Západočeská univerzita v Plzni
Fakulta aplikovaných věd
Katedra informatiky

DIPLOMOVÁ PRÁCE

Systém pro řízení a monitorování síťového provozu

Vypracoval: Bc. Radek Vozák
Vedoucí práce: Ing. Jiří Ledvina, CSc.

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně a že jsem uvedl všechny zdroje a literaturu, ze kterých jsem čerpal.

V Plzni dne 26.6.2014

Podpis: .....

Abstrakt

Tato práce se zabývá realizací systému pro řízení a monitorování síťového provozu na prvcích Mikrotik RouterBoard s operačním systémem RouterOS. Pro testy byly vybrány routery RB1100, RB433AH, RB600, RB2011L, RB450 a testovací server Intel s operačním systémem Ubuntu 13.10. Prvním úkolem je seznámení s hardwarem RouterBoard a softwarem RouterOS a možnostmi použití v oblasti monitorování a řízení síťového provozu. Následujícím krokem je vytvoření vlastního systému, který zahrnuje: monitorování prvků v síti, řízeních a priorizaci datových toků a webové rozhraní pro snadné ovládání. Posledním krokem je otestování systému na vybraných routerech a ověření funkčnosti navrženého systému.

Abstract

This work deals with realization of a system for controlling and monitoring of network traffic on routers Mikrotik RouterBoard with the operating system RouterOS. The routers RB1100, RB433AH, RB600, RB2011L, RB450 and the testing server Intel with the operating system Ubuntu 13.10 were chosen for the testing of the system. The first task is familirization with the hardware RouterBoard and the software RouterOS and the possibility of usage in the area of monitoring and controlling network traffic. The next step is the actual realization of the system which includes: monitoring of the routers in the network, controlling and priorization of data-flows and a web interface for easy controlling of the system. The last step is system-testing on the chosen routers and verification of functionality of the designed system.

Poděkování

Na tomto místě bych rád poděkoval Ing. Jiřímu Ledvinovi, CSc., vedoucímu práce, za cenné rady, připomínky a metodické vedení. Dále své rodině za vytvoření vhodných podmínek pro psaní diplomové práce a svým přátelům za psychickou podporu.

Obsah

Přehled zkratek

Zkratka	Celé slovo
ARP	Address Resolution Protocol
ASBR	Autonomous System Boundary Routers
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CCR	Cloud Core Router
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HDLC	High-Level Data Link Control
HT	Hyper-Threading
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPSEC	IP security
ISP	Internet Service Provider
LSA	Link-state Advertisement
MAC	Media Access Control
NAT	Network Address Translation
OSPF	Open Shortest Path First
PCQ	Per Connection Queue
PoE	Power over Ethernet
POP3	Post Office Protocol Version 3
RAM	Random Access Memory
RB	Router Board
RED	Random Early Detection
RFC	Request for Comments
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RSVP	Resource Reservation Protocol
SFP	Small Form-factor Pluggable Transceiver
SFQ	Stochastic Fairness Queuing
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus

1 Úvod

Internet, WiFi, router, „megabit“ a mnoho dalších pojmů z oblasti informačních technologií proniká každým dnem čím dál tím víc do podvědomí běžných uživatelů, aniž by si to sami uvědomovali nebo o to měli zájem. Kdo by si dnes uměl představit svět bez Facebooku, novinek na Seznamu, počítačových online her a dalších vymožeností moderní doby. Tyto pojmy se stávají denních chlebem každého z nás a jediný rozdíl mezi jednotlivými uživateli je ten, že pro každého jedince jsou tyto služby jinak důležité.

Od dítěte, chystajícího si plynule zahrát online hru se svými kamarády, přes pracující střední generaci toužící po stabilním a rychlém přístupu na web až po naše prarodiče, kteří si pouze chtějí jednoduše popovídat se svými příbuznými po Skypu. A právě v této chvíli nastupuje na scénu monitorování a řízení síťového provozu, díky němuž je možné každému uživateli sítě upřednostnit právě tu službu, která ho nejvíce zajímá.

Téma diplomové práce jsem si vybral proto, abych se pokusil zdokonalit řízení a stabilitu datových toků v síti občanského sdružení PlzenecNET, o.s., kterou buduji již od svých šestnácti let.

Prvním bodem této práce bude popis aktuálně používaných prvků firmy Mikrotik RouterBoard, na nichž je tato síť od začátku svého vzniku budována. V současnosti obsahuje několik stovek zařízení tohoto typu. Popsány budou desky, komunikační rozhraní a rozšiřující moduly.

Druhým bodem bude stručný popis teorie síťové komunikace, který je potřebný k definici základních pojmů, se kterými se bude v dalším textu pracovat. Budou zde vysvětleny principy komunikace mezi dvěma síťovými prvky v počítačové síti.

Následovat bude představení operačního systému RouterOS instalovaném na tomto typu hardwaru. Důraz bude brán na záležitosti, které jsou podstatné pro základní nastavení systému, zprovoznění počítačové sítě, řízení datových paketů skrz síť a dohled aktivních prvků.

Za stěžejní a nejnáročnější část celé práce považuji návrh pravidel pro řízení síťového provozu a priorizaci datových paketů v síti. Zápis konfigurace do jednotlivých prvků bude probíhat skrz jednoduché webové rozhraní. Součástí systému bude i zobrazení monitorovaných dat. V této části bude kladen důraz na to, aby bylo možné jednotlivým uživatelům nastavit vlastní prioritní model.

Posledním důležitým bodem k dokončení celé práce bude nasazení celého systému v reálných podmínkách a následné zdokumentování jeho chování. Hardware občanského sdružení PlzenecNET, o.s. mi bude pro tyto účely k dispozici.

2 Mikrotik RouterBoard

Mikrotik RouterBoard je v informačních technologiích označení pro malé základní desky, které jsou uživatesky rozšiřitelné o doplňující prvky (bezdrátové miniPCI karty, externí antény, paměti, SFP moduly, ...). Výsledný prvek lze následně použít například jako bezdrátový přístupový bod, router, optický či metalický switch, bezdrátový klientský router nebo podobné síťové prvky. V základní konfiguraci obsahují RouterBoardy procesor, integrovanou operační paměť a dle typu desky několik síťových karet, SFP slotů, USB portů, miniPCI-E slotů atd. Jako základní operační systém dodávaný pro desky Mikrotik RouterBoard je systém RouterOS, který je založen na Linuxu a budu o něm mluvit podrobněji v dalších kapitolách. Je však možno využít i jiné Linuxové distribuce a díky tomu zakomponovat desky to téměř jakékoliv počítačové sítě.

2.1 Architektury

Dělení RouterBoardů podle architektury je velmi důležitou součástí při instalaci operačního systému. Přestože se operační systém dodává předinstalovaný, velmi často se jedná o neaktuální verzi a je hned při prvním spuštění vhodné stáhnout nejnovější fimrware s instrukční sadou pro daný typ procesorů. Použití daného typu procesorů určuje dané skupině velmi často zaměření, pro které je vhodné tyto typy RouterBoardů použít. Firma Mikrotik v současné tobě rozlišuje tyto architektury:

2.1.1 MIPSBE

- CRS série - jedná se o chytré přepínače z řady Smart Switch s možností vyhrazení portů pro routování
- RB4xx série - desky s větším množstvím ethernetových portů či miniPCI slotů. Velmi často využívané poskytovateli internetového připojení
- RB7xx série - desky sloužící pro bezdrátové spoje a kancelářské routery
- RB9xx série - desky sloužící pro bezdrátové spoje a kancelářské routery
- RB2011 série - středně výkonné víceportové routery pro nasazení v menších firmách
- SXT - bezdrátové klientské zařízení s duální anténou na krátkou vzdálenost
- OmniTik - bezdrátový přístupový bod s duální anténou
- Groove - bezdrátový klientský RouterBoard připojitelný přímo na anténu pomocí konektoru N
- METAL - bezdrátový klientský RouterBoard připojitelný přímo na anténu pomocí konektoru N v kovovém provedení
- SEXTANT - bezdrátové klientské zařízení s duální anténou většího zisku

2.1.2 PPC - PowerPC

- RB3xx série - desky s větším množstvím ethernetových portů či miniPCI slotů
- RB600 série - desky sloužící pro výkonné bezdrátové přístupové body ISP
- RB800 série - desky sloužící pro výkonné bezdrátové přístupové body ISP
- RB1xxx série - velmi výkonné víceportové routery, vhodné jako centrální prvky

2.1.3 MIPSLE

- RB1xx série - starší RouterBoardy s větším množstvím ethernetových portů či miniPCI slotů.
- RB5xx série - starší typ desky sloužící pro malé bezdátové přístupové body ISP

2.1.4 TILE

- CCR série - nejnovější řada centrálních víceportových routerů s šestnácti nebo třicetišesti jádry.

2.2 Hardwarová vybavenost a značení

Výběr vhodného RouterBoardu pro konkrétní aplikaci není jednoduchou záležitostí. Je potřeba zvážit především parametry, které souvisejí s datovou propustností jednotlivých prvků. Pro tuto klasifikaci je rozhodujícím parametrem výkon procesoru. Pokud je třeba zařízení nasadit v aplikacích, které potřebují ukládat data na vestavěnou paměť, bude rozhodujícím parametrem velikost paměti RAM. Dalším kritériem může být počet metalických, optických či bezdrátových interfaců. Díky opravdu velice rozsáhlé nabídce RouterBoardů zavedla firma Mikrotik značení, které specifikuje danou hardwarovou výbavu vybrané desky. Toto rozlišení pomocí velkých písmen se ovšem týká pouze modelů, které mají několik verzí. Mikrotik aktuálně rozlišuje tyto verze:

- A - více paměti pro ukládání uživatelských dat
- H - vyšší výkon procesoru
- G - gigabitové ethernet porty
- U - přítomnost USB portu pro připojení k UPS nebo externí paměti
- R - označení pro desku s integrovanou bezdrátovou kartou
- N - podpora protokolu 802.11n u bezdrátových karat
- L - verze „lite“ - chudší výbava oproti klasickým verzím, avšak při zachování výkonu

Příklad označení RouterBoardu je: RB433UAHL. Z názvu je možné rovnou odvodit, že se jedná o desku typu RB433 (architektura MIPSBE), která je vybavena portem USB, rozšířenou vestavěnou pamětí RAM, výkonnějším procesorem, ale zároveň se jedná o verzi „lite“, která značí absenci portu RS-232 a umělé ethernet porty místo kovových. Čísla za modelovou řadou korespondují s počtem ethernetových portů a miniPCI slotů. Z názvu „RB433“ je proto možné vyčíst, že se jedná o RouterBoard se třemi metalickými porty o rychlosti 10/100 Mbps a třemi sloty miniPCI pro připojení rádiových karet. Jak RouterBoard typu RB433UAHL vypadá, je možno vidět na Obrázku číslo 1.

Obrázek 1: RB433UAHL

2.3 Komunikační interface

Většina dnešních datových sítí není postavena jen na jednom typu přenosového média. Skoro ve všech případech se jedná o kombinaci optické, metalické a bezdrátové sítě. Při volbě správného RouterBoardu se proto nesmí opomenout výběr správného typu a množství komunikačních rozhraní (interfaců).

Od zařízení s jedním metalickým portem a jedním bezdrátovým slotem, které slouží často jako WiFi klientská jednotka (např: RB911), je možné postupně navyšovat počet těchto interfaců do požadované konfigurace (RB493AH s 9x ethernetovmý portem a 3x miniPCI slotem). Samozřejmostí je existence čistě ethernetových routerů (5 - 13 portů), které jsou v současnosti pořád častěji doplňovány o porty optické (SFP).Velmi rozšířeným RouterBoardem v optických sítích se stal typ RB2011LS, který je díky jednomu SFP slotu, deseti metalickým portům a velmi příznivé ceně často využíván jako koncové zařízení klientů připojených do této sítě. Komunikační rozhraní RouterBoardů se dají rozdělit do kategorií:

2.3.1 Metalické porty

Jedná o základní komunikační interface, který lze najít na každém RouterBoardu. Skrz tento port dochází k provotní konfiguraci RouterBoardu administrátorem. Do těchto portů je možné připojit všechny kabely vyhovující standardům cat.5,6,7 a propojit tak desku

s počítačem nebo jiným prvkem počítačové sítě. Rozlišovat můžeme z hlediska rychlosti, provedení a podporou napájení po ethernetu a to následujícím způsobem:

- Rychlost:
  - 10/100 Mbps porty - podpora Fast Ethernetu definovaného normou IEEE 802.3u
  - 10/100/1000 Mbps porty - podpora Gigabitového Ethernetu definovaného normou IEEE 802.3ab pro kroucenou dvoulinku
- Provedení:
  - kovové - klasické provedení, možnost propojení se stíněným kabelem
  - plastové - provedení ve verzi Lite
- Napájení:
  - bez podpory napájení - slouží pouze k přenosu dat
  - s podporou nápájení - tzv. PoE (Power over Ethernet) - slouží k napájení prvků po ethernetovém kabelu. Využívá se, pokud je jednotka umístěna ve venkovním prostředím daleko od elektrické sítě. Odpadá tak nutnost vést druhý napájecí kabel. PoE je definované normou 802.3af.

Jak takovéto porty vypadají v praxi, je možné vidět na Obrázku číslo 2. Na desce typu RB450G je pět kovových metalických portů s podporou Gigabitového Ethernetu a na portu 1 je viditelné označení pro podporu napájení po Ethernetovém kabelu. Při použití PoE je potřeba dodržet vstupní napětí 10-28V. Délka kabelového vedení, při kterém bude napájení po Ethernetu fungovat, roste s použitím kvalitnější kabeláže a s velikostí výstupního napětí napájecího adaptéru. Při 12V je možné dosáhnout vzdálenosti cca 20m. 24V už dovoluje jednotky napájet na vzdálenost až 50m.

Obrázek 2: B450GPOE

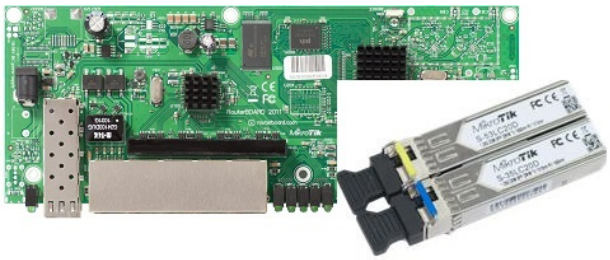
2.3.2 Optické moduly

Díky klesající ceně optických prvků, vláken a příslušenství jsou RouterBoardy stále častěji vybavovány rozhraním pro optickou komunikaci. Pokud chceme kabelovou cestou překonat vzdálenost větší, než jsou řádově stovky metrů, případně se chceme vyhnout interferencím, které jsou patrné na metalickém vedení, je použití optické technologie jedinou cestou.

Protože se Mikrotik vydal cestou variabilní desky, nejsou RouterBoardy vybaveny jedním typem optického převodníku, ale pouze šachtou umožnující do desky zasunout SFP (small form-factor pluggable) moduly. Uživateli je tak dovoleno vybrat si mezi moduly s různou rychlostí a technologií přenosu. Moduly, které Mikrotik podporuje, můžeme proto rozdělit to následujících skupin:

- Rychlost:
  - 10/100 Mbps SFP moduly - v dnešní době už se skoro nepoužívají
  - 10/100/1000 Mbps SFP moduly - nejrozšířenější
  - 10Gbit moduly - v současné době desky zatím nepodporují, samotný operační systém RouterOS už ano
- Podpora vláken:
  - Single mode - moduly pracující s tímto typem vláken umožňují přenos až na 20km. Nejčastěji je použita vlnová délka 1310nm.
  - Multi mode - moduly pro spojení vzdáleností do cca 550m. Použití vlnové délky 850nm.
- Technologie přenosu:
  - přenos po dvou vláknech - SFP modul je vybaven dvěma konektory. Jedno vlákno slouží pro příjem a druhé pro vysílání. Oba dva směry mohou vysílat na stejně vlnové délce.
  - Přenos po jednom vláknu - jedná se o technologii WDM (Wavelength Division Multiplexing - vlnový multiplex). Moduly jsou při tomto typu přenosu na každé straně optické trasy rozdílné a prodávají se proto v párech. Při přenosu jsou použity dvě vlnové délky, jedná pro vysílání a druhá pro příjem dat. Nejčastěji se jedná o kombinaci 1310/1550 nm.

Vzhledem k velikosti modulů SFP je vždy použit jeden nebo dva konektory typu LC. Na následujícím Obrázku číslo 3 je vidět RouterBoard 2011LS, jeho šachta pro SFP a jeden pár optických SFP modulů S-3553LC20D.



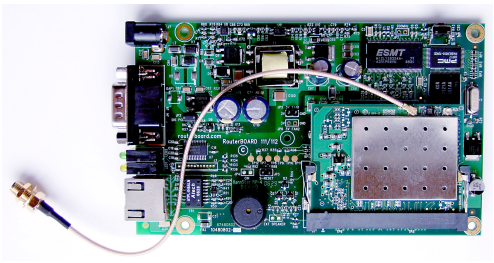
Obrázek 3: RB2011 s SFP moduly WDM

2.3.3 Bezdrátové miniPCI adaptéry

Česká republika je v současnostni Wi-Fi velmocí Evropy, proto je největší portfolio Mikrotiku zaměřeno na bezdrátové prvky. Bez rozšiřitelnosti RouterBoardů o bezdrátové miniPCI adaptéry by určitě většina ISP sáhla po řešení od konkurenčních výrobců jako například Ubiquti Networks. Svoje uplatnění si ale najdou i RouterBoardy s vestavěnou bezdrátovou částí. Dělení prvků je v tomto případě velmi jednoduché:

- RouterBoardy s vestavěnou bezdrátovou kartou bez možnosti rozšíření:
  - Vestavěná karta s integrovanou anténou - routery pro použití jako domácí/firemní přístupový bod. Př: RB951G-2HnD
  - Vestavěná karta s výstupem na externí anténu - desky použitelné pro páteřní spoje. Př: RB911G-5HPnD
  - Vestavěná karta s přímo připojenou externí anténou - bezdrátové klientské routery. Př: SXT 5HnD
- RouterBoardy s možností rozšíření o miniPCI bezdátové karty:
  - MiniPCI karty pro pásmo 2,4GHz - vysílače pro mobilní telefony a notebooky. Př: WNC CM9
  - MiniPCI karty pro pásmo 5GHz-a - vysílače pro připojení klientů v pásmu 5GHz. Př: Mikrotik R52
  - MiniPCI karty pro pásmo 5GHz-n - vysílače pro připojení klientů v pásmu 5GHz-n. Př: MikroTik R52Hn
  - MiniPCI karty pro pásmo 3,5GHz-n - karty pro spoje v licencovaném pásmu 3,5GHz. Nutné oprávnění ČTU. Mikrotik tyto karty nevyrábí, ale podporuje připojení karet UBNT XR3

Jak připojení miniPCI bezdrátové karty vypadá v reálu, je možné si prohlédnout na Obrázku číslo 4. Je zde znázorněn již historický typ RouterBoard 112 s osazenou jednou bezdátovou miniPCI kartou typu Mikrotik R52. Karta má připojený pigtail zakončený konektorem R-SMA pro připojení externí antény.



