP proxy zajišťuje směrování a řízení hovoru. Takový hovor však již není peer – to – peer, ale volání na proxy server. Většinou jsou obě tyto funkce obsažené v jednom serveru. Je dobré zmínit 2 typy terminálů, které rozlišujeme v SIPové komunikaci. UAC (user agent client) pro klienta a UAS (user agent server) pro server.

### 3.1.3 SIP zpráva

Daný obrázek ukazuje SIP Invite zprávu, která byla odeslána IP interkomem. Hlavička ukazuje základní pole, které SIP protokol využívá.

```
▷ Frame 655: 1132 bytes on wire (9056 bits), 1132 bytes captured (9056 bits) on interface 0
▷ Ethernet II, Src: 2nTeleko_01:24:5f (7c:1e:b3:01:24:5f), Dst: 2nTeleko_04:91 (00:50:c2:62:24:91)
▷ Internet Protocol Version 4, Src: 192.168.50.166, Dst: 192.168.50.100
▷ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
◢ Session Initiation Protocol (INVITE)
  ▷ Request-Line: INVITE sip:0733697644@192.168.50.100 SIP/2.0
  ◢ Message Header
    ▷ Via: SIP/2.0/UDP 192.168.50.166:5060;rport;branch=z9hG4bK1311730652
    ▷ From: "2N Helios IP Vario" <sip:vario@192.168.50.100>;tag=881408039
    ▷ To: <sip:0733697644@192.168.50.100>
      Call-ID: 1435445121
    ▷ CSeq: 20 INVITE
    ▷ Contact: <sip:vario@192.168.50.166:5060>
      Content-Type: application/sdp
      Allow: REGISTER, INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, NOTIFY
      Max-Forwards: 70
      User-Agent: 2N Helios IP Vario 2.13.3.22.6
      Content-Length:   605
  ▷ Message Body
```

*Obr. 6: hlavička SIP zprávy*

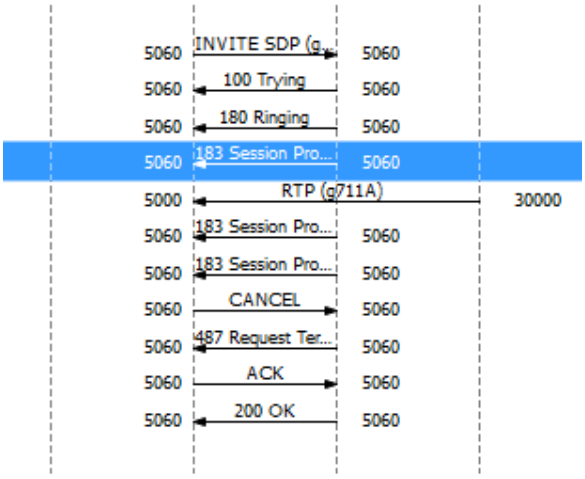
Via – reprezentuje přijímací IP adresu, port komunikace, řetězec
To – jméno, pokud je zadáno, a URI subjektu, pro který byl daný požadavek vygenerovaný
From – jméno, pokud je zadáno a URI subjektu, který daný požadavek vygeneroval
Call-ID – globální identifikace pro daný hovor
CSeq – sekvenční číslo, identifikace
Contact – kontakt, případně URI na daný subjekt, který požadavek vygeneroval
Max-Forwards – funguje jako TTL, tedy maximální počet hopů, přes který může daná správa být směrovaná

Content-Type – upřesnění obsahu těla zprávy
Content-Length – délka zprávy

V SIP signalizaci se objevuje více metod, které mohou být pozorovány v tracu. Jsou definované pomocí RFC 3261. Na obrázku 7 se objevuje metoda INVITE, která slouží k inicializaci hovoru. Dále je možné pozorovat REGISTER, který slouží pro registraci UAC k Registrar serveru. Metoda ACK slouží pro potvrzení.

Je možné se setkat s metodami jako je BYE, CANCEL nebo OPTION. Tyto metody obsahují kauzi odpovědí, které značí, v jakém stavu se daná signalizace zrovna nachází a zda je průběh komunikace v pořádku nebo někde došlo k chybě.

Mezi nejběžnější kódy odpovědí patří tyto kauzy:
**1xx**: Provisional – přijetí a zpracování požadavku
**2xx**: Succes – požadavek se úspěšně provedl
**3xx**: Redirection
**4xx**: Client Error – špatná syntaxe požadavku
**5xx**: Server Error – požadavek není možné splnit serverem
**6xx**: Global Failure – daný požadavek není možné splnit žádným serverem




*Obr. 7: Example of communication with PBX*

### 3.1.4 Kodeky a kvalitativní parametry

V současné době a vzhledem k dnes již snadno dostupným přenosovým rychlostem není VoIP technologie náročnou aplikací, co se propustnosti sítě týká. Jednak se na kvalitě daného hovoru projevuje datový tok 4 kbps – 64 kbps, ale také zpoždění paketů v síti či ztrátovost paketů. V doporučení ITU-T G.114 je definována hodnota tzv. roud - trip time či rout – trip delay, tedy maximální hodnota zpoždění, při které má člověk pocit, že ještě nedegraduje kvalitu hovoru. Jedná se o 300 ms, což odpovídá 150 ms jedním směrem. Už při zpoždění 250 ms v jednom směru je komunikace velmi nepříjemná.

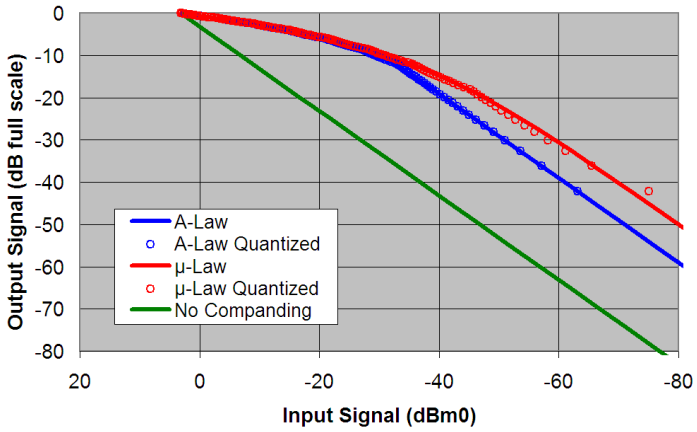
Ke zpoždění dochází všude, avšak ve většině případů se s daným zpožděním nedá nic dělat. Akustický signál je zdigitalizován a zakódován použitým kodekem. Poté je zabalen do paketů a odeslán do koncové destinace, kde dochází k opačnému procesu rozbalení a dekódování. Jak již bylo napsáno toto zpoždění je stálé a neměnné. Dá se manipulovat pouze se zpožděním dané sítě, a to například pomocí služby QoS, kde jsou dané VoIP pakety upřednostňovány v routerech před ostatním provozem. Toto upřednostňování funguje na základě jasných pravidel.

### 3.1.5 Kodeky

V prostředí VoIP se nejčastěji používá hybridní kódování, které kombinuje kódování tvaru vlny a parametrické kódování. Hovorový signál se segmentuje velikostí okna 20 ms a z nich se určí vhodná budící posloupnost a parametry filtru. Na principu hybridního kódování pracují třeba filtry CELP (Code Excited Linear Predictor).

Mezi nejzákladnější kodek patří kodek G.711, který je považován za základní kodek i v klasické telefonní síti. Použité kódování u kodeku G.711, pro převod analogového signálu na digitální, je PCM. Analogový signál je vzorkován frekvencí 8000 vzorků/ s a každý vzorek má 8 bitů. Z toho vychází šířka pásma 64 kbit/ s.

V dnešní době jsou používány dvě charakteristiky typu A (A-Law) a μ (μ-Law) ke kompresi/ expanzi signálu. A-Law účinně snižuje dynamický rozsah signálu, čímž se zvyšuje účinnost kódování. Tzv. „signal – to – distortion“ je lepší pro daný počet bitů než u μ-Law získané lineární kódování. Charakteristiky A-Law signálu se používají v Evropě a vychází z něj klasická rychlost E1. Oproti tomu μ-Law algoritmus poskytuje větší dynamický rozsah než A-Law na úkor horší „signal – to – distortion“ pro malé signály. Je používán v Americe a Japonsku.




*Obr. 8: A-Law, μ-Law*

Jak již bylo uvedeno, jedná se o nejzákladnější kodek v telekomunikacích ať už ve VoIP světě, tak i ISDN světě, a proto by ho měla většina zařízení podporovat. Často používaný kodek je kodek G.729, který používá kódování CS-ACELP (Conjugate

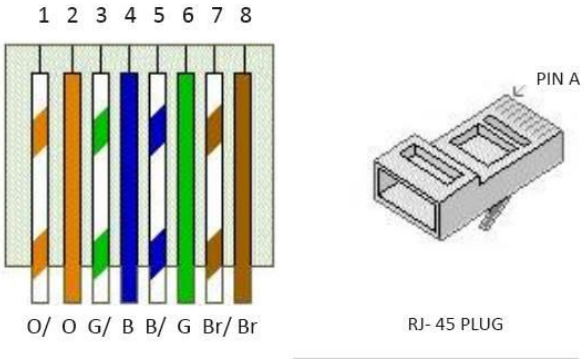
Structure Algebraic Code Excited Linear Prediction). Jeho přenosová rychlost však není 64 kbit/s ale 8 kbit/s. Je určen tedy pro sítě s menší kapacitou.

## 3.2 ISDN

ISDN znamená Integrated Services Digital Network, tedy Digitální síť integrovaných služeb nabízející plně digitální přenos mezi účastníky. Určen je hlavně pro přenos audia, ale také pro přenos videa či textu. V Evropě je zavedeno a implementováno EURO – ISDN zaručující shodnou implementaci v rámci celé Evropy.

Technologie ISDN nabízí dva typy připojení, BRI (Basic Rate Interface) a PRI (Primary Rate Interface). V této práci bude rozebráno PRI rozhraní, které nabízejí brány – 2N Stargate a 2N BlueTower. Ve světě jsou nejvíce rozšířené dva přístupy, a to 30B+D (Evropa a Austrálie) či 23B+D (Severní Amerika či Japonsko). Obě varianty nabízí kanál s propustností 64kbps. Evropská varianta tedy odpovídá toku E1 (2,048 Mbit/s) s tím, že nultý kanál je určen pro synchronizaci a 16. Kanál, tzv. D kanál, slouží pro přenos signalizace.

Pro přenos je použito 4 – drátové vedení zakončené klasickým RJ45 konektorem. Dvojici drátů odpovídá vždy daný směr. Maximální dosah se odhaduje kolem 1500m, pro běžný provoz se odhaduje hodnota kolem 1000m.



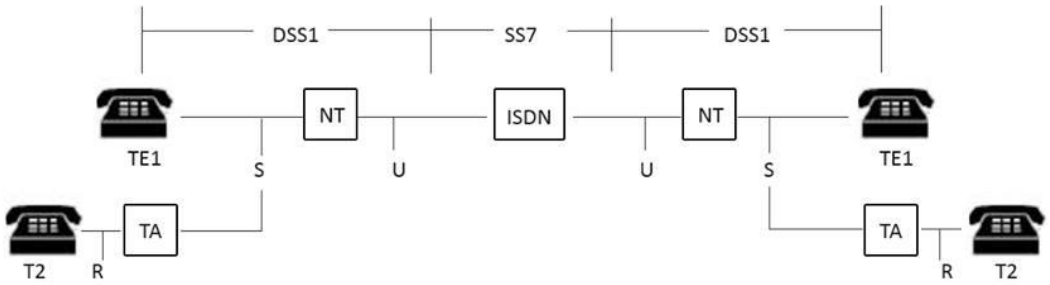

**TE mód**
Pin1, Pin2 - příjem
Pin4, Pin5 - vysílání
**NT mód**
Pin1, Pin2 - vysílání
Pin4, Pin5 - příjem

*Obr. 9: RJ-45 koncovka*

### 3.2.1 ISDN signalizace

V ISDN se používají různé typy signalizace. Pro přenos účastnické signalizace se nejvíce používá DSS1 (Digital Subscriber System No. 1), komunikace mezi ústřednami většinou u operátora zajišťuje SS7 (Signaling System No.7). DSS1 nabízí dva módy připojení, a to buď NT (Network Termination), která je většinou na straně operátora nebo TE (Terminal Equipment) na straně PBX.

Obrázek 10 znázorňuje rozdělení SS7 a DDS1. Je důležité zdůraznit, že každá ústředna disponuje vlastní proprietární signalizací umožňující spravovat příchozí hovory a transformovat je do jiné signalizace. V obr. je značená písmenem U.




*Obr. 10: Rozdělení komunikace*

### 3.2.1.1 Fyzická vrstva

Jak bylo vysvětleno v kapitole 2.1, fyzická vrstva řeší bitový přenos a jeho synchronizaci. Podrobněji je popsána v I.430 pro BRI a I.431 pro PRI. Pokud není aktivní fyzická vrstva, může být problém v konektorech, synchronizaci či špatném zapojení ve smyslu NT proti NT či TE proti TE. Platí, že vždy musí být jedna strana „master“ NT a druhá „slave“ TE.

### 3.2.1.2 Spojová vrstva

Spojová vrstva, často označovaná také jako L2, zajišťuje transformaci dat síťové vrstvy a jejich předání vrstvě fyzické. Jedním z dalších velmi důležitých úkolů je alokace D kanálů. Každé spojení se identifikuje pomocí DLCI identifikátoru, který obsahuje každý rámec. Jeho hlavní funkcí je detekce chyb a jejich oprava. Ty, které opravit nejdou, jsou hlášeny řídící entitě. Protokol spojové vrstvy u D – kanálu se jmenuje LAP – D (Link Access Procedure on the D – Channel).

Spojová vrstva poskytuje jak potvrzené, tak i nepotvrzené zprávy. Pro potvrzené zprávy se používá rámec HDLC (High Definition Link Control) a jsou číslovány. V DSS1 existují dva formáty rámců. První formát neobsahuje informační pole, slouží pro řídící a dohledové služby. Druhý formát slouží k přenosu signalizační zprávy ze třetí vrstvy. Ve spojové vrstvě je možné se také setkat s TEI (Terminal Endpoint Identifier). Jedná se o číslo definující konkrétní terminál v rámci daného rozhraní.

### 3.2.1.3 Síťová vrstva

Síťová vrstva (L3) umožňuje sestavit spojení využívajíc k tomu L2. Přenášená data jsou chráněna pomocí algoritmů pro detekce chyb. Síťová vrstva zajišťuje sestavení, ruší spojení ve spojové vrstvě, přiděluje a ruší TEI. Její funkcí je i řízení přenosu zpráv.

### 3.2.2 DSS1

Účastnická signalizace DSS1 je binární signalizace, která se přenáší pomocí D kanálu. Slouží zejména k sestavení a ukončení hovoru. ISDN je síť s přepínáním okruhů, cesta je nejdříve sestavena pomocí signalizace, dále dochází k rezervaci kanálů, a ten je využíván po celou dobu hovoru. DSS1 umožňuje posílat zprávy vztahující se k hovoru, příkladem takové zprávy může být například tarifikace. Díky tomu, že jde o síť s přepínáním okruhů, mají tyto zprávy vždy lokální platnost a nejsou přenášeny od uživatele k uživateli. Zprávy je možné rozdělit do více kategorií v závislosti na jejich použití.