Obrázek 4: RB112 s miniPCI kartou R52

2.3.4 Ostatní

RouterBoardy mají i další rozhraní, přes které je možné komunikovat s okolím. Dále je zde možné nalézt čidla a výbavu pro akustickou či optickou komunikací s uživatelem. Patří mezi ně:

- USB konektor - slouží pro připojení externí paměti, dohledu záložních zdrojů nebo 3G modemů
- RS232 - sériový port slouží pro konfiguraci RouterBoardů
- Teplotní senzor - snímání teploty
- Reproduktor - zvukové zaměřování spojů, potvrzení naběhnutí operačního systému
- Diody - optická kontrola běhu zařízení. Diody je také možné použít k zaměřování spojů.

3 Teorie síťové komunikace

Než bude možné přistoupit k popisu síťových funkcí operačního systému RouterOS, je bezprostředně nutné popsat, jak fungují základy síťové komunikace mezi zařízeními v síti.

Aby bylo možné hovořit o síťové komunikaci, je potřeba nejdříve nadefinovat pojem síťová architektura. Síťová architektura je struktura, která má na starost řízení síťové komunikace v systémech a výměnu jejich dat. Vznik první architektury je úzce spjatý se vznikem prvních počítačových sítí. Postupným vývojem došlo k vytvoření dvou hlavních koncepcí: Modelu ISO/OSI a TCP/IP. Obě tyto architektury se od sebe odlišují následovně:

- ISO/OSI - sedmivrstvý model. Systém navržen pro spolehlivé a spojované služby. Zajištění spolehlivosti zasahuje až do komunikační podsítě (tj. až do úrovně síťové vrstvy). Hostitelské počítače mají relativně jednoduchou úlohu. Spojované služby jsou realizovány mechanismem virtuálních okruhů.
- TCP/IP - čtyřvrstvý model. Zajištění spolehlivosti je problémem koncových stanic a je řešeno až na transportní vrstvě. Ušetřená režie (čas) je použita pro vlastní přenos. TCP/IP proto není tak spolehlivá architektura jako ISO/OSI, nicméně poskytuje rychlou a jednoduchou komunikační síť. Využívá nespojovaný charakter přenosu - tedy jednoduchou datagramovou službu.

Pro pochopení fungování síťové komunikace je potřeba podrobně popsat funkci jednotlivých vrstev a zavést pojmy komunikační port, rámec, paket a segment. Následující text předpokládá znalost pojmů MAC adresa a IP adresa.

3.1 Architektura ISO/OSI

V roce 1984 byla přijata norma ISO 7498, která definovala použití referenčního modelu ISO/OSI vypracovaného firmou International Organization for Standardization (ISO). Norma uvádí základní principy sedmivrstvé síťové architektury. Popisuje jednotlivé vrstvy, kde každá ze sedmi vrstev vykonává skupinu jasně definovaných funkcí potřebných pro řádnou komunikaci. Pro svoji činnost využívá služeb sousední, nižší vrstvy. Naopak své služby pak poskytuje vrstvě vyšší. Mezi sedm vrstev patří:

3.1.1 Fyzická vrstva

Úkolem fyzické vrstvy je zakódování jednotlivých bitů rámce sestrojeného linkovou vrstvou do signálu určeného pro přenos přes fyzické médium a následně tento signál odeslat/přijmout. Signál může být optický, mikrovlnný nebo elektrický. Součástí fyzické vrstvy jsou:

- přenosové médium a konektory
- způsob reprezentace dat na daném médiu
- způsob, jakým jsou data zakódována

3.1.2 Linková vrstva

Zajišťuje spojení mezi dvěma fyzicky přímo propojenými uzly sítě. Uspořádává data z fyzické vrstvy do celků nazývaných rámce a zajišťuje i zpětný proces. Jak rámec vypadá je možné vidět na Obrázku číslo 5.

Obrázek 5: Rámec

- 6 bajtů cílová fyzická adresa (DA - Destination Address)
- 6 bajtů zdrojová fyzická adresa (SA - Source Address)
- 2 bajty typ protokolu (TYPE)
- 46-1500 bajtů přenášená data (DATA)
- 4 bajty kontrolní součet (CRC)

Vrstva řídí vysílání a uspořádávání přenášených rámců, nastavuje parametry přenosu a detekuje neopravitelné chyby. Formátuje fyzické rámce a opatřuje je fyzickou adresou (MAC adresou). MAC adresa se skládá z 48 bitů a zapisuje se ve formátu šesti dvojciferných hexadecimálních čísel oddělených dvojtečkou (př: 00:15:17:FA:CD:B9). Adresa je přiřazena síťové kartě při její výrobě a slouží jako jednoznačný identifikátor síťového zařízení.

Pro vyšší vsrtvy zajišťuje linková vrstva nezávislost na konkrétním typu přenosového média. Od síťové vrstvy přijímá linková vrstva paket, který doplní o hlavičku a patičku, tím vznikne rámec. Obsahem hlavičky a patičky jsou tyto informace:

- informace o začátku a konci rámce
- zdrojová a cílová fyzická adresa zařízení (tzv. MAC adresa)
- typ zprávy - definuje, o který protokol se jedná
- CRC - kontrolní součet použitý pro detekci chyb

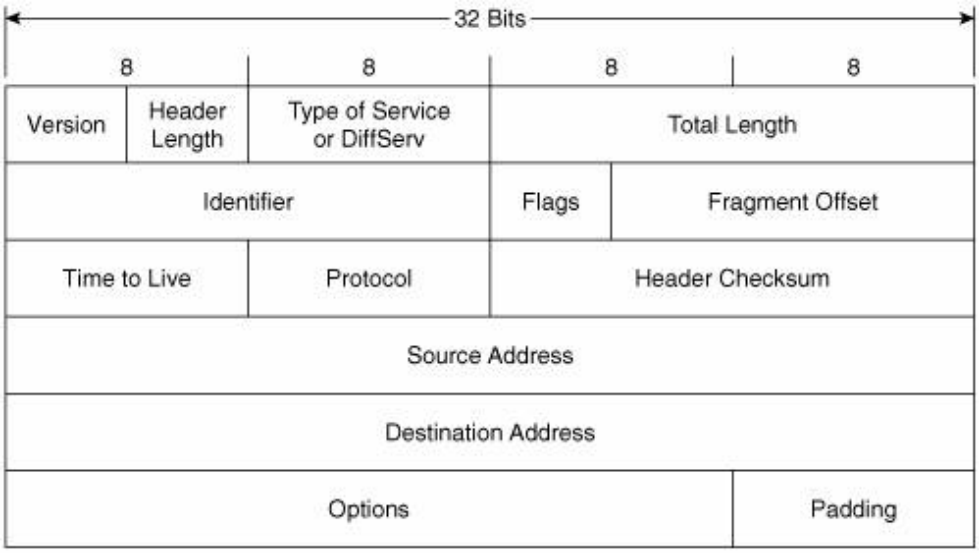
Příkladem protokolu linkové vrstvy je Ethernet, který je používaný ve většině dnešních sítí. Mezi zařízení působící na této vrstvě patří:

- most (Bridge) - starší zařízení než switch, v dnešní době se skoro nepoužívá
- přepínač (Switch) - větší datová propustnost, více portů

3.1.3 Síťová vrstva

Tato vrstva se stará o adresování a směrování datových toků v sítích. Zprostředkovává výměnu dat ve formě paketů mezi koncovými zařízeními, která spolu nejsou přímo spojena (jsou propojena skrz síť). Přijímá od vyšší transportní vrstvy segment, ke kterému přidá svojí hlavičku a tím vytváří paket. Jak paket vypadá a co obsahuje, je možné vidět na Obrázku číslo 6. Adresace se provádí pomocí IP adres, které můžou být verze 4 nebo verze 6.

- Příklad zápisu IPv4 adresy - 89.203.220.194/30
- Příklad zápisu IPv6 adresy - 2001:1a48:ffff::352/64



Obrázek 6: Paket IPv4 síťové vrstvy

- 4 bity specifikující, jestli se jedná o IPv4 nebo IPv6 paket (Version)
- 4 bity označující délku hlavičky vynásobenou 4 (IHL)
- 8 bitů označující typ služby (Type of Service)
- 16 bitů označující délku paketu v bytech (Total Length)
- 16 bitů označující identifikační tag pomáhající k rekonstrukci paketu z více fragmentů (Identification)
- 3 bity, které označují, zda je možno paket fragmentovat (Flags)
- 13 bitů označujících offset fragmentu (Fragment Offset)

- 8 bitů obsahující hodnotu TTL (Time to live); označují, přes kolik routerů může paket projít, než bude zničen
- 8 bitů označující protokol (Protocol (IP))
- 16 bitů obsahující kontrolní součet CRC (Header Checksum)
- 32 bitů obsahující zdrojovou IP adresu (Source Adress)
- 32 bitů obsahující cílovou IP adresu (Destination Address)

Nejznámějším protokolem síťové vrstvy je protokol IP. Mezi zařízení působící na této vrstvě patří Směrovače (Routery).

3.1.4 Transportní vrstva

Úkolem transportní vrstvy je identifikovat komunikace jednotlivých aplikací a předávat přijatá data příslušné aplikaci. Transpotní vrstva přijímá z vyšších vrstev souvislý datový tok a před odesláním dělí tento tok do segmentů (tzv. segmentace). Při přijetí naopak tyto segmenty sestavuje (tzv. reassembling). Adresace se provádí pomocí komunikačních portů v rozsahu 0 - 65535. Přidělování portů je řízeno doporučeními organizace IANA.

- 0 - 1023 - Well known porty (systémové porty)
- 1024 - 49151 - Registered (uživatelské porty)
- 49152 - 65535 - Dynamic (dynamické porty)

Nejznámějšími protokoly transportní vrstvy jsou protokoly UDP a TCP.

- TCP (Transmission Control Protocol) - tento protokol zaručuje spolehlivé doručování a správné pořadí dat
- UDP (User Datagram Protocol) - „nespolehlivý“ protokol - nezaručuje, zda se paket neztratí nebo zda paket bude doručen ve zprávném pořadí

Příkladem může být například Telnet fungující na protokolu TCP a na portu 23 nebo Winbox používaný pro konfiguraci RouterOS, který funguje na protokolu TCP a portu 8291.

3.1.5 Relační vrstva

Umožňuje vytvoření a ukončení relačního spojení, synchronizaci a obnovení spojení. Obecně lze říci, že úkolem této vrstvy je synchronizovat dialog mezi spolupracujícími relačními vrstvami obou systémů, které spolu komunikují a řídit výměnu dat mezi nimi. Obnovení spojení je zajištěno pomocí synchronizačních značek, které vytváří právě relační vrstva. Datové jednotky přenášené relační vrstvou se nazývají Session Layer Protocol Data Unit. Příkladem protokolů relační vrstvy jsou:

- RPC (Remote Procedure Call) - vzdálené volání procedur
- SSL (Secure Socket Layer) - zabezpečení a šifrování spojení

3.1.6 Prezentační vrstva

Hlavní funkcí vrstvy je transformovat data do tvaru, který používají aplikace. Formát dat nemusí být na komunikujících systémech stejný, proto prezentační vrstva zajišťuje převod mezi syntaxí používanou na daném systému a syntaxí obecnou. Prezentační vrstva se zabývá pouze strukturou dat, nikoliv jejich významem. Mezi funkce patří např. přizpůsobení pořadí bajtů, převod kódů a abeced. Datové jednotky přenášené presentační vrstvou se nazývají PPDU (Presentation Layer Protocol Data Unit). Funkce prezentační vrstvy jsou

- Šifrování dat
- Komprimace dat
- Konvertování dat

3.1.7 Aplikační vrstva

Jedná se o vrstvu nejbližší uživateli, která již nezajišťuje služby pro vyšší vrstvu. Příklady funkcí zajišťovaných touto vrstvou jsou souborové přenosy, sdílení zdrojů, přístup k databázím, prohlížení webových stránek, ovládání programů, apod. Datové jednotky přenášené aplikační vrstvou jsou APDU (Application Layer Protocol Data Unit).

3.2 Architektura TCP/IP

TCP/IP je síťová architektura, která vznikla v sedmdesátých letech. Byla vytvořena ministerstvem obrany USA původně pro vojenské účely pod názvem ARPANET. Po ověření funkčnosti paketové (přepínané) technologie vláda rozhodla testovací síť nezrušit a tak se tato architektura dostala do akademického prostředí. Hned poté se do základního ARPANETU začaly přidávat nové protokoly a funkce a tím postupně vznikl dnešní Internet. Architektura TCP/IP využívá oproti architektuře ISO/OSI pouze čtyři vrstvy. Rozdíl odpovídajících vrstev je přehledně znázorněn na Obrázku číslo 7.

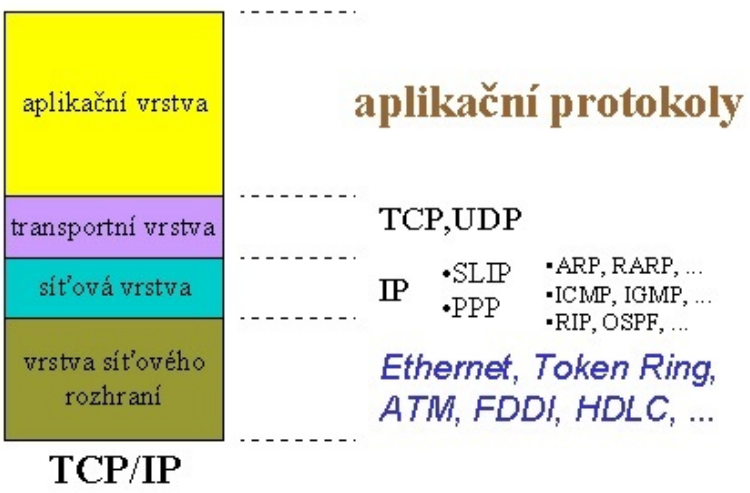
<table>
<tr><th>TCP/IP</th><th>Model ISO/OSI</th></tr>
<tr><td rowspan="3">Aplikační vrstva</td><td>Aplikační vrstva</td></tr>
<tr><td>Prezentační vrstva</td></tr>
<tr><td>Relační vrstva</td></tr>
<tr><td>Transportní vrstva</td><td>Transportní vrstva</td></tr>
<tr><td>Síťová (IP) vrstva</td><td>Síťová vrstva</td></tr>
<tr><td rowspan="2">Vrstva síťového rozhraní</td><td>Linková vrstva</td></tr>
<tr><td>Fyzická vrstva</td></tr>
</table>

Obrázek 7: Rozdíl mezi ISO/OSI a TCP/IP

Mezi základní čtyři vrstvy TCP/IP patří vrstva síťového rozhraní, síťová vrstva, transportní vrstva a vrstva aplikační. Schéma je možné vidět na Obrázku číslo 8.:

3.2.1 Vrstva síťového rozhraní

- nejnižší vrstva, které specifikuje samotný přístup k fyzickému přenosovému médiu. TCP/IP na této vrstvě nikterak nespecifikuje přenosové technologie. Předpokládá se, že použije to, co vznikne na základě jiných technologií (například Ethernet) a nepovažuje za potřebné znovu vyvíjet řešení, které je již funkční. TCP/IP si klade za úkol to, jak již tyto existující technologie co nejlépe využít a zpřístupnit je tak vyšším vrstvám. Každá přenosová technologie má svá specifika, mezi něž patří různé způsoby adresování, různá velikost přenášených rámců, různý charakter poskytovaných služeb. Příklady těchto technologií jsou:



Obrázek 8: Vrstvy TCP/IP

- Ethernet
- Token Ring
- ATM (Asynchronous Transfer Mode)
- FDDI (Fiber Distributed Data Interface)
- HDLC (High-Level Data Link Control)

3.2.2 Síťová vrstva

- vrstva, která již není závislá na konkrétní přenosové technologii, se nazývá vrstva síťová. Často se označuje jako Internet Layer (vrstva vzájemného propojení sítí) nebo je možné se setkat s označením IP vrstva. Úkol této vrstvy je přibližně stejný jako u síťové vrstvy v referenčním modelu ISO/OSI - stará se o to, aby se datové pakety dostaly od odesílatele skrz síť k příjemci přes případné směrovače (brány). Díky nespojovanému charakteru přenosu v TCP/IP je na úrovni této vrstvy zajištěna jednoduchá datagramová služba. Základním protokolem Internetové vrstvy je protokol IP a mezi další, používané a nejznámější patří např:

- ARP (Address Resolution Protocol)
- ICMP (Internet Control Message Protocol)
- IGMP (Internet Group Management Protokol)
- IPSEC (IP security)

Směrování v sítích TCP/IP je zajištěno pomocí směrovacích protokolů, které taktéž spadají do Internetové vrstvy. Nejčastěji je možné se setkat s:

- RIP (Routing Information Protocol) ve verzích 1 a 2
- OSPF (Open Shortest Path First)
- BGP (Border Gateway Protocol)

Podrobnější popis a základní principy fungování routovacích protokolů OSPF a BGP jsou uvedeny v kapitole 4.3.2.

3.2.3 Transportní vrstva

- využívá nespojovaný a nespolehlivý přenos na úrovni síťové vrstvy. Alternativně však nabízí i přenos spojovaný a spolehlivý. Transportní vrstva je implemetnována až v koncových zařízeních a umožňuje tak přizpůsobit chování sítě možnostem a potřebám aplikace. Základnímu protokoly této vrstvy jsou:

- TCP (transmission control protocol) - zajišťuje spolehlivý a spojovaný přenos
- UDP (user datagram protocol) - zajišťuje nespolehlivý a nespojovaný přenos. Je jen lehkou nadstavbou nad síťovou vrstvou a nijak nemění povahu přenosových služeb síťové vrstvy.

Oba protokoly slouží primárně k odlišení jednotlivých spojení na jedné IP adrese. Pokud se k jednomu serveru chce připojit vice klientů, použijí se k rozlišení jejich spojení tzv. porty. Pomocí portů je možné teoreticky rozlišit až 65535 spojení.

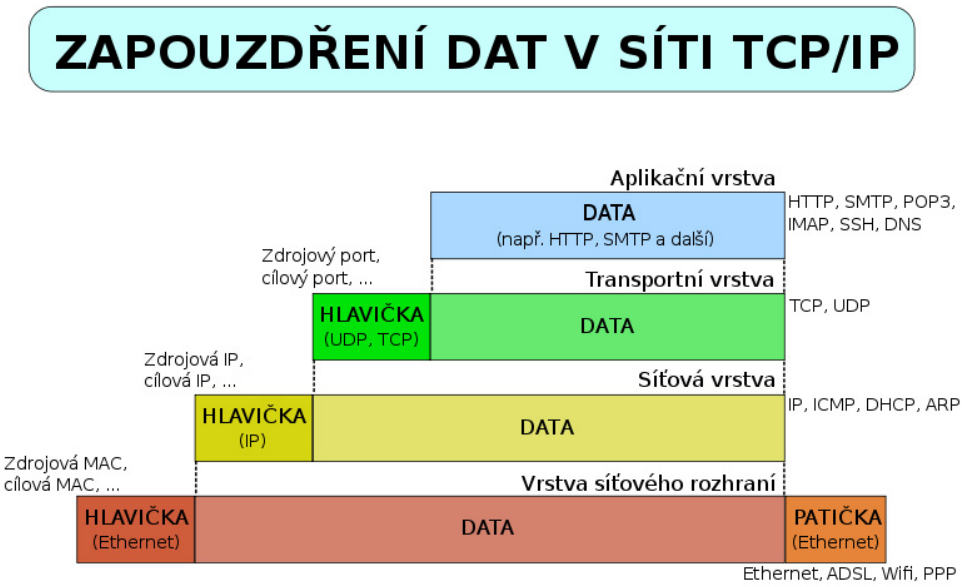
3.2.4 Aplikační vrstva

- tvoří nejvyšší vrstvu TCP/IP. Jejími entitami jsou jednotlivé aplikační programy či procesy, které oproti referenčnímu modelu ISO/OSI komunikují přímo s transportní vrstvou a využívají jejích služeb ve formě protokolů UDP a TCP. Funkce prezentační a relační vrstvy v modelu ISO/OSI si musejí v architektuře TCP/IP realizovat aplikační programy samostatně. Každé síťové spojení aplikace je jednoznačně určeno číslem portu, transportním protokolem a IP adresou počítače. Mezi nejznámější protokoly aplikační vrstvy patří například:

- HTTP (Hypertext Transfer Protocol)
- FTP (File Transfer Protocol)
- POP3 (Post Office Protocol)
- IMAP (Internet Message Access Protocol)
- DNS (Domain Name System)

3.3 Zapouzdření dat

Po podrobném popisu jednotlivých vrstev architektury TCP/IP je na Obrázku číslo 9 graficky znázorněno, co která vrstva přidává do výsledně odeslaných dat z daného zařízení. Data z aplikační vrstvy se při předání do vrstvy transportní rozšiřují o hlavičku, která uvádí zdrojový a cílový port komunikace. Při průchodu vrstvou síťovou se jedná o zdrojovou a cílovou IP adresu. V poslední řadě vrstva síťového rozhraní přidává do hlavičky zdrojovou a cílovou MAC adresu zařízení a do patičky typ technologie, kterou se data budou přenášet.

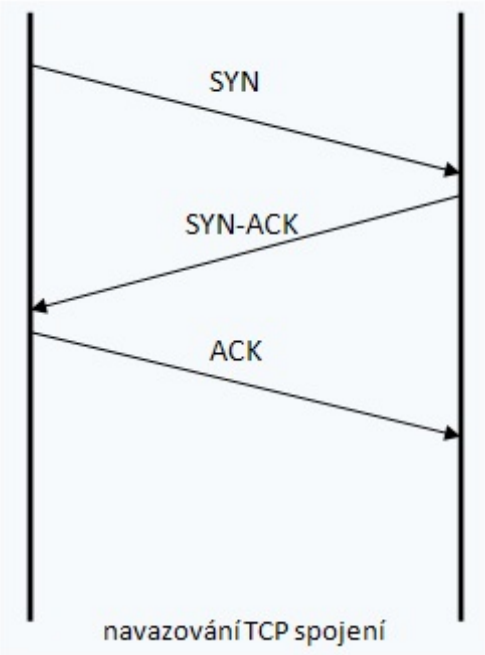


Obrázek 9: Zapouzdření dat v síti TCP/IP

3.4 Navázání síťového spojení

Jak detailně probíhá navázání síťového spojení, je nejlepší popsat na konkrétním případě. Klientský počítač se chystá kontaktovat webový server umístěný v internetu. Pomocí služby DNS klient zjistí převodní vztah mezi názvem a IP adresou cílového serveru. Následně začíná spojovací proces. PC vyšle do sítě broadcast a pomocí protokolu ARP zjistí MAC adresu brány. Jakmile ji obdrží vytvoří TCP paket s cílovým portem 80 a náhodně vybraným portem zdrojovým a nastaví mu flag SYN. K paketu přidá cílovou adresu webového serveru a svoji zdrojovou IP adresu. V posledním kroku se doplní zdrojová MAC adresa klienta a cílová MAC adresa brány. Takto vytvořený paket se odesílá do sítě. Brána po přijetí paketu přepíše hlavičku vrstvy síťového rozhraní a ověří v směrovací tabulce, zda má nějaké informace o cílovém webovém serveru. Následně nastaví cílovou MAC adresu nové brány a zdrojovou MAC adresu na MAC adresu odchozího rozhraní a posílá paket dále do sítě. Paket takto cestuje sítí až do segmentu, kde se nachází webový server. V posledním

kroku brána nastaví jako cílovou MAC adresu fyzickou adresu webového serveru. Webový server po přijetí paketu s flagem SYN odpovídá klientovi stejným paketem SYN-ACK. Paket cestuje stejným způsobem zpátky ke klientovi. Jakmile dorazí, klient odpovídá serveru paketem s flagem ACK. Tento proces se nazývá třícestný handshake a grafické znázornění je možné vidět na Obrázku číslo 10. Po úspěšném provedení tohoto procesu může začít skutečná datová komunikace.



Obrázek 10: Třícestný handshake

4 RouterOS

4.1 Základní informace

MikroTik RouterOS je routerový operační systém založený na Linuxu, vhodný zejména pro bezdrátové spoje. Firma Mikrotik začala s vývojem prvního operačního systému v roce 1995 v Lotyšsku. Získání zkušeností s PC bylo základním pilířem k vybudování routovacího softwaru MikroTik v2 PC, který přinesl výbornou ovladatelnost komunikačních periferií. Verze 2 byla také požadováná za první stabilní verzi.

4.1.1 Funkce operačního systému

Proměna obyčejného PC v plně nastavitelný a spolehlivý router nebyla ještě nikdy jednodušší. RouterOS je možné bez problému nainstalovat na architekturu x86. Z obyčejného PC lze tak během 30 minut získat velmi výkonný router s nepřeberným množstvím funkcionalit. Všechny tyto funkce lze samozřejmě provozovat i na deskách RouterBoard, na kterých se dodává RouterOS již předinstalovaný. Mezi základní funkce tohoto operačního systému patří:

- Router s podporou IPv4, Ipv6 a všech dynamických protokolů (RIP, OSPF,BGP)
- Omezující či bezpečnostní Firewall
- Proxy server, NTP server, DNS server
- Server pro monitorování síťového provozu
- Hotspot řešení pro hotely, restaurace a kavárny
- Gateway pro řízení přistupu uživatelů na internet

4.1.2 Licence

Funkcionalita operačního systému je omezena výběrem vhodné licence. V současné době Mikrotik rozlišuje šest licencí (podrobný přehled lze nalézt v Příloze 1) :

- L0 - Trial licence, která funguje pouze 24 hodin
- L1 - Demo licence - je potřeba registrace
- L3 - WISP CPE - licence pro bezdátové klienty, není možno vytvářet řežim přístupového bodu
- L4 - WISP - možno vytvářet přístupové body, veškerá funkcionalita je aktivní, počet tunelů (PPPoE, L2TP) omezen na 200
- L5 - WISP - stejné jako L4, navýšený počet aktivních tunelů
- L6 - Controller - všechny funkce dostupné bez omezení

4.2 Možnosti konfigurace

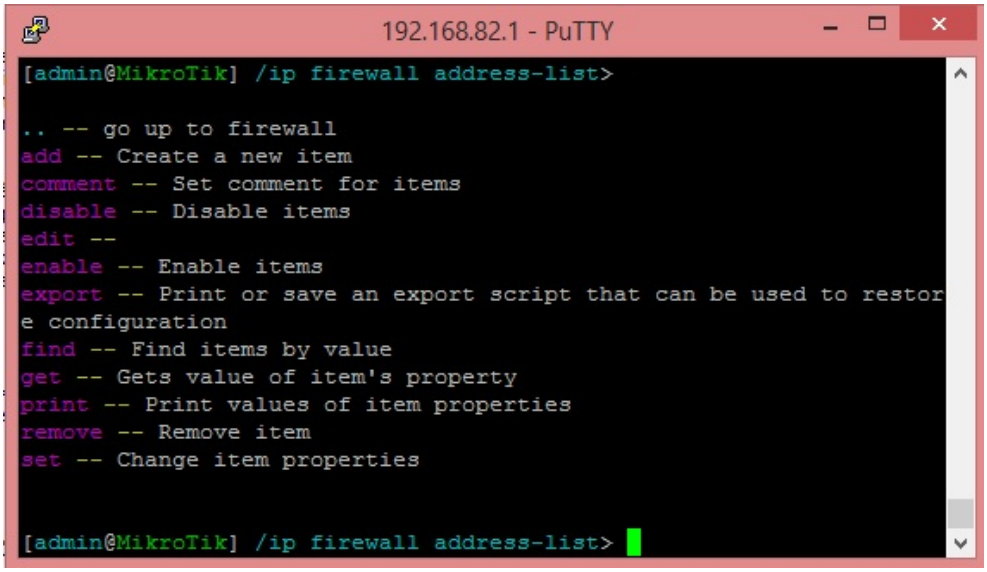
4.2.1 Inicializace RouterOS

RouterOS se vždy před prvním použitím nachází v defaultním nastavení. Při každém spuštění systému dochází k inicializaci a veškerý podporovaný hardware je po úspěšném naběhnutí systému připraven k použití. Při prvotním startu jsou všechna zařízení zakázána s výjimkou sériového portu a Ethernetového portu číslo jedna. Přes obě dvě tato rozhraní lze provést základní konfiguraci zařízení. Do zařízení je možné se připojit příkazovou řádkou, grafickým rozhraním nebo v omezené míře přes rozhraní webové. Pro popis jednotlivých možností je potřeba nejdřív vymezit několik pojmů:

- Telnet - nešifrovaný protokol, který umožňuje uživateli připojit se ke vzdálenému PC. Posílá zadávaná hesla v nezabezpečené formě, což je v mnoha případech nežádoucí.
- SSH - zabezpečený komunikační protokol, náhrada telnetu.
- Putty - klientský program protokolů Telnet a SSH pro systémy Windows.

4.2.2 Příkazová řádka

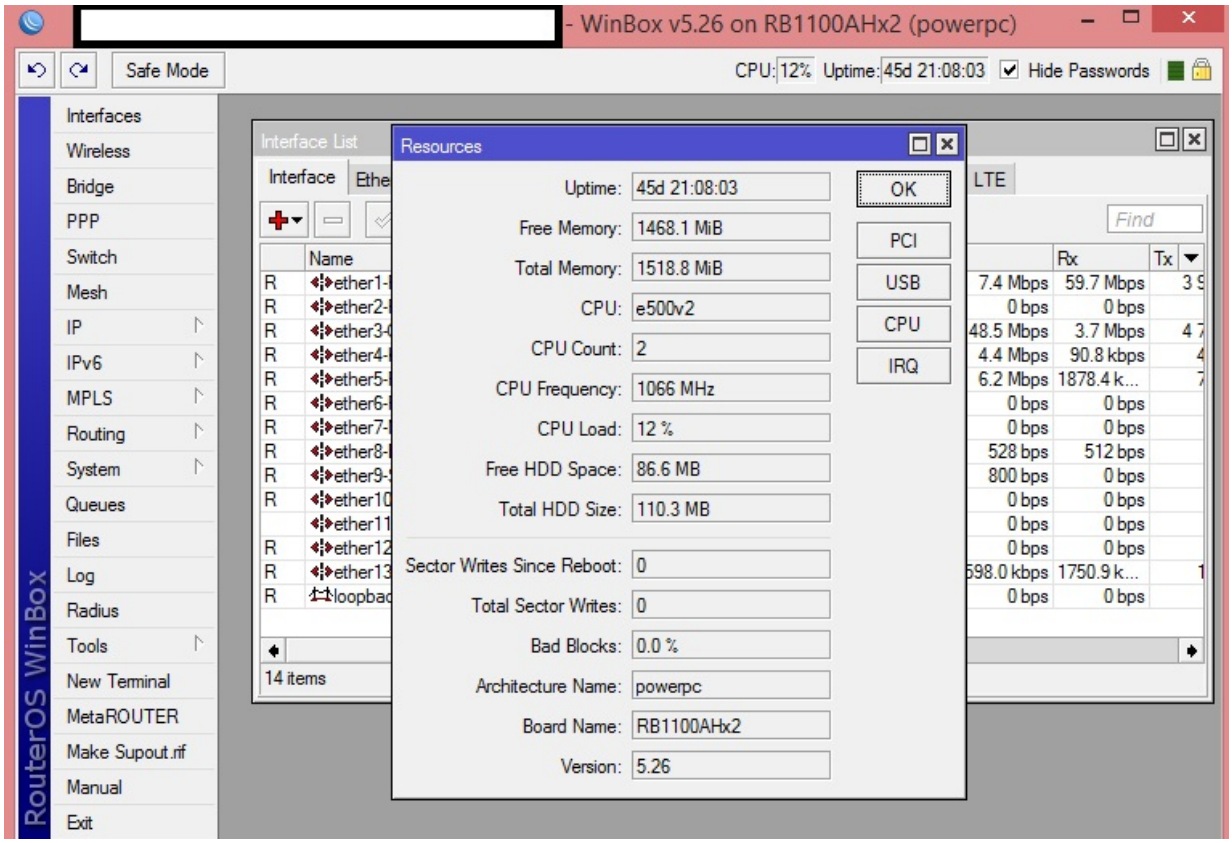
Ovládání RouterOS přes příkazovou řádku je jediné, které umožňuje kompletní administraci tohoto systému. Ovladání je velmi logické, ucelené a intuitivní. Nelze přehlédnout podobu s ovládací konzolí produktů značky CISCO. Příkazová řádka je vybavena velmi podrobnou nápovědou, která se dá kdykoliv vyvolat napsáním otazníku „?“. Příklad nápovědy a toho, jak terminál ve skutečnosti vypadá, lze nalézt na Obrázku číslo 11. Pro ilustraci je zde použit výstup programu Putty, který s RouterOS komunikuje přes protokol SSH.



Obrázek 11: Příkazový řádek - program Putty

4.2.3 Winbox

V některých případech může nastat, že administrátor nepotřebuje přístup ke všem funkcionalitám systému RouterOS a upřednostní uživatelsky příjemnější grafické rozhraní. Pro tuto situaci vyvinul Mikrotik klientský program Winbox. Nastavení systému přes utilitu Winbox je velmi rychlé a pohodlné.



Obrázek 12: Winbox - ukázka grafického rozhraní

4.2.4 Webové rozhraní

Poslední možností, jak systém nastavit, je použití webového rozhraní, které umožňuje přístup k omezeným funkcionalitám systému a je tak vhodné pouze pro koncové uživatele a jednoduché nastavení routerů pro použití v domácí síti. V tomto případě je možné použít tzv. „Quick setup“, který v několika málo krocích provede uživatele konfigurací a připraví RouterBoard spolu se systémem k základnímu použití.

4.3 Síťová funkcionalita RouterOS

4.3.1 Základní nastavení pro komunikaci

Aby bylo možné routery s operačním systémem RouterOS provozovat v síti, je zcela nezbytné provést prvotní konfiguraci základních parametrů. V zařízení se po zapojení napájení inicializuje veškerý hardware a start operačního systému je následně signalizován hlasitým dvojím pípnutím. V této chvíli se RouterBoard nachází ve výchozím stavu. Na portu ether1 má nastavenou IP adresu 192.168.88.1/24 a tento port je aktivní. Pro ověření přístupu slouží v této chvíli uživatelské jméno admin a výchozí heslo je prázdný řetězec. Do zařízení je možné se připojit programem Putty a protokolem SSH zmíněném v kapitole 4.2.2.