#### 3.2.2.1 Nejdůležitější zprávy používané v signalizaci DSS1

**Alerting** – Volaný uživatel je vyzváněn. Tato zpráva je posílána volajícím síti či sítí volanému.

**Call Proceeding –** Sestavení hovoru bylo zahájeno, další dodatečné zprávy/ informace k hovoru budou zamítnuty. Směr zprávy je zde opačný než u Alerting zprávy, tedy volaný posílá zprávy síti a síť volajícímu.

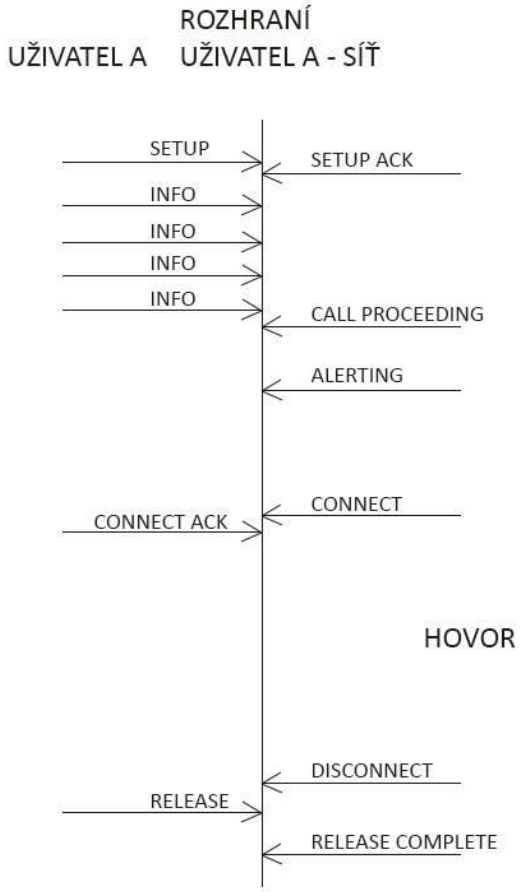
**Connect** – Signalizace přijetí hovoru voláným uživatelem. Směr je v tomto případě totožný s Alertingem. Na tuto zprávu přijde odpověď ACK v opačném směru.

Mezi další důležité zprávy při sestavení hovoru patří **Progress** či **Setup, Setup ACK**, které slouží pro zahájení sestavení hovoru a jeho potvrzení. Za nejdůležitější zprávy v informační fázi hovoru lze považovat **Resume** či **Suspend.**

**Resume** – Zpráva pro pokračování přidržení hovoru odeslána uživatelem k síti. Jako odpověď dostane uživatel **Resume ACK** či **Resume Reject** a to buď potvrzení přidržení, či upozornění na chybu požadavku Resume.

**Suspend** – Zpráva pro přidržení hovoru odeslána uživatelem k síti. Tak jako v minulém případě jsou zde možné obě odpovědi, a to **Suspend ACK** či **Suspend Reject**, které i významově odpovídají předchozímu popisu.

Nejdůležitější zprávy, které signalizace DSS1 používá pro ukončení hovoru, je zpráva **Disconnect**, která je odeslána uživatelem k síti. Jedná se o požadavek na ukončení spojení a uvolnění kanálu. Tato zpráva může být přijata i opačně, a to jako informační zpráva ze sítě o tom, že bylo dané spojení ukončeno. Zpráva **Release** signalizuje rozpojený kanál. Uživatel nebo síť, která poslala danou zprávu, se bude snažit uvolnit kanál a referenční číslo hovoru. Jako odpověď na Release je poslána zpráva **Release Complete,** což znamená, že i druhá strana uvolnila kanál a referenční číslo hovoru.




*Obr. 11:DSS1 zprávy*

## 3.3 M-Bus protokol

Protokol M-Bus (Meter-Bus) byl původně vyvinut jako nový evropský standard pro vzdálené odečty „heatmeters“, tedy měřičů tepla. Dá se ale také použít jak pro ostatní typy čítačů, tak i různých senzorů a akčních členů, kde není zásadní rychlá odezva v čase *„V praxi je možno si představit oblasti měření a regulace topných systémů, plynu, odběru vody a elektrické energie.“* M-Bus rozhraní musí splňovat velké specifické nároky, musí umět připojit velké množství zařízení na velké vzdálenosti. Jedná se až o jednotky kilometrů. Velký důraz je kladen na minimalizaci chybovosti, která se může při velkých vzdálenostech objevit.

Jak již bylo psáno, slouží M-Bus protokol pro vyčítání hodnot například z vodoměrů a podobně. Toto vyčítání naměřených hodnot nebývá velmi časté a nemá příliš velké nároky na latenci. Přenosové rychlosti u M-Bus jsou do 9600Bd. Tento dosavadní výčet vlastností umožnil implementaci protokolových vrstev OSI modelu programově.

***Základní vlastnosti rozhraní M – Bus:***

- *Na základě uvedených vlastností speciální implementace fyzické vrstvy*
- *Galvanicky oddělené rozhraní*
- *Možnost napájení po sběrnici*
- *Dosah až několik kilometrů, dvoulinka*
- *Komunikace Master – Slave*
- *Maximální počet uživatelů až 250*
- *Sudá polarita, 8 bitů, asynchronní přenos*
- *Přenosová rychlost 300 až 9600 Bd*
- *Zabezpečení pomocí kontrolního součtu*

Standart M-Bus používá pro komunikaci sběrnici. Všechna zařízení jsou spojena na jednotné sběrnici, toto s sebou nese výhodu připojování a odpojování jednotlivých zařízení bez omezení komunikace zbylých stanic.

| Layer | Functions | Standard | Chapter |
|---|---|---|---|
| Application | Data structures, data types, actions | EN1434-3 | 6 |
| Presentation | empty | | |
| Session | empty | | |
| Transport | empty | | |
| Network | extended addressing (optional) | - | 7 |
| Data Link | transmission parameters, telegram formats, addressing, data integrity | IEC 870 | 5 |
| Physical | cable, bit representation, bus extensions, topology, electrical specifications. | M-Bus | 4 |

| MANAGEMENT LAYER | |
|---|---|
| Application Layer | |
| Presentation Layer | |
| Session Layer | |
| Transport Layer | |
| Network Layer (if address = 253) | Address 253 / Enable Disable CI=$52/$56 |
| Data Link Layer | |
| Physical Layer | Address 254 (255) |

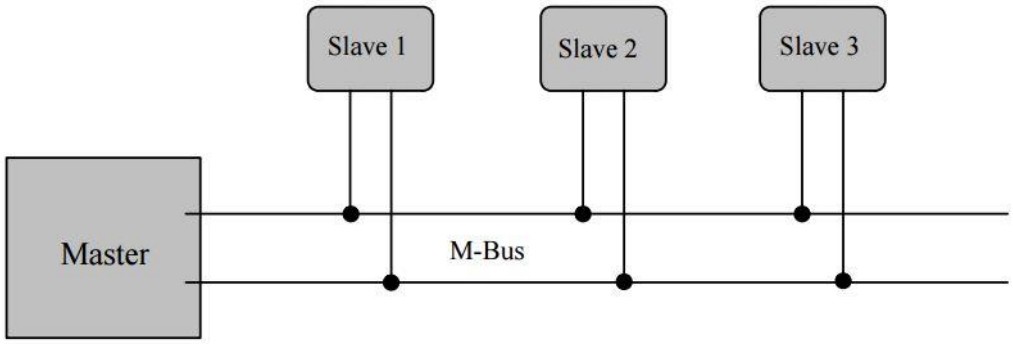
*Obr. 12:Vrstvy M-Bus protoku*

Samotný OSI model M-Bus rozhraní nejvíce používá fyzickou, spojovou a aplikační vrstvu. Ostatní vrstvy OSI modelu nejsou využity, protože M-Bus není implementován v síti, a tak těchto vrstev není potřeba. Místo toho je implementována tzv. „Management Layer“, která je vidět na obrázku 12. Adresy 254 a 255 jsou rezervované pro správu fyzické vrstvy a adresa 253 pro vrstvu třetí, a to pouze v určitých případech. S touto novou vrstvou - „Management Layer“ je možno přímo řídit každou OSI vrstvu v případě implementace nových prvků, které plně nevyhovují klasickému OSI – modelu.

### 3.3.1 Fyzická vrstva

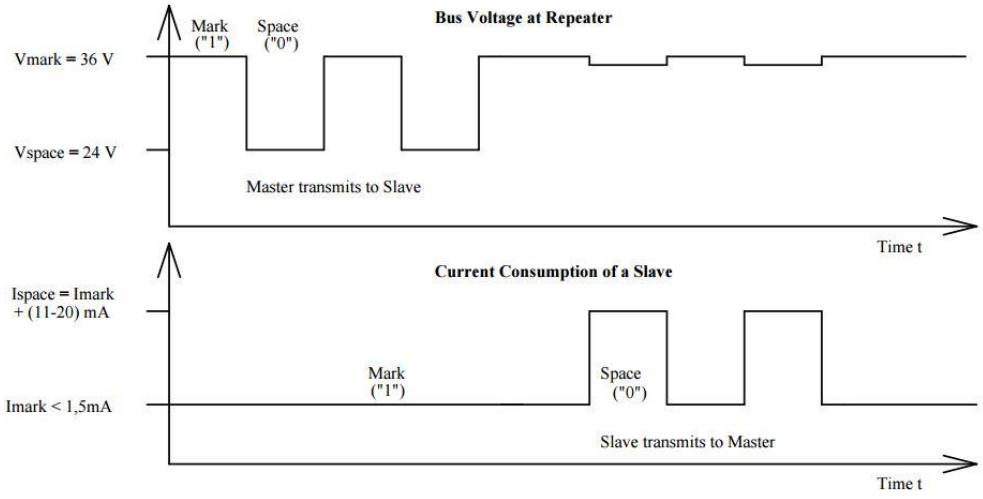
M-Bus je systém, ve kterém jednotlivá zařízení komunikují po sběrnici. Komunikace je kontrolována jedním masterem „(Central Allocation Logic)“ a větším

počtem účastnických stanic – Slaves spojených pomocí klasické dvojlinky, což představuje obrázek 13.




*Obr. 13: M-Bus zapojení*

K dosažení rozsáhlé sběrnicové sítě s nízkými náklady na přenosové médium byl použit telefonní kabel, tzv. dvojlinka, ve spolupráci s rozhraním RS232. Co se týká napájení účastnických stanic, jsou jednotlivé bity na bus sběrnici reprezentovány podle obr. 14. Přenosy bitů od master jednotky k Slave jednotce je dosaženo pomocí změny napěťové úrovně. Logická "1" odpovídá jmenovitému napětí +36 V na výstupu Bus ovladače (repeater), který je součástí master jednotky. Pro logickou "0" je napětí sníženo o 12 V na +24 V na výstupu. Bity zasílané ve směru od Slave k Master jsou kódovány modulací aktuální spotřeby Slave jednotky. Logická "1" je reprezentována konstatním proudem do 1,5 mA, a to bez ohledu na napětí, teplotu či čas. Logická "0" pak zvýšeným proudem o 11 – 20 mA. Takto je možno napájet daný měřák či senzor a zároveň komunikovat po daném rozhraní.




*Obr. 14: Logické stavy M-Bus*

Přenos logické "0" Slave jednotkou má za následek snížené napětí na sběrnici Repeateru vzhledem k výstupní impedanci. To je možné pozorovat na obrázku 16. Klidový stav nastává, když je na sběrnici v logické "1", tj. sběrnice má napětí +36 V na

Repeateru. Za těchto podmínek jsou Slave jednotky napájeny klidovým proudem max. 1,5 mA pro každou z nich. Pokud Slave posílá logickou “0“, konstatní proud je vysílán z Master a napájí bus. Důsledkem tohoto chování je napětí pro logickou “1“ u Master nižší než +36 V v závislosti na vzdálenost mezi Masterem a Slavem. Slave proto nesmí rozpoznat absolutní napěťové úrovně, ale místo logické “0“ detekovat snížené napětí o 12 V. Repeater sebe přizpůsobí ke klidové hodnotě proudu (“1“) a interpretuje zvýšený proud na busu o 11 – 20 mA jako reprezentaci logické “0“. Toho lze dosáhnout s přijatelnou složitostí pouze tehdy, když je logická “1“ definována jako +36 V, tj., že v každém okamžiku je přenos možný pouze v jednom směru - ať už z master do slave, nebo slave na master (half duplex).

Díky tomuto chování, tzn. přenos ve směru Master-Slave se změnou napětí o 12 V a v opačném směru se změnou alespoň o 11 mA, bylo dosaženo vysokého stupně citlivosti na vnější rušení.

### 3.3.2 Linková vrstva

Fyzická vrstva vytváří určité požadavky na vrstvu Linkovou. Kromě toho, že se jedná o poloduplexní asynchronní sériový přenos s rychlostí přenosu dat mezi 300 a 9600 Baud, kde minimálně každý jedenáctý bit odpovídá logické “1“, tak by popsaná struktura měla být Master-Slave. Jednotlivé Slave jednotky spolu nemohou navzájem komunikovat. Protokol Linkové vrstvy je založen na mezinárodní normě IEC 870-5, která definuje protokoly přenosu pro dálková ovládání zařízení a systémů. V ní jsou uvedeny tři rozdílné telegramy lišící se startovacími znaky.

Podle IEC 870-5 jsou dnes chápány tři různé třídy integrity dat (I1, I2 a I3) pro přenos dálkově vyčítaných dat. Třída integrity je kvocient mezi mírou nezjištěných falešných zpráv a pravděpodobností chybných bitů v průběhu přenosu. Pro výše uvedené třídy integrity dat jsou dnes používány různé formáty dat. Pro M-Bus protokol je v linkové vrstvě použit formát třídy FT 1.2, která je obsažena v datech integrity class I2. Formát třídy FT 1.2 určuje čtyři různé komunikační rámce, které mohou být rozpoznány pomocí speciálních znaků. Jednotlivé rámce jsou popsány níže.

| Jednotlivý znak | Krátký rámec | Kontrolní rámec | Dlouhý rámec |
|---|---|---|---|
| E5h | Start 10h | Start 68h | Start 68h |
| | Pole C | Pole L = 3 | Pole L |
| | Pole A | Pole L = 3 | Pole L |
| | Kontrolní suma | Start 68h | Start 68h |
| | Stop 16h | Pole C | Pole C |
| | | Pole A | Pole A |
| | | Pole CI | Pole CI |
| | | Kontrolní suma | Uživatelská data (0 - 252 bytů) |
| | | Stop 16h | Stop 16h |

*Tab. 4: M-Bus rámce*

- *Jednotlivý znak*
- *Krátký rámec*
- *Kontrolní rámec*
- *Dlouhý rámec*

V tabulce 4 jsou zobrazeny jednotlivé rámce spolu s jednotlivými znaky. Každý znak obsahuje konkrétně 0xE5h a je použit jako potvrzující zpráva. Krátký rámec má fixní délku začínající vždy úvodním znakem 0x10, následují pole C a A, kontrolní součet a Stop znak 0x16. Pole C a A budou popsány níže. Dlouhý rámec obsahuje úvodní znak 0x68, následně je dvakrát posláno pole L. Za dvojicí polí L obsahuje dlouhý rámec znovu úvodní znak 0x68. Následně je odesláno funkční pole C, adresové pole A a kontrolní informační pole CI, uživatelská data (0 – 252 bytů), kontrolní součet a ukončovací znak 0x16. Kontrolní rámec svým obsahem odpovídá dlouhému rámci. Neobsahuje pouze uživatelská data, která se přenáší. Kontrola je počítána z polí C, A a CI.

**Pole A**

Pole A, adresové pole, slouží k adresaci příjemce při vysílání rámce a identifikaci odesílatele při příjmu rámce. Velikost daného pole je 1 byte a z toho vycházející rozsah adres 0 – 255. Adresy 1 až 250 mohou být přiřazeny jednotlivým Slavům. Nepřihlášený Slave má z výroby defaultní adresu 0 a jakmile se připojí k M-Bus, tak si alokuje jednu adresu z daného rozsahu. Speciální adresy 254 (0xFE) a 255 (0xFF) jsou použity pro distribuci zpráv všem účastnickým stanicím (Broadcast). Rozdíl mezi 254. a 255. adresou spočívá v tom, že při poslání zprávy s adresou 254 odpoví všechny účastnické

stanice a při použité adrese 255 neodpoví nikdo. Při potvrzovacím broadcastu je zřejmé, že na sběrnici dojde ke kolizím. Slouží tedy pouze pro testovací účely. Adresa 253 (0xFD) indikuje adresaci v síťové vrstvě. Adresy 251 a 252 jsou uchovány pro budoucí účely.

**Pole C**

Funkce pole C, kontrolní pole, specifikuje směr toku dat, je zodpovědné za další úkoly v obou směrech komunikace. V tabulce 5 je ukázáno kódování individuálních bitů v C poli.

| Číslo bitu | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| Vyslání | 0 | 1 | FCB | FCV | F3 | F2 | F1 | F0 |
| Příjem | 0 | 0 | ACD | DFC | F3 | F2 | F1 | F0 |

*Tab. 5: Pole C – kódování jednotlivých bitů*

Bit s nejvyšší hodnotou je rezervován pro budoucí funkce. V tabulce je prezentován hodnotou 0. Bit 6 je použit k určení směru toku dat. FCB (Frame Count Bit) vysílaném na 5. pozici řídící stanicí je indikován při bezchybné komunikaci. Při posílání daného bitu se střídá log. 0 a log. 1 tak, aby byla zamezena ztráta při přenosu. Pokud řídící stanice nedostala potvrzení na předchozí rámec, vyšle daný rámec znovu se stejným FCB bitem. Bit FCV (Frame Count Valid) definuje, zda je FCB platné či nikoliv. Pokud posílá řídící stanice FCV jako logickou 1, znamená to, že FCB má být zohledněno a bráno v úvahu. Při log. 0 je bit FCB ignorován.

Bity signalizující Slavem v pozici 5 a 4 mají jiný význam než pro Master. Bit ACD (Access Demand) signalizuje Masteru, že daná účastnická stanice má data s vyšší prioritou, které potřebuje přeposlat. Tato data obecně mají být poslána ihned, jak se uvolní pásmo. Bit DFC (Data Flow Control) slouží k řízení datového toku tak, jak již název napovídá. Log. 1 říká řídící stanici, že Slave nyní není schopen akceptovat další data. Po změně na log. 0 dává účastnická stanice najevo, že je již schopna přijímat další data. Podpora Class 1, bitů DFC a ADC není nijak vyžadována normou. Bity F0, F3 kódují vlastní účel zprávy.

**Pole CI**

Kontrolní informační pole nese informaci, která je již součástí aplikační vrstvy. Více bude uvedeno v kapitole pro aplikační vrstvu.

### 3.3.3 Síťová vrstva

Z výše popsaných vlastností pole A v linkové vrstvě je znám daný adresový rozsah 1 – 250 Slavů. Pokud by však došlo k situaci, že primární rozsah 250 adres nestačí, je možno implementovat síťovou vrstvu. Není možné, aby daná účastnická stanice měla neustále adresu na hodnotě 0. V takovém případě je automaticky nastavena hodnota linkové vrstvy na hodnotu 253 a použije se rámec pro přiřazení sekundární adresy, který je možné vidět v tabulce 6. Daná sekundární adresa se skládá z více částí. Jedná se o identifikační číslo, výrobce, verzi a použité médium. Účastnická stanice pak komunikuje v linkové vrstvě s adresou 253 a odlišuje se právě těmito nastavenými parametry. V případě, že se nějaká adresa uvolní, dostane danou jednotku konkrétní účastnické stanice.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 68h | 0Bh | 0Bh | 68h | 53h | FDh | 52h | 1D1-4 | Man 1-2 | Gen | Med | CS | 16h |

*Tab. 6: Rámec pro sekundární adresu*

### 3.3.4 Aplikační vrstva

Standardizovaný aplikační protokol podle standardu EN1434 – 3 definuje význam pole CI a výměnu uživatelských rámců. Tento standart je použitelný pro komunikaci s tepelnými měřidly a dalšími spotřebitelskými metry pro plyn a vodu. Standart EN1434-3 pouze mapuje datovou strukturu v příchozím směru, tedy od Slave k Master jednotce.

**Pole CI**

Pole CI (Control Information Field) definuje v rámci sekvence aplikačních dat a typ, který mají být odeslána. Standart EN1434 – 3 definuje dvě možné datové sekvence ve vícebytovém záznamu. Druhý bit (0x04), který je nazýván M bitem nebo „Mode“ bitem, nese informaci o bytové sekvenci ve vícebytových datových strukturách. Pokud je nastaven Mode2, nejvýznamnější bity multibytového záznamu jsou přeneseny jako první. V logické 0, což odpovídá „Mode 1“, je tomu naopak. Obecně se doporučuje používat pouze „Mode 1“.

Následná tabulka 7 ukazuje zprávy posílané řídící stanicí doplněná tabulkou 8 obsahující zprávy poslané účastnickou stanicí.

Mezi velmi důležitou součást patří velikost pole uživatelských dat. Z tabulky 4 pro Dlouhý rámec vychází pro Dlouhý rámec uživatelská data 0 – 252 bajtů. Tato uživatelská data přenáší naměřená data daného přístroje. Je definováno několik možností, jak dané pole může vypadat. Mezi nejznámější patří Pole uživatelských dat s pevnou strukturou, Pole uživatelských dat s proměnnou strukturou. Tyto formáty jsou více popsány ve standardu M – Bus.

| Mode 1 | Mode 2 | Application | Definition in |
|---|---|---|---|
| 51h | 55h | data send | EN1434-3 |
| 52h | 56h | selection of slaves | Usergroup July '93 |
| 50h | | application reset | Usergroup March '94 |
| 54h | | synronize action | suggestion |
| B8h | | set baudrate to 300 baud | Usergroup July '93 |
| B9h | | set baudrate to 600 baud | Usergroup July '93 |
| BAh | | set baudrate to 1200 baud | Usergroup July '93 |
| BBh | | set baudrate to 2400 baud | Usergroup July '93 |
| BCh | | set baudrate to 4800 baud | Usergroup July '93 |
| BDh | | set baudrate to 9600 baud | Usergroup July '93 |
| BEh | | set baudrate to 19200 baud | suggestion |
| BFh | | set baudrate to 38400 baud | suggestion |
| B1h | | request readout of complete RAM content | Techem suggestion |
| B2h | | send user data (not standardized RAM write) | Techem suggestion |
| B3h | | initialize test calibration mode | Usergroup July '93 |
| B4h | | EEPROM read | Techem suggestion |
| B6h | | start software test | Techem suggestion |
| 90h to 97h | | codes used for hashing | obsolete and no longer recommended |

| CI M=0 | CI M=1 | Application | Defined in |
|---|---|---|---|
| 70h | | report of general application errors | Usergroup March '94 |
| 71h | | report of alarm status | Usergroup March '94 |
| 72h | 76h | variable data respond | EN1434-3 |
| 73h | 77h | fixed data respond | EN1434-3 |

*Tab. 7, 8: Pole CI, právy poslané účastnickou stanicí*

## 3.4 Wireless M-Bus

Wireless M-Bus představuje bezdrátovou verzi specializovaného protokolu M-Bus pro přenos dat, který je primárně určený pro vodoměry, měřidla tepla a elektroměry. Tato verze realizuje přenos dat vzduchem a to s sebou nese některé výhody oproti klasické drátové verzi, například snadnější instalaci a možnosti rozšíření. Oproti klasické drátové verzi se Wireless M-Bus liší v prvních dvou vrstvách OSI modelu, které se díky jinému použitému médiu liší.

Wireless M-Bus je kompatibilní s mezinárodním ISO/ OSI modelem, pouze vrstvy 1,2 a 7 jsou řádně implementovány.

| | |
|---|---|
| Vrstva 7 | Aplikační vrstva (EN 13757 - 3) |
| Vrstva 2 | Linková vrstva (EN 13757 - 2 nebo EN 13757 - 4) |
| Vrstva 1 | Fyzická vrstva (EN 13757 - 2 nebo EN 13757 - 4) |

*Tab. 9: Wireless M-Bus vrstvy*

Aplikační vrstva implementuje všechny ostatní vrstvy protokolu požadované pro konkrétní použití, a to i v případě routování, které se řeší ve 3. vrstvě. Takto snížená modularita vede ke kompaktní implementaci provozované na velmi malém zařízení s minimálními výpočetními prostředky. Zároveň je však důvodem, proč daný protokol nenabízí routovací protokoly. Obecně M – Bus cílí na asymetrickou topologii sítě s nízkonákladovými a nízko energeticky náročnými měřidly na jedné straně a sběrnice dat s vyšším výkonem na straně druhé. V současné době mohou být podporovány

pouze point – to – point nebo hvězdicové topologie sítě. Topologie Mesh nebo vícestupňové topologie nejsou zatím možné.

### 3.4.1 Režimy rádiového přenosu

Protokol Wireless M – Bus definuje několik režimů S, T a R. Každý z těchto režimů reprezentuje určitou přenosovou rychlost. Ve specifikaci je dále provoz dělen na 1 či 2. Toto označení dělí přenos dat na jednosměrný nebo obousměrný. Podrobně jsou dané rychlosti popsány následující tabulce 10.

| Přenosová rychlost | Označení jednocestné komunikace | Označení dvoucestné komunikace |
|---|---|---|
| 4,8 kb/s | neexistuje | R2 |
| 32,768 kb/s | S1/ S1m | S2 |
| 100 kb/s | T1 | T2 |

*Tab.. 10: Rádiové přenosy*

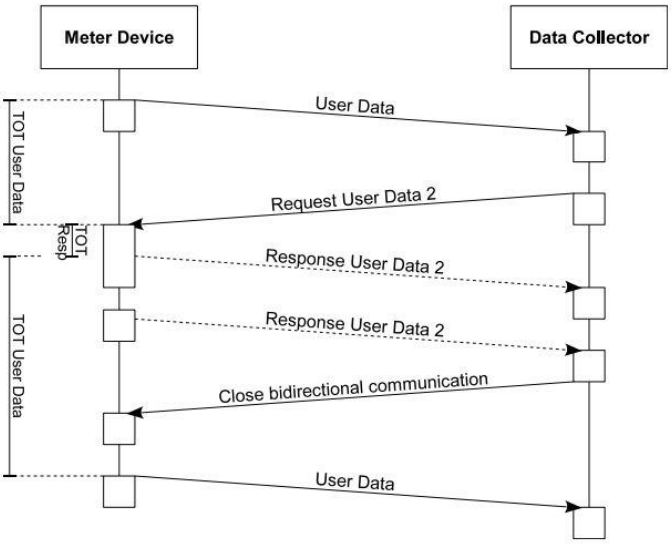
Tabulka dále demonstrativně deklaruje jednotlivé přenosové rychlosti a režim komunikace. Režim komunikace T1 je vhodný pro přenos datových informací od měřičů a vodoměrů, jedná se pouze o jednosměrnou komunikaci. Oproti tomu T2 režim je určen pro dvoucestnou komunikaci, která se zobrazuje mimo čtení i přenos naměřených dat od uživatelských stanic. Je možné i zpětné ovládání aktivních členů. Při vývoji byl režim T1, T2 chápán jako režim s častým přenosem. Pro snížení požadavků na energii byly režimy T navrženy tak, že se přenos aktivuje po krátkou dobu a díky vyšší rychlosti se přenesou veškerá data. Oproti T1, T2 jsou režimy S1, S2 pomalejší. Nabízí 32,768 kbps. Využití najdou v systémech, kde je třeba poslat pravidelně malý objem dat.

Využití režimu R2 je spíše ve speciálních případech. Již z dané přenosové rychlosti je zjevné, že bude použit v případě velmi malého množství dat. Díky malé rychlosti, byl v tomto režimu kladen velký důraz na citlivost příjmu signálu. Oproti režimům S a T je R nejlepší pro přenos na velkou vzdálenost.

### 3.4.2 Rádiová komunikace

Protokol Wireless M – Bus využívá 12 kanálů v pásmu ISM. Toto pásmo není nikterak licencované. Frekvenční rozsah je udáván mezi 868 MHz až 870 MHz, konkrétně pak frekvenční pásmo 868,30 MHz pro S1, S2 i T1, T2. Každý režim pak disponuje dalšími požadavky, naříklad specifikovaný kanál, přenos frekvence či toleranci přenosové rychlosti. Díky těmto vlastnostem je možno na přímou viditelnost komunikovat až na dosah 500 či 600 m.

Komunikace probíhá pomocí hvězdicové struktury, tzn. jednotlivé účastnické jednotky komunikují s Mastrem, který vyčítá jednotlivé Slavy. Master slouží jako tzv. koncentrátor, tak jak funguje i SmartCom Pro. Jednotlivé zprávy ukládá a ty pak dále distribuuje do sítě. Je dobré zmínit, že časování je rozdílné pro každý režim, různé přenosové rychlosti.




*Obr. 15: Wireless M-Bus komunikace*

### 3.4.3 Princip adresace

Způsob adresovaní u protokolu M-Bus byl popsán v kapitole 3.3.3. Protokol Wireless M-Bus do jisté míry převzal způsob adresování od své drátové verze. Účastnické jednotky mají přidělenou adresu, kterou používají pro příjem i vysílání. Master stanice shromažďuje a uchovává tabulku přihlášených účastnických stanic. Komunikace poté probíhá s přihlášenými účastnickými stanicemi. Lze komunikovat i s účastnickými stanicemi, které nejsou zaregistrovány u Master stanice. Takové řešení je vhodné pro malé sítě, ale ve větších sítích se upřednostňuje klasické M-Bus řešení pro svoji jednoznačnost připojení. Nabízí se však řešení oba protokoly zkombinovat.