Výchozí stav RouterBoardu není žádným způsobem použitelný v již fungující a nakonfigurované síti. Pro uvedení do stavu, kdy router bude moci komunikovat s okolím, bude zabezpečen a bude podporovat základní síťové služby, je potřeba nastavit následující parametry:

- Heslo a identita

  Prvním krokem při nastavení, který je nutný pro zabezpečení, je změna (nastavení) administrátorského hesla. Po přihlášení do zařízení výchozími údaji toto provedeme jednoduchým napsáním *password*. Po vyplnění starého, nového a potvrzením nového hesla, je heslo úspěšně změněno, jak je vidět na Obrázku číslo 13.

```
[admin@MikroTik] > password
old-password: ******
new-password: ******
confirm-new-password: ******
```

Obrázek 13: Změna administrátorského hesla

  Aby bylo možné jednotlivé routery od sebe v síti rozeznat, je nutné každému přiřadit jiné jméno (identitu). Výchozí nastavení je jméno Mikrotik. Změnu tohoto názvu provedeme příkazem: *system identity set name=MujRouter* . Změna se projeví okamžitě a je patrná z Obrázku číslo 14.

```
[admin@Mikrotik] > system identity set name=MujRouter
[admin@MujRouter] >
```

Obrázek 14: Změna identity routeru

- Natavení IP adresy

  IP adresa 192.168.88.1/24 je určena pro prvotní konfiguraci routeru. Samozřejmostí je, že si uživatel může nastavit jakoukoliv IP adresu na libovolné komunikační rozhraní routeru. Adresa se v operačním systému RouterOS zadává vždy s maskou a to ve zkráceném tvaru (tj například 192.168.88.1/24 znamená ve zkutečnosti IP adresa 192.168.88.1 s maskou 255.255.255.0). Nastavení IP adresy na příslušné rozhraní provedeme příkazem: *ip address add address=10.0.0.10/24 interface=ether2*. Tímto příkazem je rozhraní ether2 přiřazena IP adresa 10.0.0.10 s maskou 255.255.255.0. Následně je možné přehled všech aktuálně přiřazených IP adres vypsat příkazem *ip address print*. Výstup je pak podobný tomu na Obrázku číslo 15.

```
[admin@MujRouter] > ip address add address=10.0.0.10/24 interface=ether2
[admin@MujRouter] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   10.0.0.2/24        10.0.0.0        bridge-local
 1   192.168.88.1/24    192.168.88.0    ether1
 2   10.0.0.10/24       10.0.0.0        ether2-master-local
[admin@MujRouter] >
```

Obrázek 15: Přiřazení IP adresy danému rozhraní

  Pokud chceme IP adresu smazat, je potřeba použít příkaz *ip address remove X*, kde za X dosadíme číslo interface uvedeném ve výpisu příkazem print. Pro smazání IP adresy 192.168.88.1/24 je nutné uvést *ip address remove 1*. Tímto dojde k přerušení komunikace a znovupřipojení do routeru bude nutné navázat na IP adrese 10.0.0.2 a na rozhraní ether2.

- Bridge

  Velmi často je potřeba jednu IP adresu přiřadit na více komunikačních rozhraní. Příkladem může být použití routeru pro domácí účely, kde rozhraní ether1 chceme použít pro připojení do internetu, ale ostatní rozhraní chceme používat v rámci lokální sítě a chceme, aby byla dostupná na všech portech pod stejnou adresou. Za tímto účelem Mikrotik vyvinul funkci Bridge. Bridge je virtuální rozhraní, se kterým se dá ve výsledku pracovat jako s rozhraním fyzickým. Pod jeden virtuální Bridge lze přiřadit několik fyzických rozhraní a vytvořit tak skupinu rozhraní, kterým lze následně přiřadit společnou IP adresu. Konfigurace je opět velmi jednoduchá. V prvním kroku je potřeba virtuální rozhraní vytvořit. To lze provést příkazem: *interface bridge add name=bridge-local*. Následuje už pouze zařazení fyzických rozhraní pod vytvořený bridge. Toto lze provést příkazem *interface bridge port add interface=ether1 bridge=bridge-local*. Kontrolu správného zařazení zajišťuje opět příkaz print v dané kategorii: *interface bridge port print*. Výstup takovéto konfigurace je zobrazen na Obrázku číslo 16.

```
[admin@MujRouter] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #     INTERFACE                 BRIDGE                 PRIORITY  PATH-COST
 0     wlan1                     bridge-local               0x80         10
 1     ether2                    bridge-local               0x80         10
 2 I   ether1                    bridge-local               0x80         10
```

Obrázek 16: Bridge - virtuální rozhraní

Bridge můžeme využít také ve speciálním případě pokud RouterBoard chceme nastavit do módu, kdy zařízení nebude sloužit jako router, ale pouze jako switch. V tomto případě všechny fyzické rozhraní přiřadíme pod jedno virtuální, kterému přiřadíme IP adresu pro přístup do managementu.

- NTP (Network Time Protocol)

  Protokol přesného síťového času byl vyvinut za účelem synchronizace hodin PC, routerů a dalších síťových zařízení po počítačové sítí. Zajišťuje, aby všechna zařízení v síti měla stejný a přesný čas. To je zejména vhodné pro zaznamenávání logovacích údajů či pro tvorbu záložních kopií konfigurace. Současná verze je NTP verze 4, a podrobný popis je uveden v RFC 5905. V operačním systému Mikrotik RouterOS je tato funkce samozřejmě dostupná. V každém zařízení lze nastavit primární a sekundární NTP server, od kterého má zařízení přijímat synchronizační pakety. Pro konfiguraci NTP serveru slouží příkazy:

  system ntp client set primary-ntp=95.47.186.253
  system ntp client set secondary-ntp=95.47.187.253
  system ntp client set enabled=yes

  Pro správné nastavení časového pásma je nutné uvést ještě příkaz:

  system clock set time-zone-name=Europe/Prague

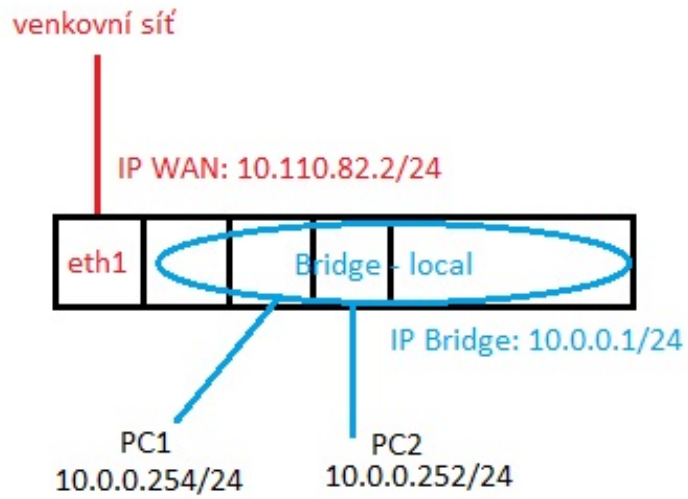
  Výpis správného času je následně volán příkazem: *system clock print* a je zobrazen na Obrázku číslo 17.

```
[admin@MujRouter] > system clock print
            time: 13:02:59
            date: jun/05/2014
  time-zone-name: Europe/Prague
      gmt-offset: +02:00
      dst-active: yes
```

Obrázek 17: Nastavení času

- NAT (Network Address Translation)

  Překlad síťových adres je proces, při kterém dochází k úpravě síťového provozu procházejícího přes router za pomoci přepisu zdrojové nebo cílové IP adresy (případně i TCP či UDP portů u průchozích paketů). Často se lze setkat i s názvy Network Masquerading či IP Masquerading. NAT nám ve výsledku umožňuje úsporu IP adres v dané síti. Příkladem opět může být malá domácí síť, ve které se vyskytují 2 počítače a cílem NATu je, aby v rámci sítě, do které jsou připojeny, vystupovaly pod jednou IP adresou. Zapojení je znázorněno na Obrázku číslo 18.



Obrázek 18: Příklad zapojení domácí sítě s NATem

Mikrotik pro NAT používá tři základní pravidla:

- dst-nat - překlad na základě cílové IP adresy
- src-nat - překlad na základě zdrojové IP adresy
- masquarede - speciální příklad src-nat, který je velmi jednoduchý na konfiguraci

Omezení NATu je na první pohled velmi zřetelné. NAT sice umožní dvěma počítačům přístup do sítě, ale znemožní přímý přístup k nim z venkovní sítě. Řešením je poté přesměrování daných služeb (portů) pomocí dst-nat. Na obrázku číslo 19 jsou uvedeny příkazy, které by umožnily dvěma počítačům PC1 a PC2 vystupovat do venkovní sítě pod adresou 10.110.82.2/24 zadané na rozhraní ether1, ale zároveň umožnily se z venkovní sítě na PC1 připojit pomocí Windows vzdálené plochy (port 3389) a na PC2 pomocí programu LM FREE (port 5650). Komunikace na tyto stroje by pak probíhala na adresách 10.110.82.2:3389 a 10.110.82.2:5650.

```
/ip firewall nat
add action=dst-nat chain=dstnat comment=RDP-WINDOWS dst-address=10.110.82.2 \
    dst-port=3389 protocol=tcp to-addresses=10.0.0.254 to-ports=3389
add action=dst-nat chain=dstnat comment="RDP-LM FREE" dst-address=10.110.82.2 \
    dst-port=5650 protocol=tcp to-addresses=10.0.0.252 to-ports=5650
add action=masquerade chain=srcnat comment=MASKARADA out-interface=\
    ether1-internet
```

Obrázek 19: Příkazy pro nastavení NAT

- DHCP (Dynamic Host Configuration Protocol)

  Protokol, který se používá pro dynamickou konfiguraci klientských zařízení připojených do počítačové sítě. DHCP přiděluje jednotlivým strojům zejména IP adresu, masku sítě, implicitní bránu a adresy primárního a sekundárního DNS serveru. RouterOS umožňuje jak dynamické tak statické přidělení těchto údajů. Nejprve je zapotřebí uvést, v jakém rozsahu chceme IP adresy přidělovat. To je možné zadat příkazem: *ip pool add name=dhcppool ranges=10.0.0.100-10.0.0.254*, z něhož je jasně patrný zadaný rozsah IP adres. Následně je potřeba nastavit síť a gateway, která se bude koncovým stanicím propagovat. To zařídí příkaz: *ip dhcp-server network add address=10.0.0.0/24 gateway=10.0.0.1*. Jako poslední je potřeba spustit DHCP server *add name=dhcpserver address-pool=dhcppool interface=bridge1 disabled=no*.

  Pokud je potřeba přiřadit stanicím staticky vždy stejnou IP adresu, je potřeba do skupiny leases uvést MAC adresu stroje a údaje, které mu mají být přiřazeny. To lze udělat příkazem:
  ip dhcp-server lease add address=10.0.0.252 client-id=1:70:71:bc:6c:7b:69 comment=Server mac-address=70:71:BC:6C:7B:69 server=dhcpserver

  Výpis všech zařízení s přiřazenou IP lze vypsat pomocí *ip dhcp-server lease print*

```
#    ADDRESS                                MAC-ADDRESS       HOST-NAME          SERVER
0    ;;; DCP-7065DN-tiskarna
     10.0.0.253                             30:05:5C:24:74:91 BRN30055C247491    dhcp1
1    ;;; Server-Linux
     10.0.0.252                             70:71:BC:6C:7B:69 Brody-PC           dhcp1
2    ;;; Alena-HP
     10.0.0.250                             00:21:00:3D:68:22 Alena-ntb          dhcp1
3    ;;; SamsungTV
     10.0.0.249                             0C:89:10:B8:8C:07                    dhcp1
4    ;;; Brody-Lenovo
     10.0.0.247                             0C:8B:FD:C9:0C:E8 Brody-Lenovo       dhcp1
5    ;;; Brody-phone
     10.0.0.248                             A0:E4:53:B7:87:4B android-51807...    dhcp1
6    ;;; Brody-Ubuntu-fujitsu
     10.0.0.254                             00:1E:33:E0:06:1F brody-ubuntu       dhcp1
7 D  10.0.0.244                             00:21:6A:70:81:CA Brody-ntb          dhcp1
8 D  10.0.0.246                             1C:7B:21:BD:E0:BA android-e34b0...    dhcp1
```

Obrázek 20: Výpis tabulky DHCP leases - zařízení s přidělenou IP

4.3.2 Směrování mezi routery

Směrování datových paketů v síti je často označováno pojmem routování. Při tomto procesu dochází k určování cest datagramů jednotlivými směry na základě směrovací tabulky. Směrovací tabulka je vyplněna administrátorem staticky a nebo je dynamicky naplněna pomocí směrovacího protokolu a algoritmu, který daný protokol používá. Obsahem této tabulky je cílová síť společně s maskou, brána, na kterou se mají dané pakety pro tuto síť směrovat, a název odchozího rozhraní. Velmi často je také uvedena defaultní routa, která odkazuje na implicitní gateway. Veškeré pakety, které nesplňují žádné z routovacích pravidel, jsou poslány na implicitní bránu.

- Statické směrování

  Při použití statického routování je třeba, aby administrátor zadal do routeru pro každou routovanou síť jeden záznam. To je sice vhodné například pro koncové stanice či routery, kde je provoz směrován pouze jedním směrem a lze použít defaultní routu, ale už to není vhodné pro větší sítě, kde sebemenší změna v návrhu topologie sítě by pro administrátora znamenala zásah do konfigurace několika síťových prvků.

  Přidání defaultní routy do prvků Mikrotik RouterBoard lze provést příkazem: *ip route add dst-address=0.0.0.0/0 gateway=10.110.82.1*. Směrovací tabulku lze vypsat pomocí příkazu *ip route print* a příklad takové tabulky je uveden na Obrázku číslo 21. Z výpisu je patrné, že defaultní routa byla zadána staticky (je označená písmenem S - static).

```
[admin@MujRouter] > ip route add dst-address=0.0.0.0/0 gateway=10.110.82.1
[admin@MujRouter] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          10.110.82.1               1
 1 ADC  10.0.0.0/24        10.0.0.1        bridge1                   0
 2 ADC  10.110.82.0/24     10.110.82.2     ether1-internet           0
 3 ADC  192.168.10.0/24    192.168.10.20   bridge1                   0
[admin@MujRouter] >
```

Obrázek 21: Výpis směrovací tabulky se staticky zadanou defaultní bránou

- Dynamické směrování

  Při použití dynamického směrování jsou tabulky plněny automaticky a v pravidelných intervalech dynamicky reagují na změny topologie sítě. Pro naplnění tabulek je možno použít několik dynamických protokolů, které se dělí do dvou tříd:

  – interior - RIP v1 a v2, OSPF
  – exterior - BGP

Rozdíl mezi statickým a dynamickým směrováním je zřejmý. Na zařízeních, kde se konfigurace mění jen zřídka, je vhodné použít statické směrování. Pravým opakem jsou pak páteřní prvky sítě, kde se konfigurace může dynamicky měnit dle funkčnosti a nefunkčnosti linek. Rozdíly mezi jednotlivými dynamickými protokoly už na první pohled patrné nejsou, proto se následující text bude věnovat stručnému popisu a základnímu nastavení tří nejpoužívanějších protokolů, které systém RouterOS podporuje.

- RIP (Routing Information Protocol)
  RIP je vhodný pouze do menších a středně velkých sítí. Používá k určení cesty Distance Vector Algoritmus, u kterého není možné ohodnotit linky například dle jejich kapacity. Základním parametrem DVA algoritmu je počet skoků mezi jednotlivými routery. Maximální počet skoků je 15, což je jedna z nevýhod a omezuje tak použití RIPu ve větších sítích. Druhou velkou nevýhodou je pomalá konvergence tohoto algoritmu. Problémy s pomalou konvergencí a zacyklením řeší RIP ve verzi 2 pomocí „split horizon with poisoned reverse“. Veškeré další informace a podrobnosti je možné dohledat v RFC 2453. Nastavení RIP na prvích Mikrotik RouterBoard je velmi dobře popsáno na *http://www.mikrotik.com/testdocs/ros/2.9/routing/rip.php*.

- OSPF (Open Shortest Path First)
  Na rozdíl od RIP je OSPF směrovací protokol, který je určen pro středně velké a velké počítačové sítě. Routery, používající tento protokol, si v daných intervalech mezi sebou posílají „Hello“ pakety a kontrolují tak stav sousedních routerů. Při zjištění jakékoliv změny, router posílá informaci všem routerům v síti a ty si na základě toho přepočítají svojí směrovací tabulku. Linky lze ohodnotit různou hodnotou „Cost“, která je brána v úvahu při výpočtu nejlepší trasy. Výměna těchto informací probíhá pomocí LSA (Link State Advertisement) paketů, které si router ukládá do své topologické databáze. Výsledkem je vždy shodná topologická databáze na všech směrovačích. Z této databáze následně každý router pomocí Dijsktrova algoritmu vypočte optimální trasy pro směrování.

  OSPF je nejpoužívanější protokol používaný uvnitř autonomních systémů (autonomní systém je skupina směrovačů a IP prefixů se společnou směrovací politikou a jednotnou správou). OSPF dělí autonomní systém na několik oblastí, které se nazývají *area* a jsou obvykle značené 32 bitovým číslem (vypadají stejně jako IP adresa). Výhodou těchto oblastí je, že výše zmíněné LSA pakety jsou šířeny pouze v rámci jedné oblasti a nedochází tak ke zbytečnému zahlcení sítě. OSPF rozlišuje tři druhy oblastí:

  – páteřní (backbone) - oblast označovaná 0.0.0.0. Do této oblasti jsou připojeny všechny ostatní a tato oblast je připojena do internetu
  – tranzitní (tranzit) - oblast, která je připojena do páteřní oblasti více cestami
  – stub - oblast, která je připojena do páteřní pouze jednou cestou

  Routery, které jednotlivé oblasti spojují, mají speciální označení ABR (Area Border Router). Speciálním případem je router, který zastává hraniční funkci celého au-

tonomního systému a označuje se ASBR (Autonomous System Boundary Router). Více o protokolu OSPF je možné nalézt v RFC 2328. Základní nastavení OSPF v oblasti backbone pro systém Mikrotik RouterOS je podrobně uvedeno na adrese: *http://wiki.mikrotik.com/wiki/Manual:OSPF-examples*.

Výstup z dynamicky naplněné routovací tabulky je uveden na Obrázku číslo 22. Písmeno „o“ zde značí routy, které byly do tabulky přidány dynamicky pomocí protokolu OSPF.

```
[admin@Letkov_Brody] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADo  0.0.0.0/0                          10.110.252.174          110
 1 ADo  10.109.88.232/29                   10.110.252.174          110
 2 ADo  10.109.88.240/29                   10.110.252.174          110
 3 ADo  10.109.103.248/29                  10.110.252.174          110
 4 ADo  10.109.165.248/29                  10.110.252.174          110
```

Obrázek 22: Výpis části dynamicky naplněné směrovací tabulky za pomoci OSPF

- BGP(Border Getaway Protocol)
  BGP je zástupcem „exterior“ routovacího protokolu a je určen pro směrování mezi autonomními systémy jednotlivých poskytovatelů. Směrování mezi autonomními systémy má svoje charakteristické požadavky. Směrovací tabulky obsahují v případě tzv. „Full BGP“ tabulky stovky tisíc záznamů. Nejdůležitějším kritériem často nebývá vzdálenost zdroje od cíle, ale cena linky, případně další uživatelsky nastavované atributy (například seznam tranzitních autonomních systémů). Podrobný popis protokolu je možné nalézt v RFC 4271. Velmi pěkný příklad jednoduchého nastavení BGP pod operačním systémem RouterOS je dostupný na adrese:
  http://isp-servis.cz/config_mikrotik.html. V tomto případě se přes BGP šíří pouze defaultní routa, což je pro provoz internetu dostatečné. Reálný výpis defaultní routy naučené přes BGP je ukázán na Obrázku číslo 23.

```
[brody@gw.plzenec.net] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADb  0.0.0.0/0                          89.203.220.193           20
```

Obrázek 23: Výpis části dynamicky naplněné směrovací tabulky za pomoci BGP

4.4 Monitorování zařízení

Informace, zda monitorované zařízení v dané době funguje, jakým způsobem je zatíženo, jaká je aktuální verze operačního systému či jak tyto informace vypadaly v historii, jsou informace, které by měly být součástí každého monitorovacího systému. Dohled (monitoring) je jedna z nejdůležitějších součástí řádně fungující sítě. Administrátor sítě, která funguje na prvcích RouterBoard s operačním systémem RouterOS, může volit z několika technologií a protokolů, aby dosáhl stavu, kdy bude znát požadované informace.

Celý monitorovací systém je možné postavit na vlastních scriptech či na bezplatných dohledovacích systémech, kdy administrátor věnuje dohledu pouze čas a svoje znalosti. Protipólem je nasazení rozsáhlých systémů z komerční nabídky, které nabízí nepřeberné množství funkcionalit. Tyto systémy jsou ovšem zpoplatněny.

- placené : ISPadmin, Zennos, MikroBill
- volně dostupné: Cacti, Nagios, Zabbix

Vzhledem k praktické části této diplomové práce se následující text nebude zabývat popisem hotových dohledovacích systémů, ale naopak se bude snažit přiblížit základní prostředky (technologie a protokoly), pomocí kterých je možné naprogramovat a sestavit vlastní základní dohledovací systém pro prvky s operačním systémem RouterOS.

Před výběrem těchto technologií je nutné si nejdříve ujasnit, co přesně je zapotřebí sledovat a jaký výstup je prioritní. Na monitoring je možné se dívat ze dvou pohledů. Prvním z nich je, že na nějakém zařízení v síti došlo k problému a je potřebné ho zkontrolovat. Druhým pohledem pak pak může být periodické získávání informací o systému na daném prvku (například využití CPU, odezva zařízení v síti). Tyto informace je pak administrátor schopný využít k dalšímu plánování sítě (upgradu prvků, či přenosových technologií). Ideální verzí dohledovacího systému by měla být kombinace obou těchto pohledů.

Mezi položky, které je možné dohledovat na systému RouterOS patří například:

- dostupnost daného RouterBoardu (latence)
- vytížení zdrojů (CPU, disk, paměť)
- informace o typu desky a verzi operačního systému
- vytížení přenosových linek
- bezpečnostní incidenty
- změny v konfiguraci (směrovací tabulky atd.)

Základní monitorovací prostředky operačního systému RouterOS jsou ve většině případů shodné z monitorováním jakýchkoliv jiných zařízení. Na následujících řádkách budou popsány ty nejpoužívanější z nich a bude zde uvedena základní konfigurace systému RouterOS, která je potřebná pro jejich bezchybnou funkčnost.

4.4.1 ICMP a PING

ICMP (Internet Control Message Protocol) je jeden z nejdůležitějších protokolů ze sady protokolů internetu. Operační systémy je používají pro posílání chybových zpráv, například pro oznámení, že požadovaná služba není dostupná. Podrobná dokumentace tohoto protokolu je dostupná v RFC 792.

V souvislosti s dohledem síťových prvků jsou ICMP pakety využívány především nástrojem PING, který posílá pakety „Echo Request“ a očekává příjem zprávy „Echo Reply“, aby určil, zda je cílový síťový prvek dosažitelný a jak dlouho paketům trvá, než se dostanou ze zdroje k cíli a zpět. PING je dostupný pod systémem RouterOS, Unix i Windows a je považován za jeden z univerzálních nástrojů pro ověřování dostupnosti prvků v síti.

Spuštění na všech systémech je prováděno příkazem *ping A.B.C.D*, kde A.B.C.D je IP adresa zařízení na které chceme zaslat dotazovací ICMP paket. Ping má i několik dalších parametrů. Mezi hlavní patří parametr count (pro systém RouterOS), který udává počet odeslaných ICMP paketů a parametr size, který udává jejich velikost. Příklad ping na zařízení s IP adresou 10.110.254.254 o počtu 5 ICMP paketů o velikosti 10000 Bytů je zobrazen na Obrázku číslo 24.

```
[admin@MujRouter] > ping 10.110.254.254 count=5 size=10000
HOST                                     SIZE TTL TIME  STATUS
10.110.254.254                          10000  61 14ms
10.110.254.254                          10000  61 23ms
10.110.254.254                          10000  61 23ms
10.110.254.254                          10000  61 16ms
10.110.254.254                          10000  61 25ms
    sent=5 received=5 packet-loss=0% min-rtt=14ms avg-rtt=20ms max-rtt=25ms
HOST                                     SIZE TTL TIME  STATUS
```

Obrázek 24: Ping na zařízení 10.110.254.254

Výstupem nástroje PING je v každém řádku aktuální odezva prvku s dotazovanou IP adresou. Je uvedena v milisekundách. Dále je v každém řádku vypsán parametr TTL (Time To Live), což je hodnota „životnosti“ paketů a značí, přes kolik routerů paket ještě může projít než bude routerem zahozen (to nastane při hodnotě 0). Po odeslání zadaného počtu ICMP paketů jsou vypsány statistiky, které udávají:

- sent/received : počet odeslaných/přijatých paketů
- packetloss : procentuálně vyjádřena ztráta paketů
- min-rtt/avg-rtt/max/rtt : minimální/průměrná/maximální doba odezvy

4.4.2 SNMP

Simple Network Management Protocol slouží k potřebám správy sítě. Protokol umožňuje sběr nejrůznějších dat z datové sítě a jejich následné vyhodnocování. Na tomto protokolu je díky své univerzálnosti v dnešní době postavena většina prostředků a nástrojů pro dohled a správu sítě.

Je potřeba rozlišovat mezi stranou monitorovanou (hlídaný systém) a monitorovací (sběrna dat). Na monitorované straně obvykle běží Agent, který shromažďuje data o daném systému. Na straně monitorovací běží manager, který se v intervalech dotazuje na požadovaná data Agenta dohledovaného systému. Komunikace mezi agentem a managerem se označuje jako SNMP operace. Může existovat i taková konfigurace agenta, která je schopna reagovat na vniklou situaci tak, že sám agent odešle zprávu managerovi automaticky bez jeho požadavku. Taková konfigurace je označována jako SNMP TRAP.

Jednoznačná identifikace informací využívaná systémem správy je uvedena v databázi MIB (Management Information Base) pomocí tzv identifikátoru objektu OID (object identifier). Aby si SNMP agent a manager mohli tyto informace předávat, je nutná znalost této databáze, která je veřejně přístupná na: *http://www.alvestrand.no/objectid/1.3.6.1.html*. OID v systému RouterOS lze u všech položek vypsat pomocí příkazu *print oid* v dané kategorii. Pokud například chceme vypsat hodnotu uptime (době běhu systému), který je dostupný v kategroii system resource, použijeme příkaz *system resource print oid*. Výstup je znázorněn na Obrázku číslo 25.

```
[admin@MujRouter] /system resource> print oid
       uptime: .1.3.6.1.2.1.1.3.0
 total-memory: .1.3.6.1.2.1.25.2.3.1.5.65536
  used-memory: .1.3.6.1.2.1.25.2.3.1.6.65536
```

Obrázek 25: Vypsání OID hodnoty uptime na systému RouterOS

Podrobný popis protokolu SNMP je uveden v RFC 1157, kde lze nalézt přesnou definici zpráv, pomocí kterých dochází k výměně informací. Patří mezi ně například get-request, get-next-request, get-response, get-bulk,trap, inform.

Protokol SNMP má aktuálně 3 verze:

- v1 - nezabezpečený přenos dat
- v2 - umožňuje autentizaci
- v3 - umožňuje autentizaci a šifrování

Operační systém RouterOS podporuje všechny tři verze. Pokud chceme docílit spolehlivého a bezpečného přenosu dat, je vhodné využít verzi 3 protokolu SNMP. V následujícím textu budou popsány konfigurační příkazy, které umožní nakonfigurovat agenta systému RouterOS tak, aby z něj bylo možné vyčítat monitorovací data pomocí SNMP ve verzi 3.

V systému router OS je při spuštění předkonfigurováno SNMP. Je zde nastaveno „community name“ na hodnotu public (přihlašovací jméno v protokolu SNMP). Není požadováno žádné heslo ani šifrování (SNMP ve verzi 1) a je povoleno pouze čtení dat. Zprovoznění takového přístupu je možné provést příkazem: *snmp set enabled=yes*.

Jak již bylo řečeno, není tento způsob zabezpečení vhodný. Tímto způsobem si jakýkoliv uživatel sítě může bez problému zjistit veškeré informace o zařízení (dostupné přes SNMP) a to není v žádném případě vyhovující. Pro plně zabezpečený přístup je nutné použít SNMP ve verzi 3, které podporuje autentizaci a šifrování. V systému RouterOS je možné volit mezi autentizačním protokolem MD5 (RFC 1321) a SHA1 (RFC3174). Šifrovací protokol je pak nastaven na DES (RFC 4772). Nastavení je možné provést příkazem: *snmp community add addresses=0.0.0.0/0 authentication-password=D1pl0mkA encryption-password=D1pl0mkA name=secure security=private*. Úspěšné založení nové zabezpečené community s autentizačními a šifrovacími údaji je viditelné na Obrázku číslo 26.

```
[admin@MujRouter] /snmp community> print
Flags: * - default
 #   NAME      ADDRESSES                                          SECURITY   REA
 0 * public    0.0.0.0/0                                          none       yes
 1   secure    0.0.0.0/0                                          private    yes
[admin@MujRouter] /snmp community> export
# jun/11/2014 11:37:29 by RouterOS 6.2
# software id = RN0W-AM9J
#
/snmp community
add addresses=0.0.0.0/0 authentication-password=D1pl0mkA encryption-password=\
    D1pl0mkA name=secure security=private
[admin@MujRouter] /snmp community>
```

Obrázek 26: Community secure pro SNMP ve verzi 3

Otestování, zda je SNMP v3 na systému RouterOS funkční, je možné provést pomocí nástroje snmpwalk nainstalovaném pod unixovým systémem. Pro zkoušku spojení je nyní možné použít nastavené údaje (jméno: secure, heslo: D1pl0mkA, šifromávání DES s heslem: D1pl0mKA a dobře známé OID uptime .1.3.6.1.2.1.1.3.0). Výstup snmpwalku je vidět na Obrázku číslo 27 a je patrné, že SNMP v3 funguje na systému RouterOS korektně.

```
plzenecnet@PlzenecNET-Kikimara:~$ snmpwalk -u secure -v 3 -a MD5 -A D1pl0mkA -l
authPriv -x DES -X D1pl0mkA 10.110.82.1 .1.3.6.1.2.1.1.3.0
iso.3.6.1.2.1.1.3.0 = Timeticks: (128463600) 14 days, 20:50:36.00
```

Obrázek 27: snmpwalk, SNMP v3, OID: uptime

4.4.3 Mikrotik API

Protože protokol SNMP je určen hlavně pro vyčítání dat, která jsou dostupná u téměř všech síťových prvků, vyvinula firma Mikrotik svoje API, přes které je možné ze systému RouterOS vyčítat o mnoho víc informací (například SSID bezdrátové karty, připojené bezdrátové klienty atd.). Pomocí API lze také do systému RouterOS hodnoty zapisovat a celou konfiguraci měnit.

API umožňuje uživatelům vytvořit vlastní software, který bude komunikovat s prvky RouterBoard. Syntaxe příkazů se velmi podobá příkazům CLI (příkazové řádky). API je podporováno systémem RouterOS od verze 3.x výše a v současnosti je vyvinuto pro mnoho programovacích jazyků (C, C++, Java, Perl, PHP, Delphi). Nevýhodou API je, že při zápisu většího množství pravidel, vyžaduje poměrně hodně času a to z toho důvodu, že jsou příkazy na router zasílány pomocí vět, které většinou obsahují jeden řádkový příkaz. Odpověď je tvořena opět API větou (nebo více větami). Toto tvoří obrovské množství komunikační režie, proto nemusí být API v některých systémech příliš vhodné.

Pokud chceme komunikovat s routerem pomocí API, je nutné API v systému RouterOS nejdříve povolit. API komunikuje na portu TCP 8728, případně na portu 8729 pokud je potřeba použít zabezpečení API-ssl. Povolení probíhá příkazem: *ip service enable 5* a *ip service enable 7*.

Syntaxe API příkazů se liší od příkazu příkazové řádky tak, že mezery mezi příkazy jsou vyplněny zpětným lomítkem a mezery v atributech jsou nahrazeny rovnítkem:

- CLI příkaz:
  ip address add address=192.168.88.1/24 interface=ether1

- API příkaz:
  /ip/address/add
  =address=192.168.88.1/24
  =interface=ether1

Podrobný popis Mikrotik API lze nalézt na: *http://wiki.mikrotik.com/wiki/Manual:API*. Jsou zde uvedeny i ukázky příkazů a zdrojové kódy API klienta pro několik programovacích jazyků. Na Obrázku číslo 28 je uveden příklad použití Mikrotik API k dohledování položek, které by jinak nešly vyčíst přes SNMP. Zde konkrétně se jedná o vypsání všech rout ze směrovací tabulky, které mají nějaký komentář.

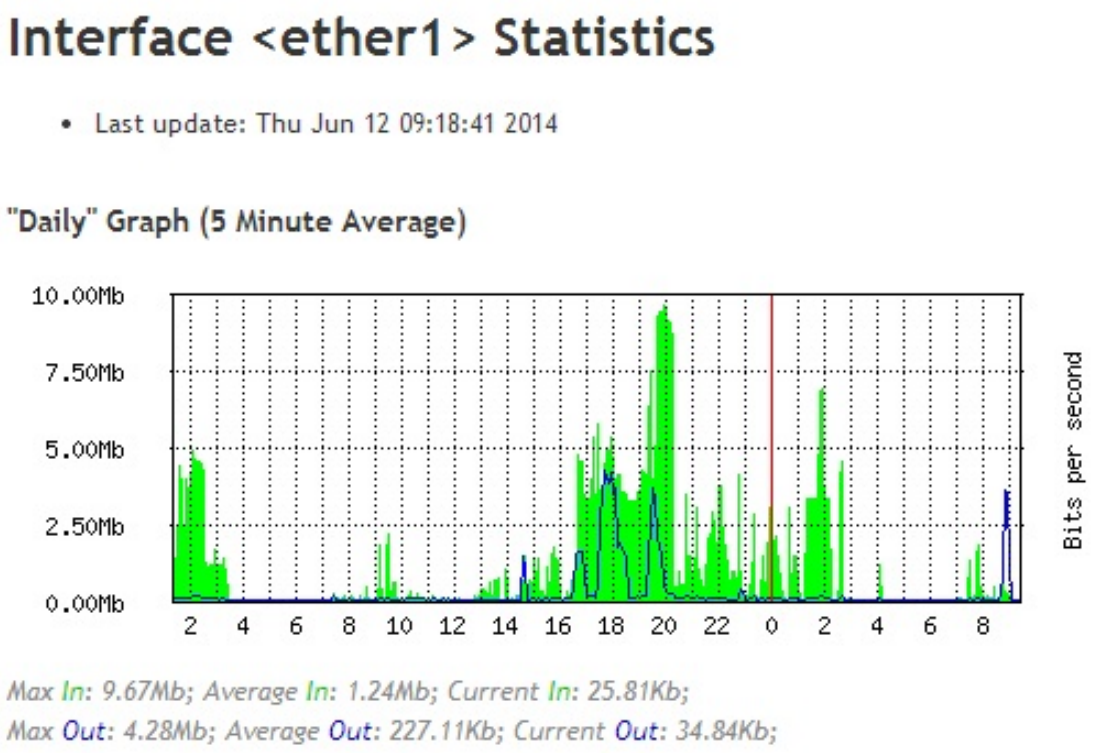
```
/ip/route/print
?>comment=
```

Obrázek 28: Použití API

4.4.4 Grafování dat

Pro získání monitorovacích dat ze zařízení byly uvedeny základní způsoby. Takto získané hodnoty je ale vhodné archivovat po nějakou dobu a ideálně hodnoty zanést do grafů. Za tímto účelem lze použít vestavěný grafovací nástroj přímo v systému RouterOS nazvaný „Graphing“. I když je jeho funkčnost značně omezená, pro základní historii přenosů na rozhraních a využití prostředků (CPU, paměť, disk) může některým administrátorům vyhovovat. Jako ideálním řešením se jeví pro zaznamenávání dat do grafu v zařízení koncových klientů, kterých v síti bývá velký počet a grafy jejich zařízení by na serverech zabíraly velmi mnoho prostoru.