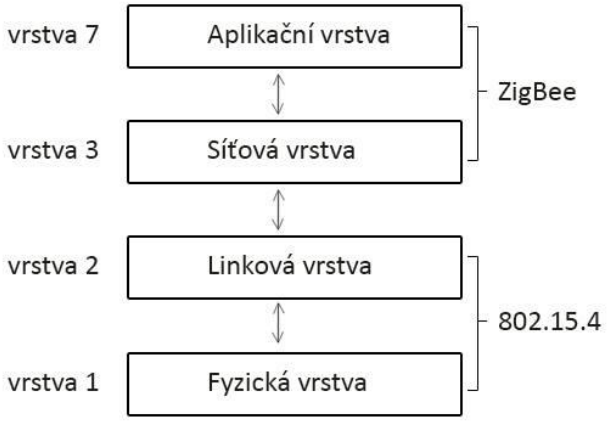
## 3.5 ZigBee

V dnešní době existuje více technologií, jak přenášet větší množství dat bezdrátově. Existují standardy jako Bluetooth, WIFI, díky kterým je možné přenášet ve vysoké kvalitě hlas, video či spojovat bezdrátově PC LAN. Technologie ZigBee je určená pro menší datové toky, nabízí minimální energetickou náročnost. Používá se proto spíše k ovládání zařízení a jednotné správě senzorů. Protokol ZigBee je chápán od 3. vrstvy do 7. vrstvy. Fyzická a spojová vrstva vycházejí ze standardu 802.15.4. ZigBee protokol vytvořila ZigBee Alliance, která udržuje a vyvíjí vícesofistikované protokoly pro pokročilé aplikace. Ve 3. a 4. vrstvě se vylepšuje ověření pro oprávněné jednotky, zaheslování pro větší bezpečnost, data routování a přesměrování pro mesh funkci sítě.

### 3.5.1 IEEE 802.15.4

Frekvence, na které funguje IEEE 802.15.4, jsou 2.4GHz a 868/ 915 MHz. Datová rychlost je pro 2.4GHz frekvenci definovaná 250 kbps, pro frekvenci 915 MHz je to 40 kbps a pro frekvenci 868 MHz je odpovídající rychlost 20 kbps. Standart využívá CSMA – CA přístup ke kanálu. Adresní místo je 64 bitový prostor, což odpovídá 18,45*1016 zařízení. Dostupnost zařízení je typicky 50 m, může se však objevit i větší vzdálenost.

ZigBee nabízí různé typy topologií sítí. Existuje hvězdicová struktura, peer – to – peer či mesh. Hlavní výhodou mesh sítě je to, že každá jednotka v síti je schopná komunikovat se všemi ostatními jednotkami, a to buď přímo, pokud na sebe jednotlivé jednotky v bezdrátové síti vidí, či nepřímo.




*Obr. 16: RM/OSI ZigBee*

### 3.5.2 Bezpečnost

Pokud je požadováno zabezpečení MAC vrstvy, použije ZigBee „MAC zabezpečení“ k ošetření MAC příkazů, beacom a potvrzovacích framů. Pro „single hop“ zabezpečení je použito zabezpečených MAC data rámců. Pro multi – hop zprávy je ZigBee závislé na vyšších vrstvách – NWK vrstva. MAC vrstva používá AES standart jako svůj klíčových zabezpečovací algoritmus.

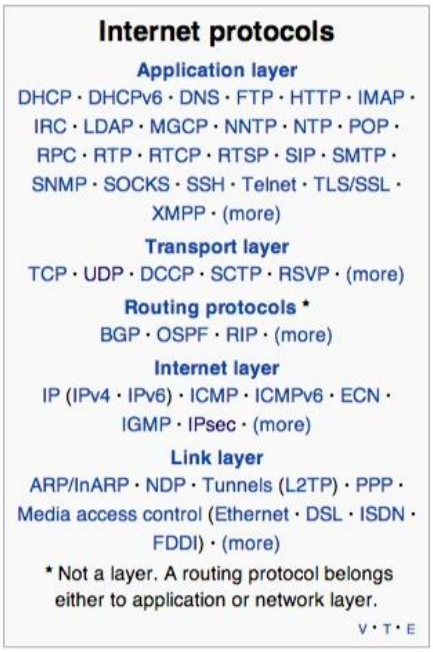
### 3.5.3 Aplikační vrstva

Aplikační vrstva se skládá z APS sub – vrstev, ZDO a továrně definovaných aplikačních objektů. APS se stará například o udržovací tabulky spojení, připojení dvou zařízení dohromady na základě jejich služby a jejich potřeby. Další funkcí je funkce „discovery“, jež je součástí ZDO. Definuje roli zařízení v síti, inicializuje spojení,

odpovídá druhé straně a navazuje zabezpečení spojení mezi síťovými zařízeními. Továrně definované aplikační objekty implementují aktuální aplikace.

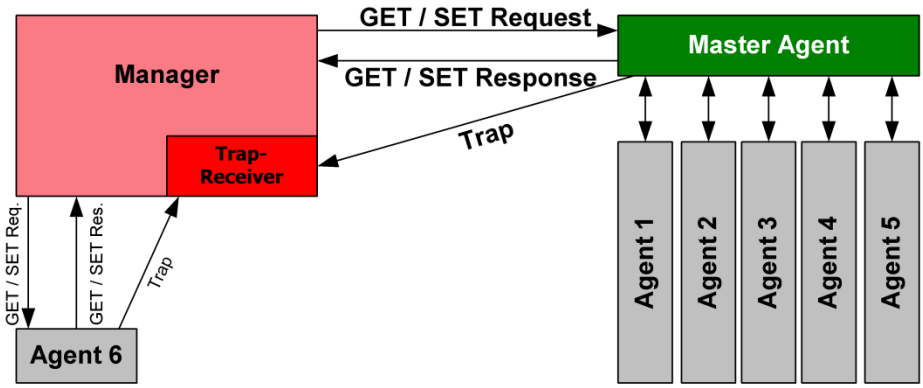
## 3.6 SNMP

SNMP bylo navrženo IETF (Internet Engineering Task Force) a je součástí skupiny důležitých internetových protokolů tzv. Internet protocol suite (Obr. 18).




*Obr. 17: Internet protocol suite*

SNMP (Simple Network Management Protocol) je Internetový protokol pro řízení/ dohled zařízení v sítích fungující na bázi IP. SNMP je většinou podporován zařízeními jako jsou směrovače, přepínače, servery, pracovní stanice, tiskárny a další. Je použit v monitorovacích systémech pro monitorování těchto zařízení. SNMP je většinou implementován pomocí protokolů jako jsou UDP, IP, CLNS, AppleTalk Datagram, IPX. V dnešní době je k dispozici SNMPv1,2 a 3. Funguje na 7. vrstvě OSI modelu nebo Aplikační vrstvě v TCP/ IP modelu. Pro komunikaci používá port 161 a UDP hlavičku. Existuje ale i SNMP, které používá TCP hlavičku.

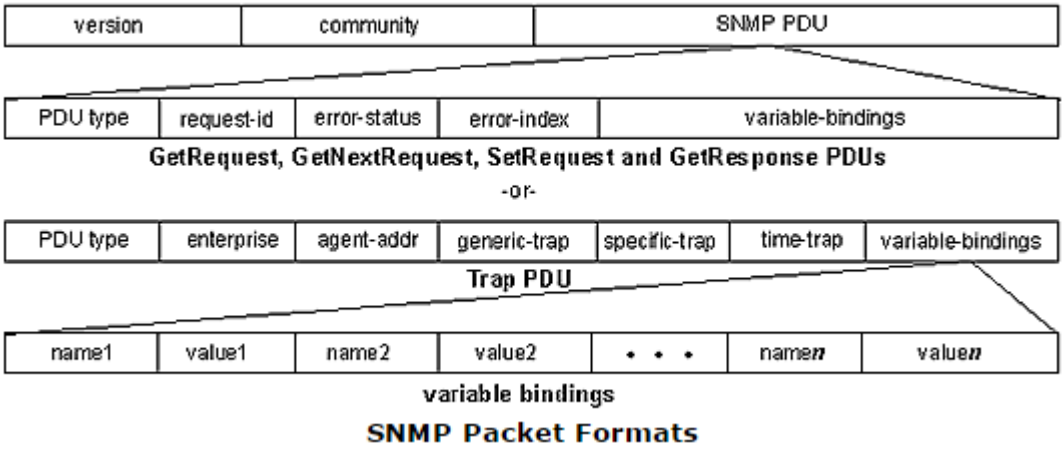



*Obr. 18: SNMP komunikace*

Na Obr. 19 je možné vidět základní koncept SNMP, kde se objevují dva základní prvky, a to Manager a Master Agent. Za manažera se dá pokládat nějaký administrativní počítač, server, který má za úkol monitorování/ řízení zařízení v síti. Toto zařízení většinou disponuje softwarem pro monitorování sítě. Druhým zařízením je Agent, monitorované zařízení, které podává manažerovi informace právě přes SNMP.

SNMP používá 7 základních typů zpráv.

1) **GetRequest** – žádost/ požadavek Manažera na zaslání hodnoty dané proměnné na monitorovaném zařízení. Agent neposílá danou hodnotu, ale pošle proměnnou (variable bindings). Manažer s ní umí pracovat
2) **SetRequest** - žádost/ požadavek Manažera na změnu hodnoty dané proměnné.
3) **GetNextRequest** - žádost/ požadavek Manažera na prozkoumání daných proměnných a jejich hodnot.
4) **GetBulkRequest** – optimalizovaná verze **GetNextRequest**
5) **Response** – odpověď agenta, pošle proměnné (variable bindings) a potvrzení na zprávy 1 – 4. Pro report chyb jsou k dispozici error – status a error – index pole.
6) **Trap** – asynchronní notifikace od agenta manažerovi. Pokud dojde k významné události na monitorovaném zařízení, to upozorní manažera zprávou. Zpráva v sobě také obsahuje sysUpTime
7) **InformRequest** – potvrzení asynchronní notifikace. Představena v SNMPv2.




*Obr. 19: SNMP PDU*

### 3.6.1 Management information base

Management information base (MIB) je databáze používaná pro zpracování entit v síti. Definuje se tzv. SMI (Structure of Management Information) specifikovaná v SNMP, která aplikuje sady souvisejících MIB objektů. Přesně v SNMPv1 definuje vysoce strukturované tabulky. Tabulky mají nula nebo více řádků. Jsou indexovány tak, aby bylo možné získat nebo změnit řádek s příkazem Get, GetNext, Set.

# 4 2N Produkty

## 4.1 2N® VoiceBlue Next

Zařízení 2N® VoiceBlue Next je zařízení, ke kterému se dají připojit až čtyři SIM karty, tedy až čtyři GSM/UMTS kanály. Hlavní funkcí je propojení VoIP sítě se sítí GSM. Brána umí pracovat se signalizačním protokolem SIP, který byl popsán v kapitole 3.1. Určena je převážně k hlasovým funkcím jako je odchozí a příchozí volání. Vedle toho je schopná dále posílat SMS zprávy, Mobility Extension, SNMP Trap errory, odesílání a příjem SMS pomocí protokolů SMTP, POP3 a dalších funkcí. Obecně je možné nastavovat bránu pomocí webového rozhraní či AT příkazů, na které reaguje v příkazové řádce. Co se týká napájení, je VoiceBlue Next schopná být napájena jak pomocí Power over Ethernet, tak pomocí externího napájení.

Čtyřkanálová varianta disponuje konektorem pro připojení Ethernet kabelu, tlačítkem reset, koaxiálním rozhraním pro anténu a dále čtyřmi sloty pro SIM karty. Každá brána je licencovaná politikou společnosti 2N Telekomunikace. Její stav je zjistitelný buď pomocí webového interface, nebo pomocí AT příkazu v příkazovém rozhraní brány.


*Obr. 20: 2N® VoiceBlue Next*

Bránu je obecně možné nastavovat pomocí webového rozhraní. Za zmínku stojí tabulka továrního nastavení, díky které je možné se do brány přihlásit. Toto nastavení opět odpovídá i pro Telnet.

**IP adresa:** 192.168.1.2
**IP maska:** 255.255.255.0
**IP gateway:** 192.168.1.1
**Username:** Admin
**Password:** 2n

Pro pokročilou konfiguraci jsou použity AT příkazy, s jejichž pomocí se dá daná brána velmi dobře překontrolovat v případě jakýkoliv technických problémů. Zde jsou

vyjmenované pouze ty nejzákladnější příkazy. Ty, které začínají **AT%id_parameter,** slouží pro zápis konfigurace do brány. Ty, které využívají **AT&sekce,** jsou určeny k vypsání konfigurace.

### 4.1.1 AT příkazy VoiceBlue Next

**Základní příkazy**
ATI3 – Firmware verze
ATI4 – Sériové číslo

**Reset**
AT&FRES – Reset brány do defaultního nastavení

**Systémová kontrola**
AT&Gxx=RESET – Reset daného GSM modulu xx

**LCR Tabulka**
AT&R – Shows LCR table

**Trace**
AT!Rx – příkaz, díky kterému je možno diagnostikovat problém v bráně
x=1 – Vrstva 1,2,3,4
x=2 – Vrstva 2,3,4
x=3 – Vrstva 3,4
x=4 – Vrstva 4

**Systémové nastavení**
AT%S70=x.x.x.x – AT příkaz pro nastavení IP adresy VoiceBlue Next
AT%S71=x.x.x.x – Tento příkaz slouží pro nastavení masky sítě

**Informace o stavu**
AT&V – Přehled o celkovém nastavení
AT&V0 – Přehled o základním GSM nastavení
AT&V# – Přehled o GSM skupinách, kde # je pro (#=1–8)
AT&VALL – Přehled o veškerých GSM skupinách
AT&VE – Přehled o VoIP parametrech

**Informace o GSM modulech**
AT&QALL – Přijatý GSM signál ze všech GSM modulů
AT&Q## – Přijatý GSM signál (##=00–15)

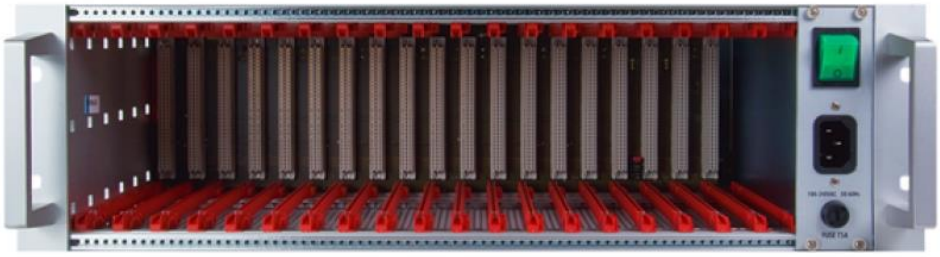
Celý seznam AT příkazů v anglickém jazyce je k dispozici dohledatelný v manuálu na stránkách 2N Telekomunikace, která má daný dokument přiložený u svého produktu.