Zapnutí grafů na RouterOS lze provést příkazem: *tool graphing interface add allow-address=0.0.0.0/0 interface=all store-on-disk=yes* , kde první parametr definuje IP adresy, pro které bude dohled dostupný (v tomto případě všechny), druhý, jaká rozhraní se mají dohledovat a třetí parametr udává, že se data mají ukládat na lokální disk. Podobným příkazem lze zapnout i grafy zdrojů: *tool graphing resource add allow-address=0.0.0.0/0 store-on-disk=yes*. Grafy jsou od každé položky tvořeny čtyři (denní, týdenní, měsíční, roční) a zobrazit je, je možné pomocí vestavěného webového serveru na adrese: http://IP-ADRESA/graphs/iface/ether1/ (pro rozhraní ether1). Jak vypadá jeden z grafů, je patrné z Obrázku číslo 29.



Obrázek 29: Graf za použití nástroje Graphing z RouterOS

Použití lokální tvorby grafů však nemusí být vždy vhodné. Příkladem může být případ, kdy je router centrálním prvkem sítě. Zařízení tvoří grafy a z nějakého důvodu se porouchá. Administrátor sítě jej vymění za zařízení jiné, ovšem o veškeré grafy by tímto způsobem přišel. Řešením této situace je použití externího grafovacího nástroje, který poběží na serveru a bude z dohledovaných zařízení periodicky vyčítat data (například pomocí SNMP) a bude je ukládat do svých lokálních grafů. I po výměně dohledovaného prvku sítě, je možné pokračovat ve vykreslování grafu a zachovat původní hodnoty. Příkladem nástroje, který je určen pro tyto účely, je RRDTool.

Vytvoření grafů pomocí nástroje RRDTool se skládá ze tří základních částí:

- Inicializace databáze
  rrdtool create CPUusage.rrd –step 60 DS:cpu:GAUGE:300:0:100 RRA:MAX:0.5:1:1500

  Význam prametrů:

  - *CPUusage.rrd* : název datového souboru
  - *–step 60* : data jsou očekávána po 60 vteřinách
  - *DS:cpu:GAUGE:300:0:100* : do proměnné cpu se budou ukládat data. 300 je interval ve vteřinách, který značí čas, po kterém bude zapsána do datového souboru 0, pokud nepřijdou další data. 0 značí minimální a 100 maximální hodnotu (rozsah CPU 0-100
  - *RRA:MAX:0.5:1:1500* : Round Robin Archiv definuje, kolik hodnot je potřeba uchovávat. Důležitá je hodnota 1, která uvádí, z kolika hodnot se má udělat průměr, než se uloží do archivu. V tomto případě se ukládá každá hodnota. 1500 značí kolik hodnot se má ukládat. 1500 hodnot v intervalu 60 vteřin uloží data po dobu 25 hodin.

- Sběr a update dat
  rrdtool update CPUusage.rrd –template cpu N:cpu

  Význam parametrů:

  - *CPUusage.rrd* : název datového souboru
  - *–template cpu N:cpu* : hodnotu N:cpu ukládáme do archivu definovaného při použití rrdtool create (DS:cpu)

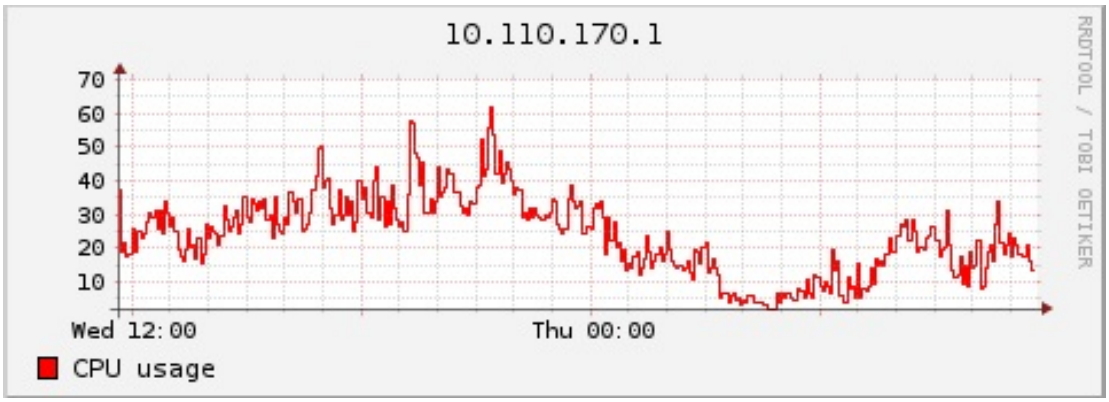
- Vytvoření grafu
  rrdtool graph CPUusage.png -a PNG –title=CPUusage
  DEF:probe1=CPUusage.rrd:cpu:MAX LINE1:probe1#ff0000:CPUusage

  Význam parametrů:

  - *CPUusage.png* - název výstupního soboru

- *CPUusage.png -a PNG –title=CPUusage* - formát souboru a nastavení popisu
- *DEF:probe1=CPUusage.rrd:cpu:MAX* : nastaví z jakého souboru a jaká proměnná se bude vykreslovat
- *LINE1:probe1#ff0000:CPUusage* : vytvoří legendu, nastaví barvu grafovací čáry a popisek legendy

Všechny uvedené příkazy jsou dostupné na Unixovém systému po řádné konfiguraci (*apt-get install mrtg rrdtool librrds-perl*). Nástroj RRDTool bude použit v praktické části této diplomové práce. Příklad vytvořeného grafu pomocí RRDTool je zobrazen na Obrázku číslo 30. Je zde vidět zatížení CPU routeru RB1200 během 25 hodin při datovém toku cca 0 - 100Mbps.



Obrázek 30: Graf za použití nástroje RRDTool

4.5 Řízení datových toků

4.5.1 QoS (Kvalita služeb)

QoS (Quality of service) je schopnost sítě, pomocí které lze některým přenosům zajišťovat lepší služby. Lze také říci, že QoS je vlastnost sítě, která umožní rozlišovat mezi různými třídami přenosů a pro každou z nich nastavit různé parametry přenosu. QoS je rozlišována dle následujících kategorií:

- Dostupnost služby - kvalita připojení do sítě
- Zpoždění služby - doba přenosu mezi zdrojem a a cílem
- Propustnost služby - maximální datový tok
- Ztrátovost paketů - množství zahozených paketů

QoS je zapotřebí, pokud administrátor potřebuje navrhnout síť, která bude škálovatelná nebo bude podporovat přenos za pomoci více tříd služeb nebo s podporou kriticky časových aplikací. K zajištění QoS v sítích jsou dnes realizovány tři základní modely:

- Služby typu Best Effort (s maximálním úsilím)
  - v modelu Best Effort posílají aplikace data dle vlastního uvážení. Žádným způsobem si nesnaží předem vyhradit cestu skrz datovou síť. Síťové komponenty se snaží data doručit co nejlépe bez ohledu na zpoždění či ztrátovost paketů. Příkladem je klasické doručování v IP sítích.
- Integrované služby (Integrated services)
  - v případě integrovaných služeb probíhá přenos dat jiným způsobem. Aplikace nejdříve oznámí požadavky na přenos formou požadovaných kvalit (QoS). Počítačová síť zjistí, zda jsou tyto prostředky k dispozici a podle toho se rozhodne, zda přenosu dat vyhoví nebo nevyhoví. V druhém případě může aplikace znovu požádat o prostředky s nižšími nároky na QOS. Jakmile je požadavek sítí přijat, dochází ze strany sítě k informování všech komponent za účelem rezervování dostatečného množství prostředků, který je potřebný pro daný přenos. K tomu slouží rezervační protokoly, jako je například RSVP (Resource reSerVation Protocol) nebo YESSIR. Více o protokolu RSVP lze dohledat v RFC 2205.
- Rozlišované služby (Differentiated Services)
  - rozdíl mezi rozlišovanými a integrovanými službami je především v tom, že diferencované služby předem neoznamují síti požadavky na přenos. Z toho důvodu nejsou potřeba ani rezervační protokoly. Implementace QoS je řešena způsobem, že každý paket vstupující do sítě, je na hraničním směrovači označen značkou, která nadále určuje jeho třídu služeb v síti. Prvky, přes které datový přenos probíhá, tuto značku pouze čtou a dle nastavených pravidel řídí způsob zpracování paketů.

Následující text bude zaměřen na diferencované služby, které budou předmětem praktické části diplomové práce.

4.5.2 Klasifikace paketů pomocí TOS a DSCP

Jak již bylo řečeno, klasifikace paketů probíhá na hraničních směrovačích a uvnitř sítě zůstává značka nezměněna. Výběr značky může být proveden například na základě zdrojové IP adresy, cílového IP adresy nebo čísla komunikačního portu protokolu TCP případně UDP. Pakety mohou být označeny již přímo od aplikace, hraniční směrovač pak tyto značky může zachovat nebo změnit na značky, které podporuje přenosová síť.

Způsob značení paketu obecně závisí na použité technologii. Značka může být obsažena uvnitř hlavičky protokolu nebo přidána vně. V případě použití diferencovaných služeb u protokolu IPv4 byla značka obsažena v poli TOS (Type of Service - RFC 791) a následně byla předefinována na DSCP (Differentiated Services Code Point - RFC 2474). Definice jednotlivých bitů pole TOS a DSCP zobrazuje Obrázek číslo 31.

Obrázek 31: pole TOS vs DSCP

Význam bitů TOS:

- 0,1,2 (precedence) - značí prioritu paketů
- bit 3 - preference nízkého zpoždění
- bit 4 - preference vysoké propustnosti
- bit 5 - preference vysoké spolehlivosti
- bity 6,7 - rezervované

Význam bitů DSCP:

- bity 0,1,2,3,4,5,6 (DSCP FIELD) - značí prioritu
- bity 6,7 - rezervované

Z obrázku i z popisu je patrné, že prvních 6 bitů vždy určuje priority přenosu a poslední 2 bity zůstávají rezervované. Toto zaručuje kompatibilitu a převodní vztah mezi značením DSCP a TOS precedencí. Tento převodní vztah je naznačen v tabulce na Obrázku číslo 32.

DSCP Name	DS Field Value (Dec)	IP Precedence (Description)
CS0	0	0 : Best Effort
CS1,AF11-13	8,10,12,14	1 :Priority
CS2,AF21-23	16,18,20,22	2 :Immediate
CS3,AF31-33	24,26,28,30	3 :Flash - mainly used for voice signaling
CS4,AF41-43	32,34,36,38	4 :Flash Override
CS5,EF	40,46	5 :Critical - mainly used for voice RTP
CS6	48	6 :Internet
CS7	56	7 :Network

Obrázek 32: Převodní vztah mezi TOS a DSCP

Praktické nastavení v systému RouterOS lze provést v podkategorii *ip firewall mangle*. Například „Manglování“ neboli značkování pravidel pro protokol SSH na základě cílové IP adresy a komunikačního portu 22 se provádí na straně brány následujícím způsobem:

- *add action=change-dscp chain=forward disabled=no dst-address=10.110.82.2 dst-port=22 new-dscp=56 passthrough=yes protocol=tcp*

Na straně klientského hraničního směrovače je pak možné provést značkování bez závislosti na IP adrese (označí se veškerý provoz protokolu SSH na portu 22 na všechny servery, které klient používá):

- *add action=change-dscp chain=forward dst-port=22 new-dscp=56 protocol=tcp*

V tomto případě hodnota DSCP=56 (111000) odpovídá hodnotě TOS=7 (111) a značí nejvyšší prioritu přenosu.

4.5.3 Typy front systému RouterOS

Pakety, které procházejí skrz router, se při příchodu a zpracování routovacím procesem zařazují do front. Typ této fronty určuje, který paket bude následně vyhodnocen jako nejvíce prioritní a odeslán. RouterOS rozlišuje následující typy front:

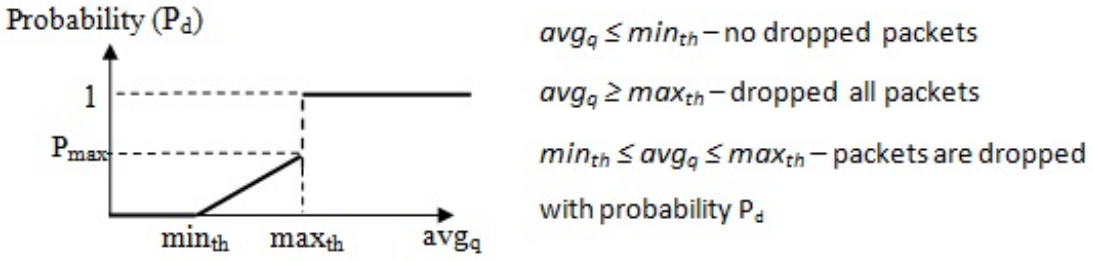
- PFIFO a BFIFO
  - obě fronty jsou typu First-In First-Out, což v praxi znamená, že data, která přijdou na router, jsou ve stejném pořadí i odeslána. Rozdíl mezi PFIFO a BFIFO je pouze ten, že jeden používá jako měrnou jednotku paket (PFIFO) a druhý byte (BFIFO).

- RED (Random Early Drop)
  - mechanismus, který se snaží předejít přetečení fronty tím, že se snaží udržet průměrnou hodnotu její velikosti (avq_q). K tomu mu slouží dvě hodnoty: minimální(min_{th}) a maximální hranice (max_{th}). Pokud je průměrná hodnota menší než minimální hranice, router nezahazuje žádné pakety. Pokud je větší než maximální, jsou naopak zahozeny všechny. V případě, že je velikost fronty v rozsahu (min_{th};max_{th}) jsou pakety zahazovány s pravděpodobností Pd podle vzorce na Obrázku číslo 33:

$$P_d = P_{max}(avg_q - min_{th})/ (max_{th} - min_{th})$$

Obrázek 33: RED - pravděpodobnost zahazování paketů

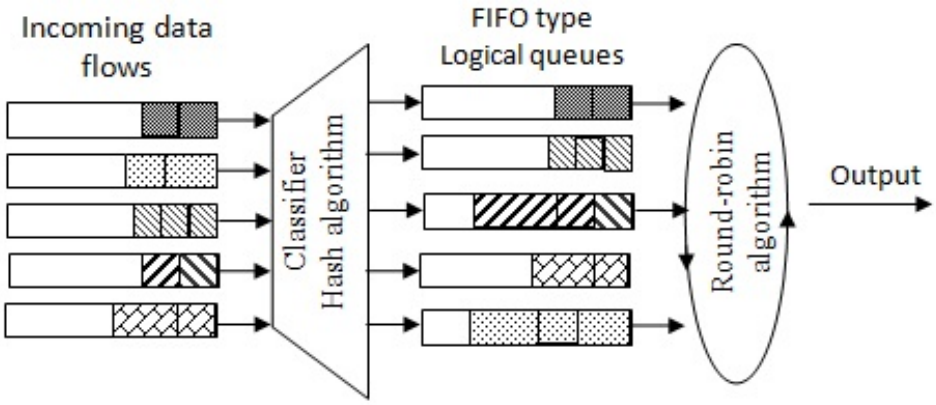
Názorně je možné hranice vidět na Obrázku číslo 34.



Obrázek 34: RED mechanismus

- SFQ (Stochastic Fairness Queuing)
  - mechanismus, který funguje na základě principu rovnoměrného přidělení přenosového pásma otevřeným sessions. Výhoda na velmi přetížených linkách je taková, že se vždy dostane na každého, kdo chce komunikovat. Naopak nevýhodou je, že pásmo nelze přidělit počítačům na základě jejich IP adresy či použitých portů.

- PCQ (Per Connection Queuing)
  - mechanismus, který je velmi podobný SFQ a funguje na základě hashovacího a Round Robin algoritmu. Přidává možnost rozlišení datového toku dle zdrojové IP adresy, cílové IP adresy, zdrojového portu nebo cílového portu. Na základě zvoleného parametru je datový tok rozdělen do nastavitelného počtu front, u kterých lze nastavit šířku pásma. PCQ se velmi často používá, pokud chce administrátor všem garantovat stejné přenosové parametry. Jak algoritmus funguje, je podrobně popsáno na: *http://wiki.mikrotik.com/wiki/Manual:Queues_-_PCQ* a znázorněno na Obrázku číslo 35.