## 4.2 BlueTower, Stargate

Brány 2N® StarGate a 2N® BlueTower jsou velmi podobné brány lišící se možným počtem připojených karet. Na úvod je nutné zmínit dvě verze CPU karty, které se z historického vývoje nabízí. Starší verze CPU karty, na rozdíl od té novější, neumí některé funkce, které je zde nutné zmínit. Starší verze nemá možnost konfigurace pomocí webového rozhraní a nemá zabudovaný účet na posílání a příjem SMS. Tyto funkce nejsou zabudované do dané stránky, avšak stránka je naprogramovaná takovým způsobem, že by do ní tyto funkce mohly být doplněny.

### 4.2.1 2N® StarGate

Brána 2N® StarGate je největší GSM bránou ve 2N® PRI rodině bran. Do racku je možno připojit 2N® StarGate pomocí 3U. Systémová sběrnice je navržena jako deska s plošnými spoji (PCB) s DIN konektory.



*Obr. 21: 2N®StarGate*

Existuje více možností, jak se dá daná brána sestavit. Velmi oblíbená je brána pro terminaci hovorů. V zemích třetího světa jsou poplatky mezi operátory vysoké, a proto vznikají místa, kde dává smysl terminace hovorů, z důvodu ušetření nákladů.

Mezi nejoblíbenější scénáře platí VoIP verze, která obsahuje VoIP kartu, CPU kartu a GSM karty, a každá karta obsahuje dva kanály. ISDN verze nahrazuje VoIP kartu PRI kartou, která obsahuje dva PRI porty. Zbytek obsahuje opět GSM karty pro směrování hovorů. Poslední použitelný scénář je použití ISDN i VoIP a GSM, jako v předchozích případech. Tato verze je zobrazena na obrázku 23.


*Obr. 22: 2N®StarGate – GSM brána*

### 4.2.2 2N® BlueTower

Ve srovnání s 2N® StarGate je 2N® BlueTower považována za nejmenší PRI bránu. Maximální kapacitu nabízí 2N® BlueTower 8 GSM kanálů. Logika zůstala stejný jako pro 2N® StarGate. Daná brána nabízí prostor pro připojení jednotlivých karet, které s sebou přináší danou funkci. Je možné připojit GSM karty s připojením kanálů, VoIP kartu či PRI kartu. Obr. 24 znázorňuje možné varianty 2N® BlueTower zapojení.

**Napájení**

Pro 2N® BlueTower se používá klasická elektrická síť, tedy interních 90 – 260 V / 50 – 60 Hz, což platí i pro 2N® StarGate, která nabízí případně redundantní napájení v případě výpadku. Hodnotami odpovídá 2N® BlueToweru.


*Obr. 23: 2N®BlueTower*

**Výhody daných zařízení**

- Až 32 GSM/ UMTS modulů (8 pro BlueTower)
- Celosvětově používaný rozsah GSM/ UMTS frekvencí
- Podpora až 2 PRI portů (DSS1 signalizace viz. kapitola 3.2) či jednoho VoIP (SIP viz. kapitola 3.1) portu
- Rozsáhlá paměť pro Call Data Records (CDR), SMS Data Records (SDR)
- Podpora SNMP, AoC, Telnet

- Posílání SMS pomocí SMTP/ POP3
- Podpora zalogování k různým BTS

### 4.2.3 AT příkazy VoiceBlue Next

**Základní příkazy**
ATI3 – Firmware verze
ATI4 – Sériové číslo

**Reset**
AT&FRES – Reset brány do defaultního nastavení

**Systémová kontrola**
AT&Gxx=RESET – Reset daného GSM modulu xx

**LCR Tabulka**
AT&R – Shows LCR table

**Trace**
AT!Rx – příkaz, díky kterému je možno diagnostikovat problém v bráně
x=1 – Vrstva 1,2,3,4
x=2 – Vrstva 2,3,4
x=3 – Vrstva 3,4
x=4 – Vrstva 4

**Systémové nastavení**
AT%S70=x.x.x.x – AT příkaz pro nastavení IP adresy VoiceBlue Next
AT%S71=x.x.x.x – Tento příkaz slouží pro nastavení masky sítě

**Informace o stavu**
AT&V – Přehled o celkovém nastavení
AT&V0 – Přehled o základním GSM nastavení
AT&V# – Přehled o GSM skupinách, kde # je pro (#=1–8)
AT&VALL – Přehled o veškerých GSM skupinách
AT&VE – Přehled o VoIP parametrech

**Informace o GSM modulech**
AT&QALL – Přijatý GSM signál ze všech GSM modulů
AT&Q## – Přijatý GSM signál (##=00–15)

## 4.3 2N® SmartCom PRO

V dnešní době dochází k velkému nárůstu trhu s „M2M“přístroji pro chytrý odečet. Pro efektivnější fungování firem jsou v současnosti instalovány k vodoměrům a elektroměrům zařízení pro inteligentní odečítání hodnot a posílání těchto hodnot dále do serveru ke zpracování. Pro příklad je možné uvést plýtvání vodou či elektřiny ve větších firmách. Díky „M2M“ (Machine to Machine) technologii je vedení firmy schopné efektivně zjistit, kde se vodou plýtvalo, a tak tomu zamezit. V součastnosti se v telekomunikacích objevují dva trendy, kam se telekomunikace budou dále posunovat, a to „Internet of Things“ či „Machine to Machine“ komunikace.

Produkt 2N Telekomunikace 2N® SmartCom PRO je zařízení z M2M rodiny komunikující Peer – to – Peer. S měřícími systémy komunikuje 2N® SmartCom PRO zejména pomocí rozhraní, která byla vysvětlena v kapitolách 3.3, 3.4 či 3.5, oblíbené rozhraní používané pro komunikaci M-Bus či Wireless M-Bus. Zařízení disponuje dále RS232 portem, slotem pro SIM kartu, pro vzdálené posílání naměřených dat pomocí GPRS či Ethernet kabelem pro komunikaci přes IP, bohužel však nenabízí PoE pro vzdálené napájení. Vedle konektoru pro Ethernet je umístěna svorkovnice pro napájení a porty pro baterii. Na 2N® SmartComu PRO jsou dále umístěna 2 relé pro sepínání či rozepínání spojů. Toto se dá využít například při UDF – Uživatelsky definovaných funkcích. Vedle relé disponuje 2N® SmartCom PRO dvěma vstupy umístěnými také na svorkovnici, které disponují stejnou společnou zemí GND. Vstupy slouží pro měření napětí, proudu a k detekci logických úrovní. Uživatel se rozhodne, které měření bude provádět, a podle toho musí použít správné jumpery pro korektní hodnoty a funkčnost.

Měření proudu lze provádět v rozmezí 4mA – 20mA, napětí v rozmezí 0 – 10V, pro detekci logických úrovní a jejich počítaní, ať už se jedná o napěťové, či proudové logické úrovně, je nutné použít jiné příkazy a správně nastavit jumpery.

V dnešní době funguje 2N® SmartCom PRO dvěma možnými způsoby. Jednotka může fungovat v režimu „Stand alone“ a tehdy nepotřebuje pro svoje fungování žádné zařízení. Komunikace je možná pomocí aplikačního softwaru pro konfiguraci jednotky či pomocí Telnetu. IP přístup umožňuje přístup na port 10000, 10001, 10002. Telnet na portu 10000 umožňuje konfigurovat 2N® SmartCom, ovládat relé a měřit výstupní veličiny na vstupních obvodech. Port 10001 přesměrovává komunikaci na RS232 rozhraní, port 10002 funguje jako trubka pro M-Bus rozhraní. Veškerá komunikace pro 10001, 10002 je přeposílána pomocí GPRS. Druhá možnost užívání jednotek a konfigurace je pomocí 2N® SmartCom Serveru. 2N® SmartCom Server slouží k vytvoření tunelů mezi jednotlivými jednotkami a 2N® SmarCom Control Panelem. Používá se pro instalace více jednotek umístěných na různých místech komunikující s 2N® SmartCom Serverem.


*Obr. 24: 2N® SmartCom PRO*

**Napájení**

Napájení 2N® SmartCom PRO vyžaduje stejnosměrné napětí 5 – 50 V se stejnou polaritou. Napájení se připojuje do 4 – pinové svorkovnice. Ale zároveň je možné k dané svorkovnici připojit i záložní baterii. Napájení je přivedeno skrze 2N® SmartCom PRO na výstup. Toto napájení lze tedy zkombinovat s relé pro další využití.

### 4.3.1 AT příkazy

Konfigurace je možná pomocí Telnet na portu 10000 či pomocí sériové linky. Na tomto portu je možno zjišťovat hodnoty na vstupech, slouží ke konfiguraci a ovládání výstupů.

**Základní příkazy**
at+cgmi – Zobrazí výrobce
at+cgmm – Zobrazí model zařízení
at+cgmr – Zobrazí firmware
at+cgsn – Zobrazí IMEI GSM modulu
at+cimi – Zobrazí IMSI SIM karty
at^sccfgall? – Zobrazí aktuální hodnoty rozhraní

**Reset**
at^screstart – Reset SmartCom PRO
at^scfres – Factory Reset SmartCom PRO

**Služby**
at^sc232lock? – Provede nastavení zámku RS232
at^scop? – Zobrazí GSM operátora, ke kterému je SmartCom aktuálně přihlášen
at^scms? – Specifikace GSM modulu
at^sig? – Intenzita signálu

**Nabíječka**
at^scchg="state" - Zjištění stavu nabíjení

- Možnosti: *Active* – aktivuje nabíjení akumulátoru
*Stopped* – nabíjení je zastaveno

**Wireless M-Bus**

at^scwmbus="get_space" – Zobrazí volné místo
at^scwmbus="mess_cnt" – Zobrazí počet přijatých zpráv
at^scwmbus="restart" – Restart Wireless M-Bus
at^scwmbus? – Zobrazí aktuální hodnoty nastavení
at^scwmbus="mode",11 – Nastavení módu
- Možnosti: 1 – T1
3 – S1
8 – C1
11 – T1+C

at^scwmbus="get_oldest"<,n> - Výčet n posledních uložených zpráv

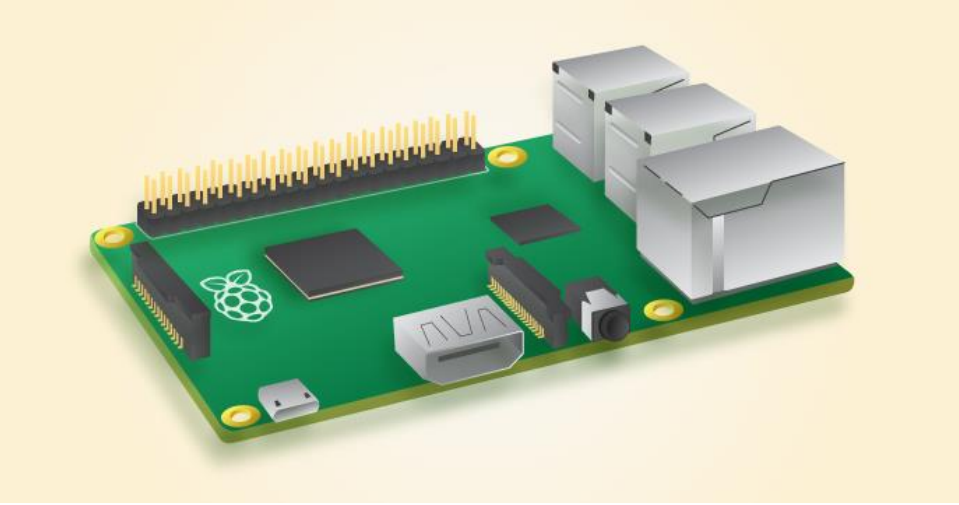
Dané skripty jsou vybrané jako ty nejdůležitější AT příkazy. Veškeré dostupné AT příkazy jsou k dispozici v návodu. Ne všechny příkazy budou uplatněny ve finální webové stránce. Stránka je navržena tak, aby se do ní daly skripty dopsat. Ty nejdůležitější budou uvedeny v „Help“ sekci, která je součástí této stránky.

# 5 Realizace

K realizaci dané stránky jsem se rozhodl použít velmi kompatibilní zařízení Raspberry 2, které má oproti klasickému serveru nesporné výhody. Raspberry je velmi nenáročné na spotřebu a nabízí dostatečný výkon pro běh webového serveru a daných skriptů. Jako webový server byl použit klasický Apache server, který plně vyhovuje danému požadavku. Aplikace jako taková není pouze jedna stránka, nýbrž více stránek. Na základě uživatelské aktivity také python skripty, které byly naprogramované pro komunikaci s danými produkty.

## 5.1 Raspberry Pi 2

V únoru 2015 bylo představeno zařízení Raspberry Pi 2, které za cenu do 50$ nabídne dostatečný výkon pro daný projekt a další služby. Raspberry Pi 2 obsahuje 900MHz čtyřjádrový procesor ARM Cortex – A7 CPU spolu s 1GB RAM. Oproti předešlé verzi rozšiřuje svoji nabídku na 4 USB, kde se dá připojit například externí disk. K 4 USB rozhraním přidává ještě slot pro micro SD kartu až do 128GB. Raspberry Pi 2 dále nabízí ethernetový port pro síťovou komunikaci či HDMI konektor, proto je velmi oblíbený i jako domácí multimediální centrum, z kterého je možno pouštět multimediální obsah. Raspberry má vlastní systém Raspbian, jedná se o linuxovou distribuci pracující na ARM infrastruktuře. Ve své diplomové práci se nebudu věnovat instalaci Raspbianu, protože již existuje spoustu návodů, a nepovažuji tedy za důležité toto zmiňovat.



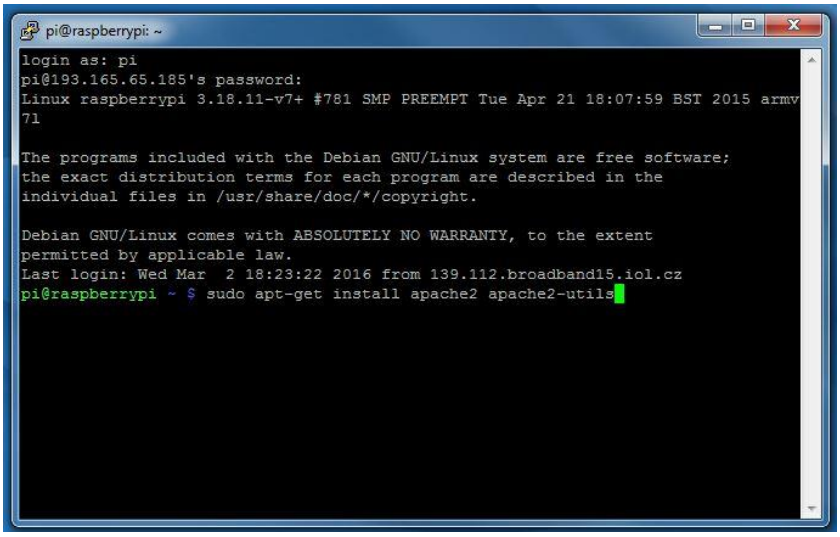
*Obr. 25: Raspberry Pi 2*

## 5.2 Instalace Apache

Raspberry Pi 2 běží na veřejné IP adrese 193.165.65.185, kde je otevřený port 80 pro webovou komunikaci a 53022 pro SSH komunikaci. Jiné porty jsou uzavřeny a neměly by být pro komunikaci přístupné. Zakazáné jsou například porty 23 pro Telnet či 443 pro HTTPS. Toto by samozřejmě mohl být bezpečnostní problém, zatím však stránka slouží k testovacím účelům interně v síti a nebyla použita pro koncové zákazníky.