Obrázek 35: PCQ mechanismus

4.5.4 Značkování paketů (mangle)

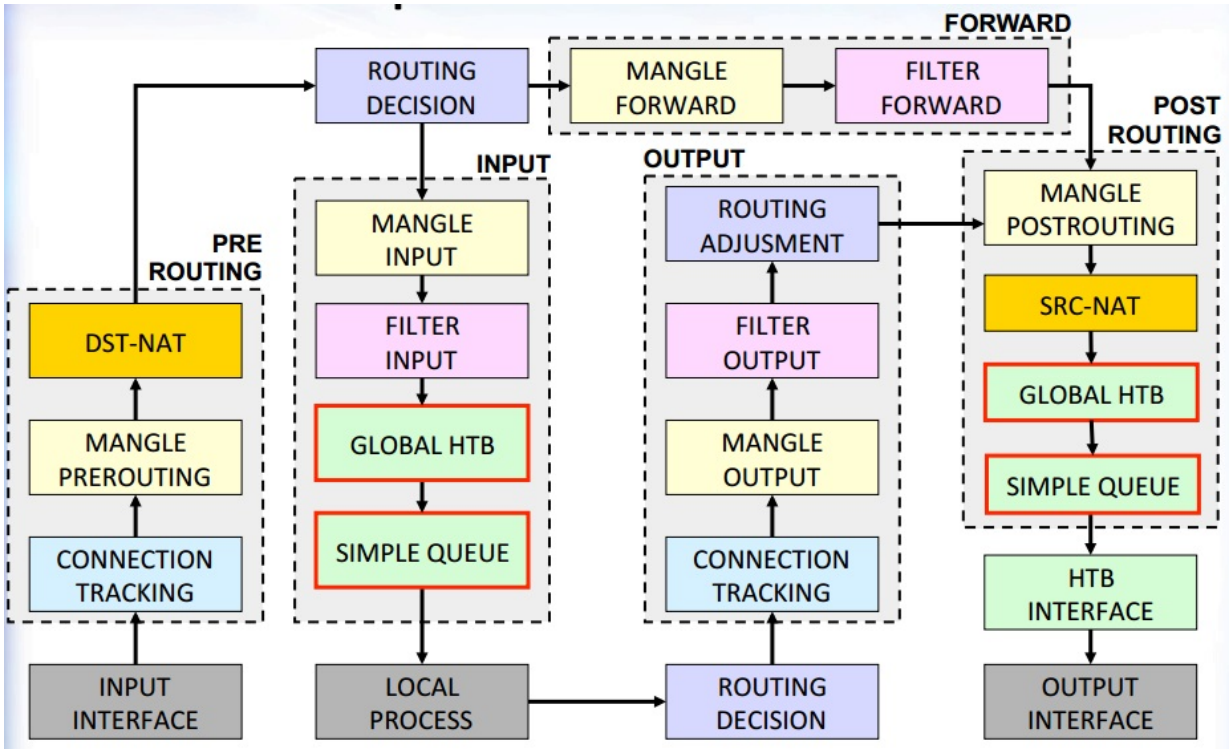
Aby bylo možné paket procházející routerem zařadit do příslušného typu fronty, je nutné jej nejprve označit. Zařazení do fronty nelze v systému RouterOS nastavit na základě značek TOS (DSCP), ale je nutné paket označit unikátní značkou *paket-mark* pomocí značkovacích pravidel (*mangle*). Tato značka slouží pouze pro klasifikaci paketů na daném routeru a po opuštění routeru není dále v síti viditelná. RouterOS umožňuje označení paketů na pěti místech routovacího procesu:

- pre-routing - označí všechny pakety vstupující do routeru
- forward - označí pakety, které pouze procházejí přes router
- input - označí pakety určené pro daný router
- output - označí pakety, které generuje router
- post-routing - označí všechny pakety, které router opouštějí

Vizualizace značení paketů a routovacího procesu ve verzi RouterOS 6.x je vidět na Obrázku 36. Označení paketů lze provést příkazem:

- *ip firewall mangle add action=mark-packet chain=forward comment="pakety_znacka_dscp_56"dscp=56 new-packet-mark=dscp_56 passthrough=no*

Tento příkaz zajistí označení paketů, které procházející skrz router (*chain=forward*) značkou dscp_56 (*new-packet-mark=dscp_56*) a mají hodnotu dscp rovnou 56 (*dscp=56*).



Obrázek 36: Routovací proces - značení paketů

4.5.5 Queue Simple a Queue Tree

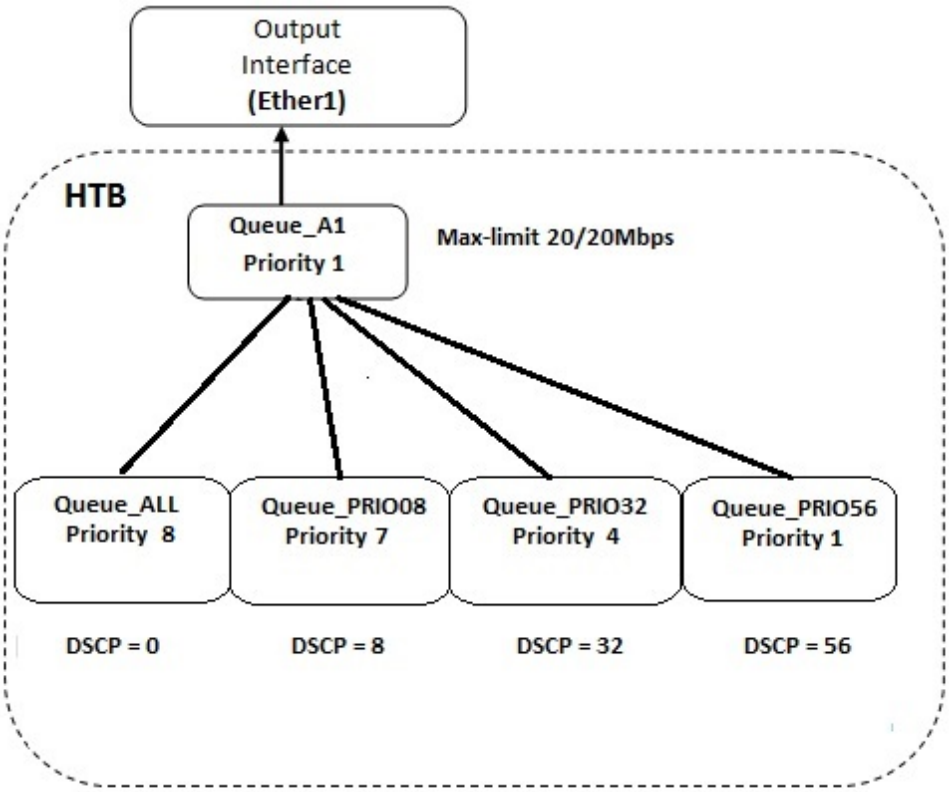
Implementace front v systému RouterOS je založena na HTB (Hierarchical Token Bucket). HTB umožňuje vytvoření hierarchické struktury front a definici vztahů mezi nimi. Od verze 6.x může být tato struktura vytvořena k pouze dvěma místům v routovacím procesu. Tato místa jsou na obrázku číslo 36 zobrazena pod názvy: *GLOBAL HTB* a *INTERFACE HTB*.

- GLOBAL HTB - do fronty jsou zařazeny veškeré pakety procházejí routerem
- INTERFACE HTB - do vybrané fronty jsou zařazeny pakety opouštějící router daným rozhraním

Fronty lze v systému RouterOS nakonfigurovat dvěma způsoby:

- Simple Queue - fronty určené pro základní omezení rychlosti upload/download
- Queue Tree - pokročilé fronty pro priorizaci paketů. K použití je potřeba značek *mangle*.

Jednotlivým frontám lze přiřadit prioritu (*priority=X*), kde X je v rozmezí 1-8 a určuje s jakou prioritou bude daná fronta zpracovávaná, když dojde k přeplnění fronty nadřazené (což může být GLOBAL fronta, INTERFACE fronta nebo uživatelem vytvořená fronta). Příklad čtyř front, podřazeným INTERFACE frontě na rozhraní *Ether1* je znázorněn na Obrázku číslo 37.



Obrázek 37: Queue Tree - HTB

Konfigurace těchto front v systému vypadá následovně:

- add limit-at=20M max-limit=20M name=Queue_A1 parent=ether1 priority=1 queue=default
- add name=Queu_PRIO56 packet-mark=dscp_56 parent=Queue_A1 priority=1 queue=default
- add name=Queue_PRIO32 packet-mark=dscp_32 parent=Queue_A1 priority=4 queue=default
- add name=Queue_PRIO08 packet-mark=dscp_08 parent=Queue_A1 priority=7 queue=default
- add name=Queue_ALL packet-mark=all parent=Queue_A1 priority=8 queue=default

5 Implementace vlastního systému

5.1 Požadavky na systém

Před implementací vlastního systému pro řízení a monitorování síťového provozu bylo nutné stanovit několik základních požadavků, které bude systém splňovat. Tato kritéria byla zvolena na základě znalostí datové sítě občanského sdružení PlzenecNET, o.s. a přizpůsobena jejím potřebám. Mezi tyto požadavky patří:

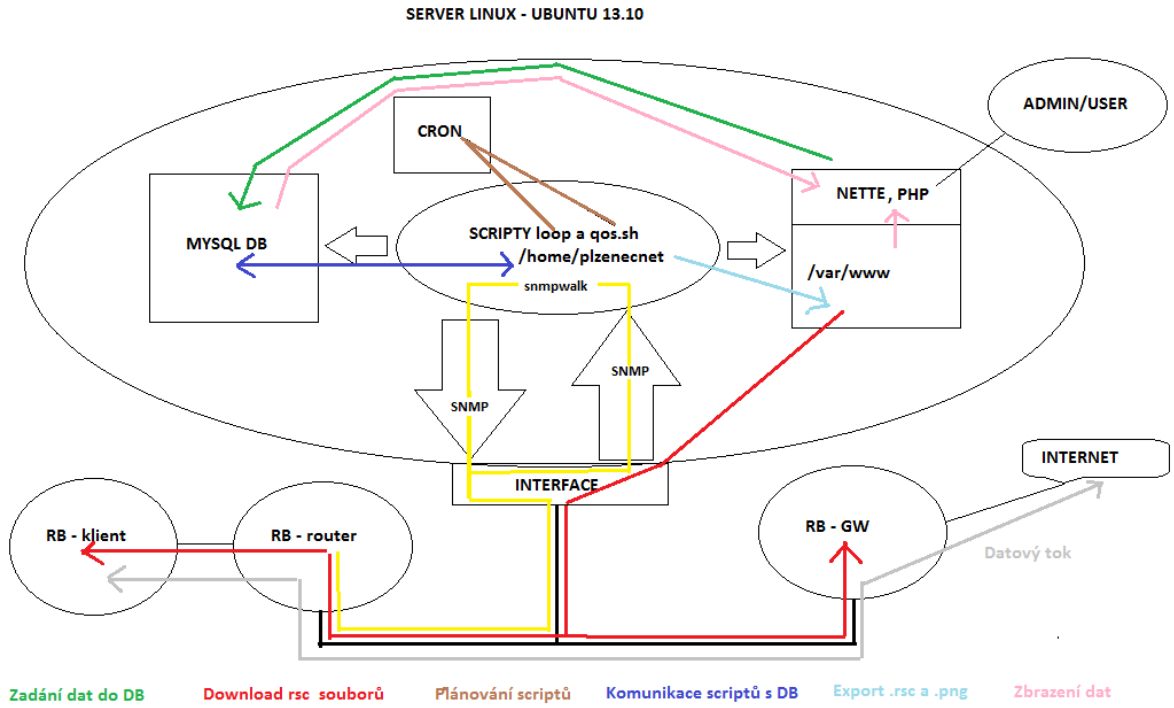
- univerzální monitorovací systém s periodickým sběrem dat
- platforma Linux a rychlý skriptovací jazyk
- webové rozhraní pro snadné ovládání systému a zobrazení dat
- řízení datových toků pro RouterOS v 6.x a vyšší
- podpora osmivrstvého priorizačního modelu na páteřních prvcích
- možnost nastavit pro každého uživatele vlastní priorizační model
- grafické zobrazení monitorovaných dat

Na základě těchto požadavků byly pro tvorbu systému vybrány následující prvky a technologie:

- monitorovací server: 2x Intel(R) Xeon(TM) CPU 3.00GHz, 8GB RAM, 2x WDC WD20EFRX-68E disk 2TB (RAID 1), základní deska: X6DHR-8G2/X6DHR-TG
- operační systém: Ubuntu 13.10
- skriptovací jazyk: Bash
- protokol na vyčítání dat: SNMP v1 a v3
- operační systém pro síťové prvky: RouterOS verze 6.x
- grafovací nástroj: RRDTool
- webový framework: Nette
- webový server: Apache/2.4.6
- databázový server: MYSQL 5.5.37
- testovací prvky pro řízení datového toku: RB1100, RB433AH, RB433AHL, RB2011L, RB450, 2x MiniPCI R52 5GHz

5.2 Serverová část systému

Základními prvky serverové části je databáze, skript na vyčítání monitorovaných dat, skript na generování pravidel QoS, CRON a webový server, který slouží pro zadávání/zobrazení dat. Na serverové části je tímto způsobem implementována dvojí funkcionalita (monitoring sítě a generování pravidel pro řízení datového toku). Na Obrázku číslo 38 je vidět, jak mezi sebou jednotlivé komponenty komunikují a jak spolupracují.



Obrázek 38: Schéma

5.2.1 Databázový model

ERA model je uveden v příloze (Přílohy - ERA model) a pro funkčnost monitorovacího systému jsou důležité následující tabulky:

- vertigo_zakaznik - obsahuje seznam zákazníků
- vertigo_sluzba_internet - obsahuje seznam služeb, které jsou přiřazeny zákazníkovi a nastavuje osmivrstvý priorizační model pro každou službu
- vertigo_qos - seznam služeb, které lze priorizovat
- vertigo_dohled - seznam routerů s jejich IP adresami, které je potřeba monitorovat

5.2.2 Skript pro monitorování sítě

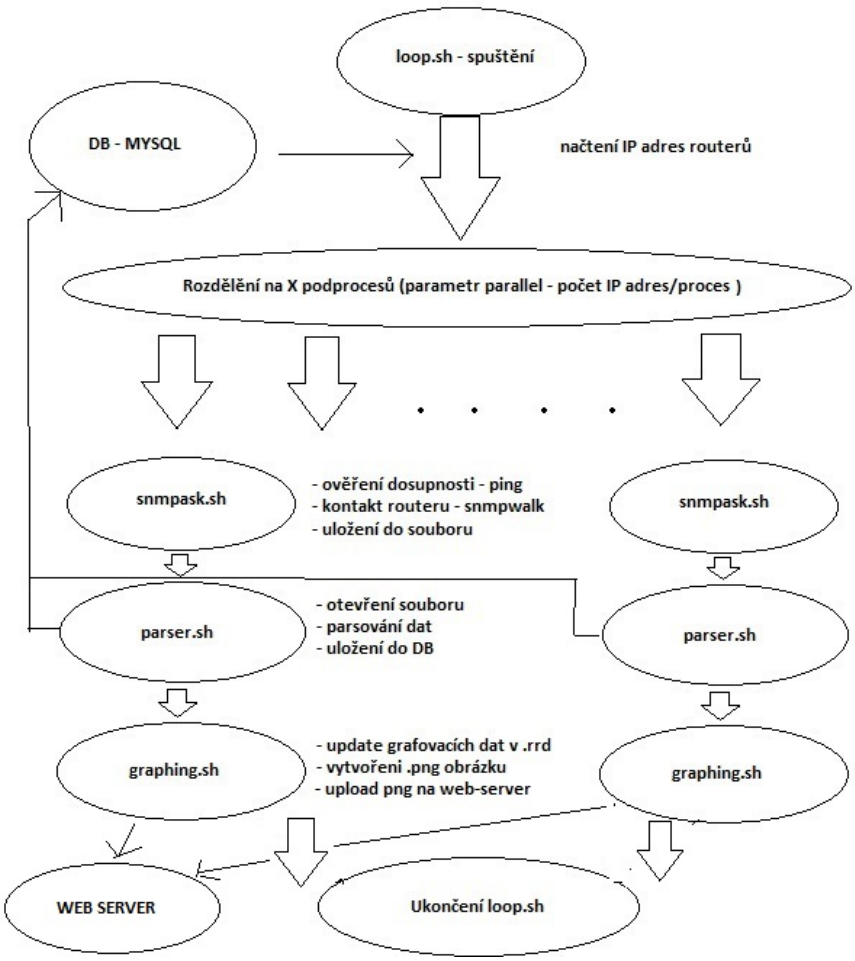
Procesní postup pro úspěšné získání monitorovaných dat z routeru v síti je následující:

- zadání routeru přes webové rozhraní do systému
- zápis údajů do databáze (název, IP adresa) do tabulky vertigo_dohled
- vytvoření RRD souboru pro grafování dat
- spuštění skriptu pro monitoring pomocí CRONu
- načtení všech IP adres routerů do skriptu loop.sh
- ověření dostupnosti routerů pomocí ping a uložení hodnoty
- pomocí nástroje snmpwalk kontaktování všech monitorovaných routerů (SNMP)
- uložení získaných informací do souboru
- zpracování souboru pomocí parseru a uložení dat do DB
- update grafovacích dat v souboru RRD a vytvoření PNG souborů s grafy
- nakopírování PNG souborů do složky webového serveru
- zobrazení získaných dat pomocí webového serveru

O vlastní monitoring se stará skript *loop.sh*, který je umístěn ve složce ./../parser/bin/. Nastavení globálních proměnných pro tento skript se provádí v souboru gobal.conf, který je na serveru umístěn v ./../parser/etc/. Zde je možné nastavit následující parametry:

- mysql: název databáze, uživatelské jméno a heslo pro přístup
- dir names: názvy pracovních adresářů
- snmpwalk: verzi SNMP a OID monitorovaných dat
- rrdtool: cestu k instalovanému nástroji rrdtool
- parallel: počet procesů, které budou kontaktovat routery
- ping: počet ICMP paketů pro získání odezvy a konstantu pro nedostupnost routeru
- parser commands: zápis příkazu pro parser (získání správných hodnot z výstupu)

Po spuštění skriptu *loop.sh.* dochází k rozdělení na několik podprocesů v závislosti na počtu monitorovaných zařízení. V každém podprocesu jsou pak postupně spouštěny skripty *snmpask.sh*, *parser.sh* a *graphing.sh.* životní cyklus je patrný na Obrázku číslo 39.