Apache je nejpoužívanější webový server s otevřeným kódem pro GNU/ Linux, Solaris, Mac OS X či Microsoft Windows. Protože nabízí velké množství různých funkcí, které uživatelé ocení, patří k oblíeným serverům. Mnohé z těchto funkcí jsou implementovány jako kompilované rozšiřující moduly pro jádro, podporující velké množství programovacích jazyků či různých atentizačních technik. Apache umí dobře pracovat se skriptovacími jazyky Perl, Python či webovým jazykem PHP. Podporuje TLS, SSL či různé filtrace.

Instalace Apache je v prostředí Linux poměrně jednoduchá. V příkazovém řádku Raspberry Pi se napíší dva linuxové příkazy *apt-get install apache2* a *apt-get install apache2-utils*, které zajistí krátkou instalaci webového serveru. Pokud nebude nic změněno, webový server bude přistupovat k adresáři */var/www/*. I mně v tomto adresáři běží webový server a jednotlivé soubory s kódem či python skripty je uložen právě zde.




*Obr. 26: Instalace Apache server*

Pro správný chod této webové aplikace je nutné nainstalovat ještě všechny balíčky pro PHP programovací jazyk. PHP je použito nejen pro stránku „Help“, která vysvětluje jednotlivé skripty a správně je zobrazuje, ale i pro potvrzovací stránku, kde PHP přenáší všechny potřebné informace a volá hlavní python skript.

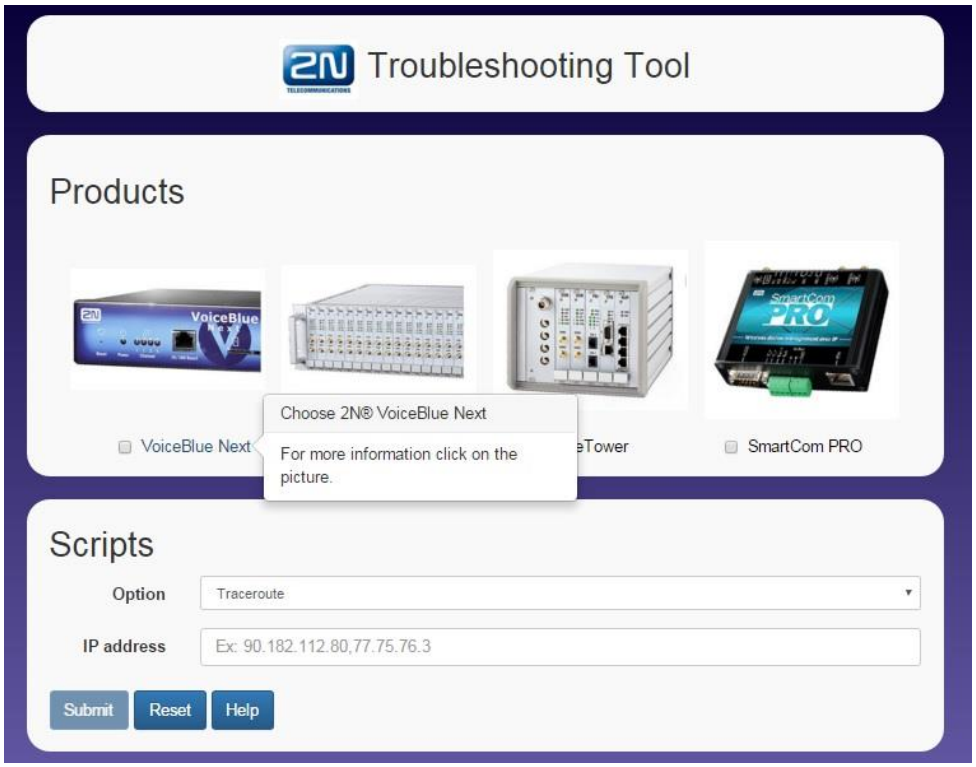
## 5.3 Troubleshooting Tool

Troubleshooting tool je stránka vytvořená k rychlému a chytrému managementu bran či SmartCom Pro. Celá stránka v sobě ukrývá HTML kód, často je použit jQuery pro různé dynamické přechody či PHP. Důležité je také zmínit, že stránka je vedená v anglickém jazyce, a to z důvodu působnosti 2N. V dnešní době se brány hodně prodávají na rozvíjejících se trzích, a proto jsem se rozhodl napsat stránku ve světovém jazyce. Stránka se skládá z několika částí. Hlavní stránka, tzv. „Dashboard“, která je dostupná na webové adrese *193.165.65.185/2N_tool,* je rozdělena do tří částí. Nadpis, výběr produktu, pro který se daný uživatel rozhodne, a sekce pro skripty, které jsou závislé na výběru produktu.

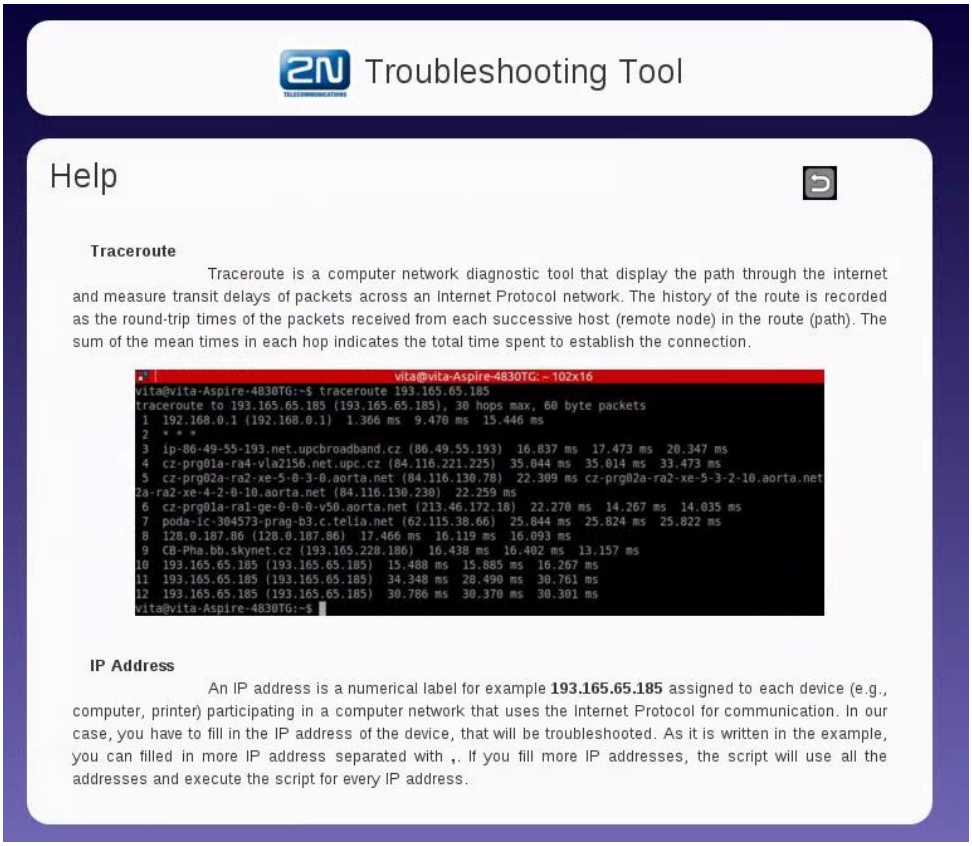
Výběr z produktů probíhá pomocí radio checkboxu a čtenář s nimi byl seznámen v kapitole 4. Zároveň je obrázek produktu „hypertextový odkaz“ na stránky 2N, kde je uživatel přesměrován přímo na daný produkt.

Po výběru produktu se uživateli v druhé sekci upraví nabídka skriptů na základě zvoleného produktu. Každý skript z nabídky musí být doplněn o nejdůležitější informace, jinak není možné tento skript odeslat do Raspberry Pi. Toto je možné vidět například na následujícím obrázku, kde je tlačítko „Submit“ zašedivělé, dokud nebude vepsána IP adresa do kolonky IP address. Vedle tlačítka „Submit“ je možné najít ještě dvojici tlačítek, která uživateli pomáhají při neznalosti či chybě. „Reset“ kompletně vymaže rozpracované zadání stránky, pokud uživatel udělá chybu nebo pokud neví, jak postupovat dále. Tlačítko „Help“ slouží k popisu, kdy uživatel přesně neví, co daný skript dělá.

Toto tlačítko uživatele nasměruje na stránku, kde má k dispozici maximum informací o daném skriptu. Součástí popisu jsou obrázky a „hypertextové“ odkazy pro důkladnější nastudování dané problematiky. Zpět se dostane příslušným tlačítkem „Zpět“ v horní části obrazovky.




*Obr. 27: Úvodní stránka*




*Obr. 28: Help*

## 5.4 Použití skriptů pro GSM brány

Pokud si uživatel zjistí všechny potřebné informace k danému skriptu z „Help“ sekce a rozhodne se ho použít, je nutné vyplnit IP adresu daného produktu. Zbylé hodnoty je možné změnit, pokud však uživatel dané hodnoty nezmění a nechá okno prázdné, doplní si stránka defaultní hodnoty z návodu daných produktů. Pro každý skript se zobrazuje jiná rozšiřující tabulka podle toho, co daný skript potřebuje. Toto je zajištěno pomocí jQuery/ Javascriptu, který si se zobrazením dané rozšiřující tabulky poradí.

V samotných oddílech je toto uděláno pomocí parametru „display:none“. Pokaždé, když uživatel zvolí určitý skript, tak se přepíše pomocná a daný oddíl se zobrazí.

```
<div class="accessories_Ping" style="display:none">
</div>
```

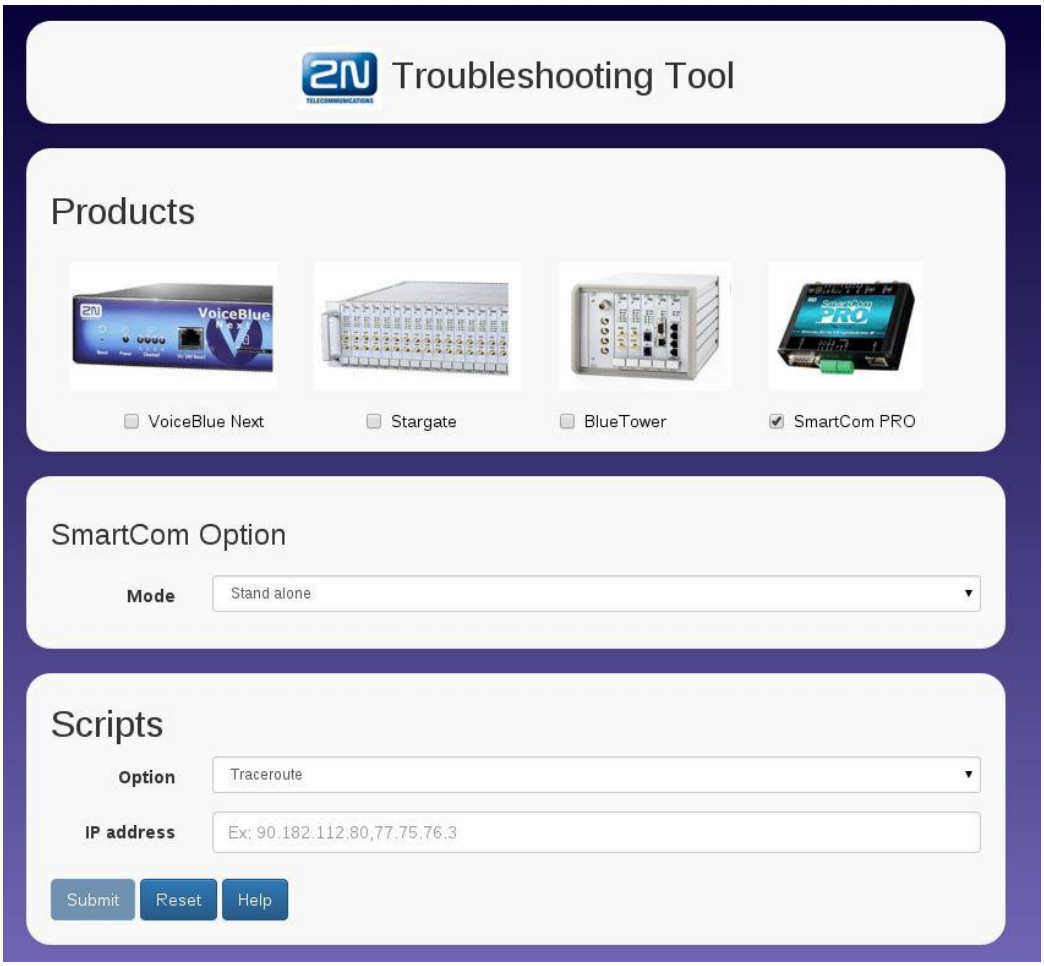
```
<script>

//OPTION mode - it will show you all the information needed to complete the
script

 $(document).ready(function() {

  $('#option').change(function() {

       $(".accessories_Ping").toggle($(this).val()=='Ping');

  }).trigger('change.accessories_Ping');

 });

 $(document).ready(function() {

  $('#option').change(function() {

          $(".accessories_username_password").toggle($(this).val() == 'Basic
      info' ||   $(this).val() == 'GSM module info' || $(this).val() == 'Restart
      GSM modules' || $(this).val() == 'Trace');

  }).trigger('change.accessories_username_password');

 });

</script>
```

*Obr. 29, 30: Skripty na rozbalování nabídky*

Poté, co uživatel vyplní všechny hodnoty, stačí kliknout na tlačítko „Submit“ a uživatel bude přesměrován na tabulky s výsledky. Zároveň se spusí python skript, který zapsané hodnoty zpracuje a provede danou akci na bránách 2N.

## 5.5 Použití skriptů pro SmartCom PRO

Použití skriptů pro SmarCom PRO funguje naprosto podobně jako pro brány. Při označení SmartCom PRO je navíc nabídnuta tabulka, která uživateli poradí, jakým způsobem SmartCom PRO funguje v síti. Zda se jedná o „Stand alone“ jednotku, do které se uživatel plánuje připojit, či o „Client – Server“ jednotku, která komunikuje skrze SmartCom server, a bude třeba využít API tunel vytvořený firmou 2N. Samotnou stránku můžete vidět na obr. 31. Dále je třeba jen zvolit daný skript a další hodnoty nutné pro realizaci python skriptů.




*Obr. 31: 2N® SmartCom PRO*

Stisknutí „Submit“ se odešlou hodnoty do Raspberry a dále python skript vyhodnotí uživatelské nastavení.

```
<button type="submit" class="btn btn-primary" name="odeslat" value="submit"> Submit
</button>
```

*Obr. 32: Submit*

Jednotlivé hodnoty jsou uloženy do textových souborů a poté si na ně python skript sahá. Na stránce s výsledky je použit jazyk PHP, který využívá metodu POST a zapisuje jednotlivé proměnné z předešlé stránky. Část realizace je ukázána na obrázku 34. Samotný skript je vyvolán pomocí exec příkazu.

```
exec('/usr/bin/python ../python/header.py');
```

*Obr. 33: Volání pomocí python skriptu*

```
<?php

//$address = array();

$IP_address=$_POST['troubleshooted_device'];

$file_address = '../data_text/IP_address.txt';

file_put_contents($file_address, $IP_address);


$script=$_POST['option'];

$file_option = '../data_text/script.txt';

file_put_contents($file_option, $script);


$unit=$_POST['devices'];

$file_device = '../data_text/device.txt';

foreach ($unit as $devices){

   $variable=$devices.",";

   file_put_contents($file_device, $variable,FILE_APPEND);

}
```

*Obr. 34: Zápis hodnot*

Samotný python skript mapuje hodnoty uložené metodou post a vyvolá jednotlivé skripty podle toho, co si uživatel vybral. Výsledné hodnoty se pak zapisují do textových souborů a jsou uživateli předány ke stažení či zobrazení na stránce. V jednotlivých kapitolách o produktech 2N byly vyjmenované nejdůležitější příkazy, díky kterým se daná zařízení ovládají. Python skript použije Telnet knihovnu pro vzdálený přístup. Pomocí telnet se skript přihlásí do brány a zde využije některý z příkazů pro získání potřebných informací. Tyto informace jsou uloženy do txt formátu a jsou vygenerovány z několika informací. Data se po tlačítku Zpět smažou z paměti, tak, aby se server po větším využití a delší době nezahltil.

```
for ($var = 1; $var <= count($unit); $var++) {

    echo '<b><img src="../data/file.png" alt="Logo" width="24" heigth="19"><a
href="../results_data/'.$script.'_'.$unit[$var-1].'_'.$time_stamp.'.txt"
title="'.$unit[$var-1].'">'.$script.'_'.$unit[$var-1].'_'.$time_stamp.'</a></b><br>';

}
```

*Obr. 35: Volání pomocí python skriptu*

```
var=0
if script=="Ping":
        for unit in devices:
                function.ping_traceroute_2n.ping(IP_address[var],unit,script,
                time_stamp,number_pings,packets_length)
                var+=1

elif script=="Traceroute":
        for unit in devices:
                function.ping_traceroute_2n.traceroute(IP_address[var],unit,script,
                time_stamp)
                var+=1

elif script=="Basic info":
        for unit in devices:
                function.basic_GSM_info.basic_info(IP_address[var],username,
                password,telnet_port,script,unit,time_stamp)
                var+=1

elif script=="GSM module info":
        for unit in devices:
                function.basic_GSM_info.gsm_module_info(IP_address[var],
                username,password,telnet_port,script,unit,time_stamp)
                var+=1
....
```

*Obr. 36: Volání konkrétní funkce v pythonu*

# 6 Závěr

V mé diplomové práci jsem čtenáře seznámil s funkcionalitou RM/OSI, rozebral jsem protokoly pro chytré vyčítání dat z měřících systému či představil komunikační protokoly vyvinuté pro přenos hlasového signálu, a to v IP síti tak v ISDN.

V úvodní části byl rozepsán plán na vytvoření webové stránky, která by pracovala s produkty 2N Telekomunikace. Stránka měla mít jednotné webové rozhraní, pomocí kterého by se vyvolávaly jednotlivé skripty. Měla obsahovat „Help“ sekci, kde budou jednotlivé skripty vysvětlené a bude vysvětleno, co jednotlivé skripty dělají. Jak bylo v práci popsáno, pro skripty byly použity GSM brány VoiceBlue Next, StarGate, BlueTower. Další produkt, se kterým moje aplikace pracuje, je SmartCom Pro. M2M produkt sloužící pro vyčítání dat z různých měřících systémů.

Aplikace nabízí jednoduchý design. Povedlo se vytvořit jednoduché, uživatelsky příjemné prostředí pro zisk potřebných informací. S tím se pojí i výhoda toho, proč byl projekt zahájen a nakonec se z něj stala diplomová práce. Webová aplikace má umožnit uživateli ovládat více bran najednou a ulehčit tak integrátorovi ovládání jednotlivých bran. Co se týká SmartCom PRO, webová aplikace nabízí pohodlné vypsání jednotlivých načtených dat. Nyní funguje SmartCom Pro ve smyslu, že uživatel použije skript pro výčet dat ze SmartCom Pro. Musí se přihlásit do konzole a udělat daný výčet. Pomocí mé aplikace je tento proces automatizován pomocí webového rozhraní. Jediné, co bude potřebovat, je mít daná zařízení připojené k internetu.

Všechny skripty jsou napsány ve skriptovacím jazyku python. Díky této práci jsem se naučil programovat v pythonu, což považuji za velkou výhodou. V dnešní době se veškeré technologie automatizují, a to včetně konfigurace sítí. Díky pythonu je možné psát různé skripty, které budou automaticky konfigurovat dané „end-pointy“ bez nutnosti výjezdního technika. Pokud bude mít koncový router vykonfigurovanou IP adresu a komunikace bude fungovat, je možné pomocí python skriptů konfigurovat dané zařízení automaticky.

# 7 Literatura


[1] Bless, Roland: NAT, IPv6. KIT, Karlsruhe 2014 [cit. 2014-12-15]. Předmět dostupný z WWW: < telematics.tm.kit.edu/english/ss2016_2929.php >.

[2] Postel, John.: RFC 791 - INTERNET PROTOCOL [online]. [cit. 2014-12-16] Dostupné z WWW: < www.tools.ietf.org/html/rfc791.txt >.

[3] Postel, John.: RFC 793 - TRANSMISSION CONTROL PROTOCOL [online]. [cit. 2014-12-17] Dostupné z WWW: < ietf.org/rfc/rfc793.txt >.

[4] Network Working Group: RFC 3261 – Session Initiation Protocol [online]. [cit. 2015-10-12]. Dostupné z WWW: < ietf.org/rfc/rfc3261.txt >.

[5] Virtuální univerzita CISCO CCNA Exploration 1.0. Aktualizováno 2007. [cit. 2013-05-12]. Dostupné z WWW: < www.netacad.com >.

[6] Wikipedia : Simple Network Management Protocol. [cit. 2014-12-17] Dostupné z WWW: < en.wikipedia.org/wiki/Simple Network Management Protocol >.

[7] Session Initiation Protocol – online přednášky [online]. [cit. 2016-02-02]. Dostupné z WWW: < en.wikipedia.org/wiki/Session_Initiation_Protocol>, < www.fel.cvut.cz/cz/education/bk/predmety/12/52/p12521404.html >.

[8] ISDN - popis signalizačního protokolu [online]. [cit. 2016-02-04]. Dostupné z WWW: < en.wikipedia.org/wiki/Integrated_Services_Digital_Network >, < www.fel.cvut.cz/cz/education/bk/predmety/12/52/p12521404.html >.

[9] M-Bus – popis bus systému [online]. [cit. 2016-02-07]. Dostupné z WWW: < www.m-bus.com/files/MBDOC48.PDF >, < en.wikipedia.org/wiki/Meter-Bus >; < automatizace.hw.cz/komunikacni-protokol-m-bus-popis-a-struktura >.

[10] Raspberry Pi 2, Raspbian – Informace o produktu Raspberry Pi 2 [online]. [cit. 2016-02-14]. Dostupné z WWW: < www.raspberrypi.org/products/raspberry-pi-2-model-b/ >, < en.wikipedia.org/wiki/Raspberry_Pi >, < www.raspbian.org/RaspbianInstaller >.

[11] 2N® SmartCom Pro – informace o daném M2M produktu [online]. [cit. 2016-02-16]. Dostupné z WWW: < https://wiki.2n.cz/pages/viewpage.action?pageId=19535175 >.

[12] 2N® VoiceBlue Next – informace o daném GSM produktu [online]. [cit. 2016-02-18]. Dostupné z WWW: < https://wiki.2n.cz/pages/viewpage.action?pageId=19532579 >.

[13] 2N®StarGate – informace o dané GSM bráně [online]. [cit. 2016-02-17]. Dostupné z WWW: < https://wiki.2n.cz/pages/viewpage.action?pageId=19071576 >.

[14] Wireless M-Bus – popis wireless bus systému [online]. [cit. 2016-02-21]. Dostupné z WWW: < www.silabs.com/products/wireless/Pages/Wireless-M-Bus.aspx >; < www.silabs.com/Marcom%20Documents/Resources/wireless-m-bus-quick-start-guide.pdf >, < www.emcu.it/WirelessMBUS/Wireless_M-BUS_Solutions_and_more.pdf >; < automatizace.hw.cz/sbernice-wireless-m-bus-popis-a-struktura >.

[15] ZigBee – popis protokolu [online]. [cit. 2016-02-25]. Dostupné z WWW: < electronicdesign.com/what-s-difference-between/what-s-difference-between-ieee-802154-and-zigbee-wireless >

[16] Dr. M. O. Faruque Sarker: Python Network Programming Cookbook [online]. [cit. 2015-11-08]. Dostupné z WWW: < it-ebooks.info/book/4634/ >

[17] Rhodes B., Goerzen J.: Foundations of Python Network Programming [online]. [cit. 2016-02-21]. Dostupné z WWW: < it-ebooks.info/book/5391/ >

[18] Přehledné příklady kódů pro tvorbu webového obsahu [online]. [cit. 2016-02-21]. Dostupné z WWW: < www.w3schools.com/ >; < www.stackoverflow.com/ >.

# 8 Seznam obrázků

# 9 Seznam tabulek

# 10 Seznam použitých zkratek

| Zkratka | Name | Název |
|---|---|---|
| RM | Reference Model | referenční model |
| OSI | Open Systems Interconnection | propojení otevřených systémů |
| TCP | Transmission Control Protocol | primární transportní protokol |
| IP | Internet Protocol | protokol síťové vrstvy |
| VoIP | Voice over IP | hlas přes IP |
| SNMP | Simple Network Management Protocol | Simple Network Management Protocol |
| LLC | Logical Cink Control | ovládání logického propojení |
| FDDI | Fiber distributed data interface | rozhraní pro data distribuovaná po vlákně |
| MAC | Media Access Control | kontrola přístupu k médiu |
| UDP | User Datagram Protocol | protokol uživatelského datagramu |
| IPv4 | Internet Protocol version 4 | internetový protokol verze 4 |
| IPv6 | Internet Protocol version 6 | internetový protokol verze 6 |
| ULA | Unique Local Address | jednotná lokální adresa |
| CGA | Cryptographically Generated Address | zabezpečená generovaná adresa |
| ICMP | Internet Control Message Protocol | internetový protokol kontrolních zpráv |
| ARP | Address Resolution Protocol | protokol pro převod adres |
| IGMP | Internet Group Management Protocol | internetový protokol skupinové správy |
| ICMPv6 | Internet Control Message Protocol version | internetový protokol kontrolních zpráv verze 6 |
| AH | Authentication header | ověřovací hlavička |
| ESP | Encapsulation security payload | zapouzdření zabezpečených dat |
| API | Application Programming Interface | programovací aplikační rozhraní |
| kbps | kilobit per second | kilobitů za vteřinu |
| Mbit/s | Megabit per second | Megabitů za vteřinu |
| HTTP | Hypertext Transfer Protocol | protokol pro výměnu hypertextových dokumentů |
| HTTPs | Hypertext Transfer Protocol secure | zabezpečenýprotokol pro výměnu hypertextových dokumentů |
| POP3 | Post Office Protocol 3 | protokol pro stahování emailových zpráv |
| FTP | File Transfer Protocol | protokol pro přenos souborů |
| IMAP | Internet Message Access Protocol | protokol pro vzdálený přístup k e-mailové schránce |
| SSH | Secure Shell | zabezpečený komunikační protokol |
| ACK | Acknowledgement | potvrzení |
| SYN | Synchronize | synchronizace |
| RPC | remote procedural call | vzdálené volání procedur |
| SSL | Secure Socket Layer | vrstva bezpečných socketů |
| GSM | Global System for Mobile Communications | globální systém pro mobilní komunikaci |
| DSS1 | Digital Subscriber System No. 1 | digitální účastnický (signalizační) systém č. 1 |
| M-Bus | Meter Bus | měřící bus |
| NGN | Next Generation Network | budoucí generace sítí |
| PBX | Private Branch Exchange | pobočková telefonní ústředna |
| RTP | Real-time Transport Protocol | *real-time transportní prokol* |
| SIP | Session Initiaion Protocol | protokol pro inicializaci relací |
| RFC | Request For Comments | žádost o komentáře |
| DTMF | Dual Tone Multi Frequency | tónová volba |
| URI | Uniform Resource Identifier | jednotný identifikátor zdroje |
| UAC | User Agent Client | užitelský agent - klient |
| UAS | User Agent Server | uživatelský agent - server |
| QoS | Quality of Services | kvalita služeb |
| ISDN | Integrated Services Digital Network | integrované služby digitální sítě |

| Zkratka | Name | Název |
|---|---|---|
| BRI | Basic Rate Interface | Basic Rate Interface |
| PRI | Primary Rate Interface | Primary Rate Interface |
| NT | Network Termination | síťové ukončení |
| TE | Terminal Equipment | koncová zařízení |
| SS7 | Signaling System Number 7 | Signalizační systém č. 7 |
| L2 | Layer 2 | vrstva 2 |
| L3 | Layer 3 | vrstva 3 |
| HDLC | High Definition Link Control | *High Definition Link Control* |
| FCB | Frame Count Bit | rámec čtených bitů |
| FCV | Frame Count Valid | počet platných rámců |
| ACD | Access Demand | požadavek přístupu |
| DFC | Data Flow Control | kontrola datového toku |
| NWK | Network | síť |
| ZDO | Zigbee Device Object | zigbee zařízení |
| CLNS | Connection-less mode Network Service | bezespojový mód síťových služeb |
| MIB | Management Information Base | databázé řídících informací |
| SMI | Structure of Management Information | struktura řídících informací |
| UMTS | Universal Mobile Telecommunication System | universální mobilní telekomunikační systém |
| CPU | Central Processing Unit | procesor |
| PCB | Printed Circuit Board | plošný spoj |
| BTS | Base Transceiver Station | základnová převodní stanice |
| M2M | Machine to Machine | od zařízen k zařízení |
| GND | Ground | zem |
| ARM | Acorn Ritch Machine | arm procesor |
| PHP | PHP: Hypertext Preprocessor | PHP: Hypertextový Preprocessor |

# Přílohy

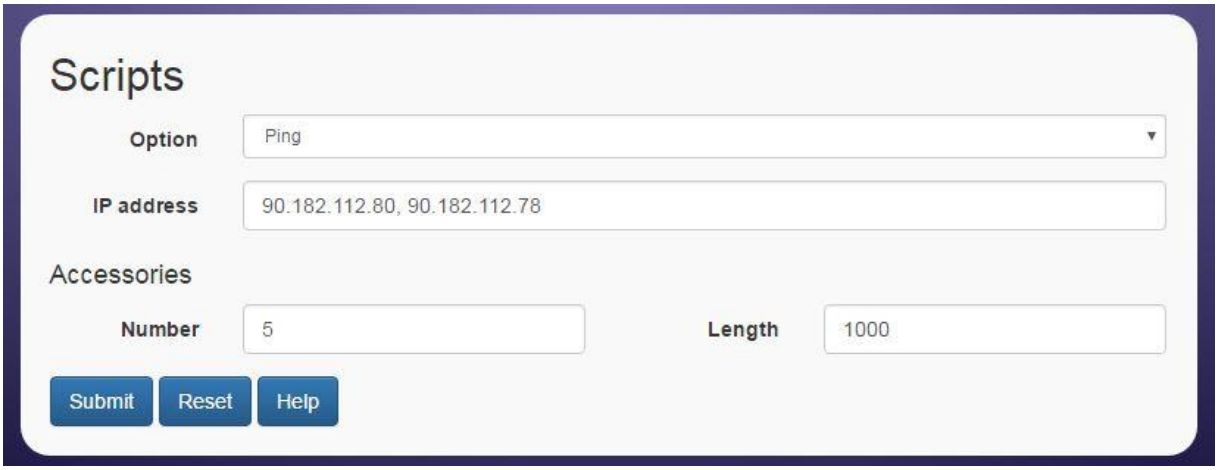
Seznam příloh:

Příloha 1 – Raspberry Pi 2 – server Troubleshooting Tool
Příloha 2 – Skript Ping a výsledek Troubleshooting Tool
Příloha 3 – Skript GSM module info a výsledek Troubleshooting Tool
Příloha 4 – Skript SmartCom M-Bus direct setup&read a výsledek Troubleshooting Tool
Příloha 5 – Skript SmartCom M-Bus get oldest a výsledek Troubleshooting Tool

## Příloha 1 - Raspberry Pi 2 – server Troubleshooting Tool

Raspberry Pi 2

## Příloha 2 - Skript Ping a výsledek Troubleshooting Tool

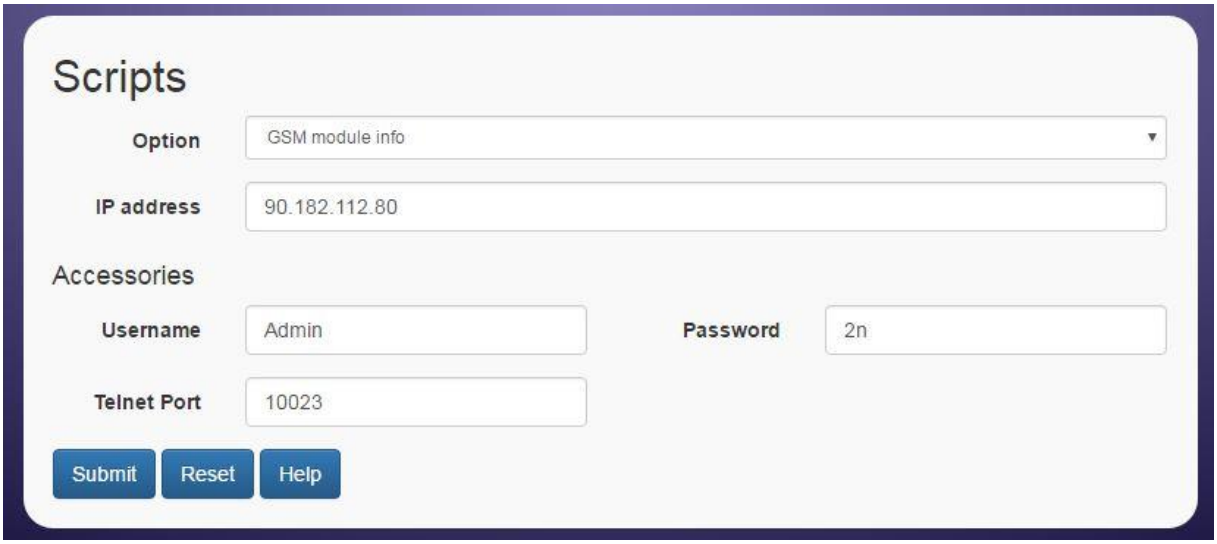



Nastavení skriptu

```
PING 90.182.112.80 (90.182.112.80) 1000(1028) bytes of data.
1008 bytes from 90.182.112.80: icmp_req=1 ttl=53 time=14.5 ms
1008 bytes from 90.182.112.80: icmp_req=2 ttl=53 time=16.3 ms
1008 bytes from 90.182.112.80: icmp_req=3 ttl=53 time=16.6 ms
1008 bytes from 90.182.112.80: icmp_req=4 ttl=53 time=15.8 ms
1008 bytes from 90.182.112.80: icmp_req=5 ttl=53 time=12.7 ms

--- 90.182.112.80 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 12.792/15.246/16.628/1.415 ms
PING 90.182.112.78 (90.182.112.78) 1000(1028) bytes of data.
1008 bytes from 90.182.112.78: icmp_req=1 ttl=53 time=17.0 ms
1008 bytes from 90.182.112.78: icmp_req=2 ttl=53 time=13.6 ms
1008 bytes from 90.182.112.78: icmp_req=3 ttl=53 time=13.0 ms
1008 bytes from 90.182.112.78: icmp_req=4 ttl=53 time=12.2 ms
1008 bytes from 90.182.112.78: icmp_req=5 ttl=53 time=12.9 ms

--- 90.182.112.78 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 12.270/13.768/17.037/1.688 ms
```

Výsledek skriptu

## Příloha 3 - Skript GSM module info a výsledek Troubleshooting Tool

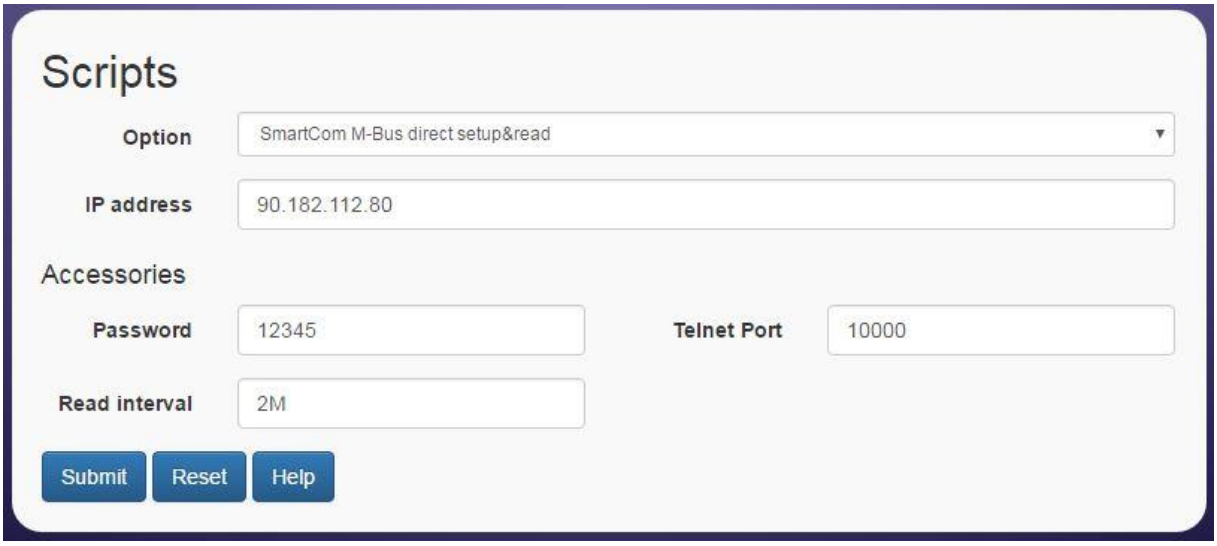



Nastavení skriptu

```
[2][ VoiceBlue Next ]  V-1.26.3.29.4  B-1.0
Date/time: 8.5.2016/11:12:16.78
SNumber: M201-5405650258

Login:

Password:

OK


int type      lay1/g/s   layer2  layer3     B1/simid  B2        mode/B3/netw
-------------------------------------------------------------------------------
#ax aux-test                     NULL
#vi voip      [4]        ----    NULL       NULL      NULL      NULL
-------------------------------------------------------------------------------
#00 MC55i     (off)  /0  BLOCK   NULL       Sim-err
#01 MC55i     (off)  /0  BLOCK   NULL       Sim-err
#02 MC55i     (off)  /0  BLOCK   NULL       Sim-err
#03 MC55i     (off)  /0  BLOCK   NULL       Sim-err

OK


#00 MC55i           gsm module g00
-------------------------------------------------------------------------------
    Layer2:         BLOCK
    Layer3:         NULL
    Network:
    Netid:          (off)  /0
    Netcell:        0,000,000,00000000,-1
    Modid:          MC55i
    Revid:          01.201
    Sernum:         359108048608341
    Simid-1:        Sim-err
    Simid-2:        Sim-err

OK

#01 MC55i           gsm module g01
-------------------------------------------------------------------------------
    Layer2:         BLOCK
    Layer3:         NULL
    Network:
    Netid:          (off)  /0
    Netcell:        0,000,000,00000000,-1
    Modid:          MC55i
    Revid:          01.201
    Sernum:         359108048607897
    Simid-1:        Sim-err
    Simid-2:        Sim-err

OK


#02 MC55i           gsm module g02
-------------------------------------------------------------------------------
    Layer2:         BLOCK
    Layer3:         NULL
    Network:
    Netid:          (off)  /0
    Netcell:        0,000,000,00000000,-1
    Modid:          MC55i
    Revid:          01.201
    Sernum:         359108049156100
    Simid-1:        Sim-err
    Simid-2:        Sim-err

OK


#03 MC55i           gsm module g03
-------------------------------------------------------------------------------
    Layer2:         BLOCK
    Layer3:         NULL
    Network:
    Netid:          (off)  /0
    Netcell:        0,000,000,00000000,-1
    Modid:          MC55i
    Revid:          01.201
    Sernum:         359108048607145
    Simid-1:        Sim-err
    Simid-2:        Sim-err

OK
Error with other GSM modules. The list of GSM modules in VoiceBlue are 4.Best regards, Technical Support.
```

Výsledek skriptu

## Příloha 4 - Skript SmartCom M-Bus direct setup&read a výsledek Troubleshooting Tool

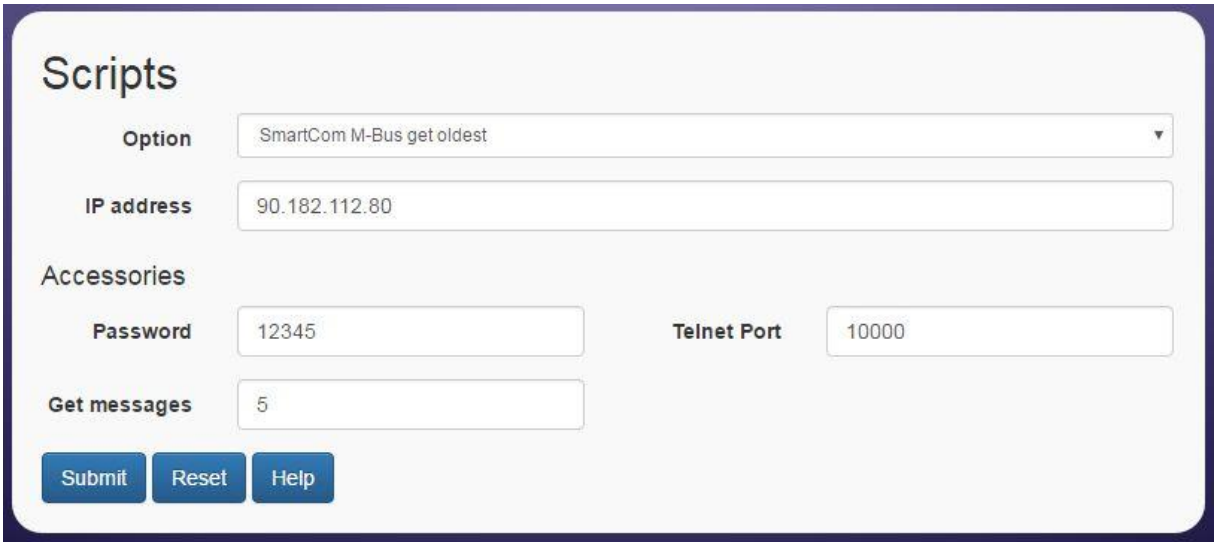



Nastavení skriptu

```
PASSWORD:
OK
at^scport2="save"
OK
AT^SCAMS="ENABLE",1
OK
AT^SCAMS="DEV_ADD",2,"MBUS","254@2400","2M"
OK
AT^SCAMS="direct_read",2,"MBUS","254@2400",
^SCAMS:
0,"","685E5E6808007268170308653299067300000000C13502100000B22060305046D1D091025326C00000C78
6817030806FD0C0A000100FA010DFD0B05313248465701FD0E004C1310200000426CFF1C0F37FD170000000000
000000027A2502027825026916"
OK
```

Výsledek skriptu

## Příloha 5 - Skript SmartCom M-Bus get oldest a výsledek Troubleshooting Tool




Nastavení skriptu

```
PASSWORD:
OK
AT^SCDATA="GET_OLDEST",3
^SCDATA:
"AMS",1463344502,55995,"MBUS",1,0,"","685E5E6808007268170308653299069200000000C13502100000B
22960205046D01170F25326C00000C786817030806FD0C0A000100FA010DFD0B053132484657 01FD0E004C1310
200000426CFF1C0F37FD17000000000000000000027A2502027825020816"
^SCDATA:
"AMS",1463344562,55996,"MBUS",2,0,"","685E5E6808007268170308653299069300000000C13502100000B
22960205046D02170F25326C00000C786817030806FD0C0A000100FA010DFD0B053132484657 01FD0E004C1310
200000426CFF1C0F37FD17000000000000000000027A2502027825020A16"
^SCDATA:
"AMS",1463344682,55997,"MBUS",2,0,"","685E5E6808007268170308653299069400000000C13502100000B
22960205046D04170F25326C00000C786817030806FD0C0A000100FA010DFD0B053132484657 01FD0E004C1310
200000426CFF1C0F37FD17000000000000000000027A2502027825020D16"
OKNumber of saved messages:
AT^SCDATA?
^SCDATA: "MESS_CNT",480
^SCDATA: "GET_SPACE",127
^SCDATA: "GET_FILTERED",""
OK
```

Výsledek skriptu