Obrázek 39: Životní cyklus loop.sh

Výstupem spuštění skriptu loop.sh jsou následující soubory:

- ./../parser/data/new/IP_ADRESA - soubor s výstupem snmpwalk
- ./../parser/data/graph/IP_ADRESA.cpu.rrd - datový soubor zatížení CPU
- ./../parser/data/graph/IP_ADRESA.lat.rrd - datový soubor odezvy routeru
- ./../parser/data/png/IP_ADRESA.cpu.png - grafický soubor zatížení CPU
- ./../parser/data/png/IP_ADRESA.lat.png - grafický soubor odezvy routeru
- ./../www/images/dohled/IP_ADRESA.cpu.png - kopie .png na web-serveru
- ./../www/images/dohled/IP_ADRESA.lat.png - kopie .png na web-serveru

5.2.3 Skript pro řízení datového toku

Procesní postup pro úspěšné nastavení priorizace datových toků v síti je následující:

- Vytvoření služby uživatele přes webové rozhraní
- Zápis údajů do databáze
- Zařazení služeb do prioritního modelu vybrané služby (webové rozhraní)
- Spuštění skriptu pro vytvoření konfiguračních souborů pomocí CRONu
- Načtení IP adres služeb a vytvoření souborů s pravidly
- Upload konfiguračních souborů na webový server
- Načtení souboru do klientských zařízení a GW

O vlastní generování priorizačních pravidel se stará *gos.sh*, který je umístěn ve složce ./../qos/bin/. Nastavení globálních proměnných pro tento skript se provádí v souboru gobal.conf, který je na serveru umístěn v ./../qos/etc/. Zde je možné nastavit následující parametry:

- mysql: název databáze, uživatelské jméno a heslo pro přístup
- dir names: názvy pracovních adresářů
- out file: hlavičky a přípony generovaných souborů

Po spuštění skriptu qos.sh dochází k načtení IP adres služeb, na kterých je potřeba aplikovat QoS. Dle zadaného prioritního modelu se vygenerují příslušné příkazy a uloží se do souboru pro klientský router a GW viz Obrázek 40.

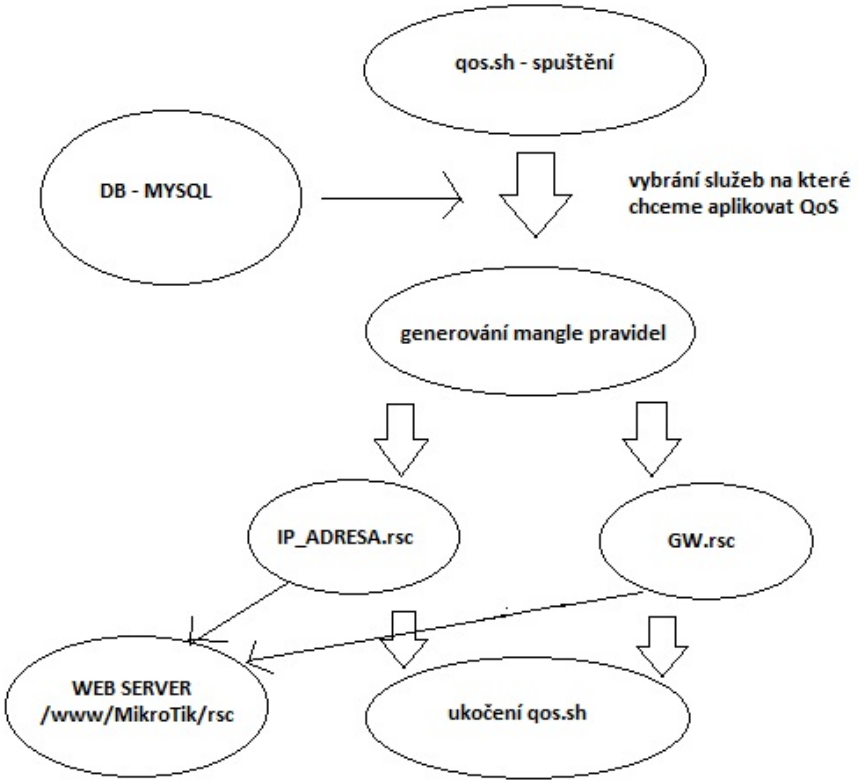
```
/ip firewall mangle remove [/ip firewall mangle find]
/ip firewall mangle
add action=change-dscp chain=forward comment="152_Radek_Vozak_sluzba_5_ping" new-dscp=56 protocol=ICMP
add action=change-dscp chain=forward comment="152_Radek_Vozak_sluzba_5_Kerio VPN_D" dst-port=4090 new-dscp=48 protocol=TCP
add action=change-dscp chain=forward comment="152_Radek_Vozak_sluzba_5_SSH_D" dst-port=22 new-dscp=40 protocol=TCP
add action=change-dscp chain=forward comment="152_Radek_Vozak_sluzba_5_WEB 443_D" dst-port=443 new-dscp=32 protocol=TCP
add action=change-dscp chain=forward comment="152_Radek_Vozak_sluzba_5_WEB_D" dst-port=80 new-dscp=24 protocol=TCP
add action=change-dscp chain=forward comment="152_Radek_Vozak_sluzba_5_CounterStrike_D" dst-port=27015-27030 new-dscp=8 protocol=TCP
```

Obrázek 40: Příklad vygenerovaného souboru s pravidly pro klientský router

Výstupem spuštění skriptu qos.sh jsou následující soubory:

- ./../qos/data/IP_ADRESA.rsc - soubor s příkazy pro klientský router
- ./../qos/data/gw.rsc - soubor s příkazy pro gateway
- ./../Mikrotik/rsc/IP_ADRESA.rsc - kopie .rsc na web-serveru
- ./../Mikrotik/rsc/gw.rsc - kopie .rsc na web-serveru

Životní cyklus skriptu qos.sh je zobrazen na Obrázku číslo 41.



Obrázek 41: Životní cyklus qos.sh

5.2.4 CRON

CRON je cyklický plánovač pro systém Linux. Pomocí tohoto nástroje je možné periodicky spouštět vytvořené skripty ve zvolených intervalech. Zvolen byl interval jedné minuty pro monitorovací skript a pěti minut pro skript na řízení datového toku. V obou skriptech jsou implementovány zámky, které zamezí dvojímu spuštění skriptů, kdyby z nějakého důvodu nestačily v uvedeném intervalu doběhnout do konce. Screen plánovače obsahuje Obrázek číslo 42.

```
# m h  dom mon dow   command
*/1 * * * * /home/plzenecnet/parser/bin/loop.sh
*/5 * * * * /home/plzenecnet/qos/bin/qos.sh
```

Obrázek 42: Plánování skriptů v CRONu

5.3 Síťová část systému

Aby bylo možné z routerů vyčítat požadované informace a bylo možné řídit datový tok v síti, je nutné prvky řádně nastavit a umožnit jim načtení potřebných souborů vygenerovaných na serveru.

5.3.1 Páteřní směrovače

Z páteřních směrovačů je potřeba získat monitorovaná data pomocí protokolu SNMP a proto je nutné na routeru aplikovat příkazy, které zajistí zabezpečenou komunikaci pomocí SNMP v3:

- */snmp community add addresses=0.0.0.0/0 authentication-password=D1pl0mkA encryption-password=D1pl0mkA name=secure security=private*
- */snmp set enabled=yes trap-community=secure*

Dalším krokem je řádné označení paketů dle značek DSCP, aby je následně bylo možné zařadit do fronty.

- */ip firewall mangle add action=mark-packet chain=forward comment="priorita_56" dscp=56 new-packet-mark=dscp_56 passthrough=no*
- */ip firewall mangle add action=mark-packet chain=forward comment="priorita_48" dscp=48 new-packet-mark=dscp_48 passthrough=no*
- */ip firewall mangle add action=mark-packet chain=forward comment="priorita_40" dscp=40 new-packet-mark=dscp_40 passthrough=no*
- */ip firewall mangle add action=mark-packet chain=forward comment="priorita_32" dscp=32 new-packet-mark=dscp_32 passthrough=no*
- */ip firewall mangle add action=mark-packet chain=forward comment="priorita_24" dscp=24 new-packet-mark=dscp_24 passthrough=no*
- */ip firewall mangle add action=mark-packet chain=forward comment="priorita_16" dscp=16 new-packet-mark=dscp_16 passthrough=no*
- */ip firewall mangle add action=mark-packet chain=forward comment="priorita_08" dscp=8 new-packet-mark=dscp_8 passthrough=no*
- */ip firewall mangle add action=mark-packet chain=forward comment="priorita_other" dscp=0 new-packet-mark=dscp_0 passthrough=no*

Posledním krokem je vytvoření fronty na výstupních rozhraních dle kapacity, které je rozhraní schopné přenést. Na následujících řádcích je uveden příklad konfigurace pro rozhraní *Ether1* s fyzickou kapacitou 100/100Mbps. Frontu proto nastavíme na 95Mbps, aby nedošlo k zahlcení linky díky maximální přenosové kapacitě média.

- */queue tree add limit-at=95M max-limit=95M name=Queue_Ether1 parent=ether1 priority=1 queue=synchronous-default*
- */queue tree add name=Queue_PRIO56 packet-mark=dscp_56 parent=Queue_Ether1 priority=1 queue=synchronous-default*
- */queue tree add name=Queue_PRIO48 packet-mark=dscp_48 parent=Queue_Ether1 priority=2 queue=synchronous-default*
- */queue tree add name=Queue_PRIO40 packet-mark=dscp_40 parent=Queue_Ether1 priority=3 queue=synchronous-default*
- */queue tree add name=Queue_PRIO32 packet-mark=dscp_32 parent=Queue_Ether1 priority=4 queue=synchronous-default*
- */queue tree add name=Queue_PRIO24 packet-mark=dscp_24 parent=Queue_Ether1 priority=5 queue=synchronous-default*
- */queue tree add name=Queue_PRIO16 packet-mark=dscp_16 parent=Queue_Ether1 priority=6 queue=synchronous-default*
- */queue tree add name=Queue_PRIO08 packet-mark=dscp_08 parent=Queue_Ether1 priority=7 queue=synchronous-default*
- */queue tree add name=Queue_OTHER packet-mark=dscp_0 parent=Queue_Ether1 priority=8 queue=synchronous-default*

5.3.2 Klientské routery a GW

Zařízení uživatelů a gateway, která řídí provoz do internetu, jsou prvky, v kterých se konfigurace mění dynamicky na základě zadaných dat v systému. Proto není možné pravidla nakonfigurovat ručně, ale je potřeba na zařízeních nastavit skript, který si bude v zadaném intervalu stahovat .rsc soubory ze serveru. Tímto je zajištěno automatické přepisování pravidel na základě vstupu uživatele/administrátora.

Do konfigurace koncového prvku je potřeba přidat skript (Obrázek 43):

```
/system script
add name=get_qos policy=\
    ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,api \
    source="/tool fetch url=\"http://95.47.186.245/MikroTik/rsc/10.110.82.2.rs\
    c\" dst-path=\"10.110.82.2.rsc\";\r\
    \n:delay 2\r\
    \n/import 10.110.82.2.rsc"
```

Obrázek 43: Získání konfigurace pro klientský router s IP 10.110.82.2

Následně skript zařadit do plánovače viz Obrázek 44:

```
/system scheduler
add interval=5m name=get_qos on-event="/system script run get_qos" policy=\
    ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,api \
    start-time=startup
```

Obrázek 44: Plánovač pro skript na získání konfigurace pro klientský router s IP 10.110.82.2

Analogií jsou pak skripty umístěné do zařízení gateway. Pouze místo IP adresy stroje je použito označení *gw.rsc*.

5.4 Uživatelská část systému

Uživatelskou část systému tvoří webový server Apache/2.4.6 a webový framework Nette s podporou PHP5 a možností přímého volání SQL dotazů databáze MYSQL a skriptů shellu. Webová aplikace slouží především pro zobrazení monitorovaných dat a zobrazení grafů. Důležitou součástí aplikace jsou 2 funkcionality:

- Přidání/odebrání nového routeru pro dohled
- Přidání/odebrání nové služby a nastavení prioritního modelu

5.4.1 Přidání/odebrání nového routeru pro dohled

Pokud uživatel přidá nový router do systému, aplikace uloží zadaná data do databáze a následně spustí skript *new.sh*, který zajistí vytvoření .rrd souborů pro daný router ve tvaru IP_ADRESA.cpu.rrd a IP_ADRESA.lat.rrd a umístí je do složky ./../parser/data/graph. Po přidání už jsou informace o monitorovaném routeru obnovovány automaticky na základě funkčnosti skriptu *loop.sh* a zvoleného intervalu v plánovači CRON.

Při odebrání zařízení je volán skript *del.sh*, který zajistí smazání .rrd souborů a také grafů ze složky ./../parser/data/png a ./../www/images/dohled.

Jak probíhá přidání a odebrání routeru z dohledu přes webové rozhraní je zobrazeno v příloze číslo 2 (Uživatelský manuál).

5.4.2 Přidání/odebrání nové služby a nastavení prioritního modelu

Přidání nové služby se pojí pouze s přímým zápisem zadaných dat do databáze. Následné spouštění skriptu qos.sh u služeb, na které chceme QoS aplikovat (na základě příznaku QOS=1), zajistí vytvoření příslušných souborů .rsc.

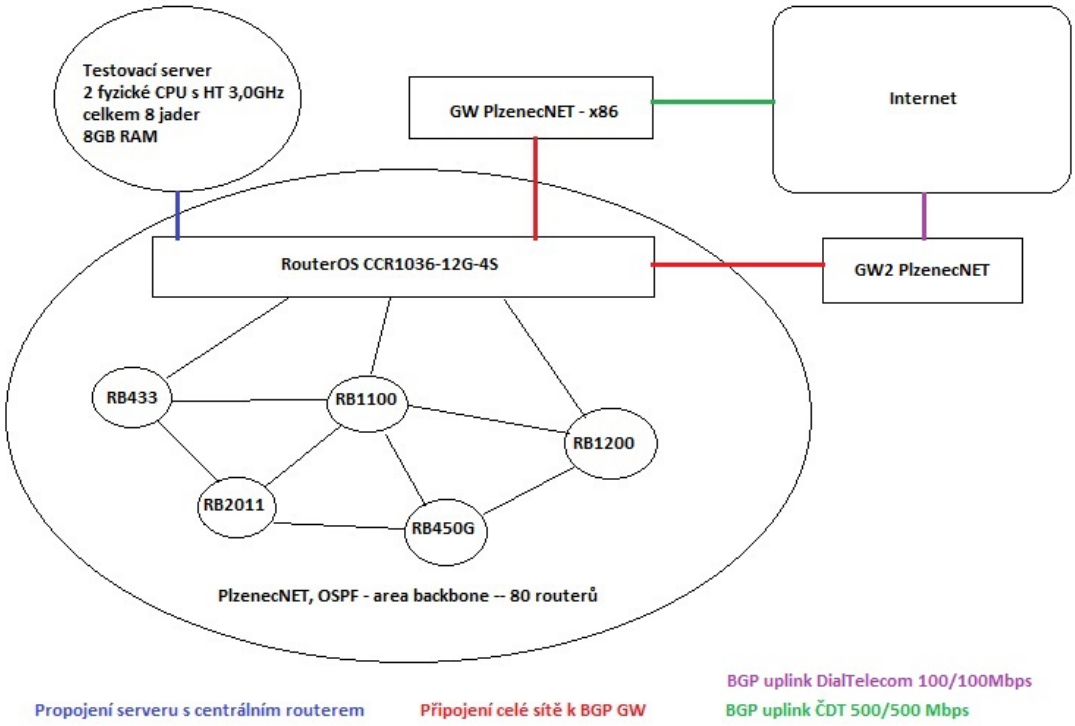
Při odebrání služby je volán skript del.sh ze složky ./../qos/bin/, který zajistí odebrání příslušného .rsc souboru z ./../qos/data/ a ./../Mikrotik/rsc/.

Přidání a odebrání služby je opět zobrazeno v příloze číslo 2 (Uživatelský manuál).

6 Testy systému v reálném provozu

6.1 Monitorování síťových prvků

Test dohledu páteřních prvků proběhl v reálném provozu na páteřní síti občanského sdružení PlzenecNET s 80 routery typu Mikrotik RouterBoard (různé verze desek i operačního systému RouterOS). Všechny routery jsou v umístěny v OSPF backbone-area. V době testu přes centrální router (který distribuuje v síti default-route) probíhal provoz cca 200Mbps směrem do sítě a 50Mbps směrem do internetu. Schéma zapojení je patrné z Obrázku číslo 45.



Obrázek 45: Schéma sítě pro testování monitoringu

Při testech monitorovacího procesu bylo provedeno měření, které mělo za úkol zjistit, při jakém počtu procesů proběhne sběr ze všech 80 monitorovaných prvků nejrychleji. Protože byl test prováděn na serveru, který disponuje 2 fyzickými CPU s podporou HT a 2 jádry/CPU, mohl systém používat 8 jader.

Předpokladem bylo, že pokud by bylo puštěno 8 procesů, z nichž každý by se snažil získat data z 10 routerů v síti, mělo by dojít k nejrychlejšímu ukončení jednoho životního cyklu skriptu *loop.sh*.

počet routerů / proces	1	10	20	50
real	15,891s	11,343s	14,924s	27,153s
user	19,115s	16,815s	13,778s	11,246s
sys	24,030s	21,649s	18,853s	15,966s

Obrázek 46: Výsledky měření pro různý počet spuštěných procesů

Měření bylo v systému Linux provedeno pomocí nástroje *time*. Z výsledků jsou patrné následující závěry:

- Nejrychleji proběhlo načtení údajů v případě, kdy 1 proces obsluhoval 10 routerů. Celkově se tedy muselo spustit 8 procesů, což odpovídá očekávání.
- V případě 50 routerů na proces je patrné nejkratší využití CPU (v uživatelském a kernel módu). Výsledný čas běhu aplikace je však zdaleka nejhorší a to proto, že procesy musely čekat na výstup snmpwalk (I/O operaci).
- V případě 1 router/1 proces je patrná vzrůstající režie. Čas *user* a *sys* je měřen na všech CPU dohromady a proto teoreticky může být větší než doba běhu skriptu *real*.

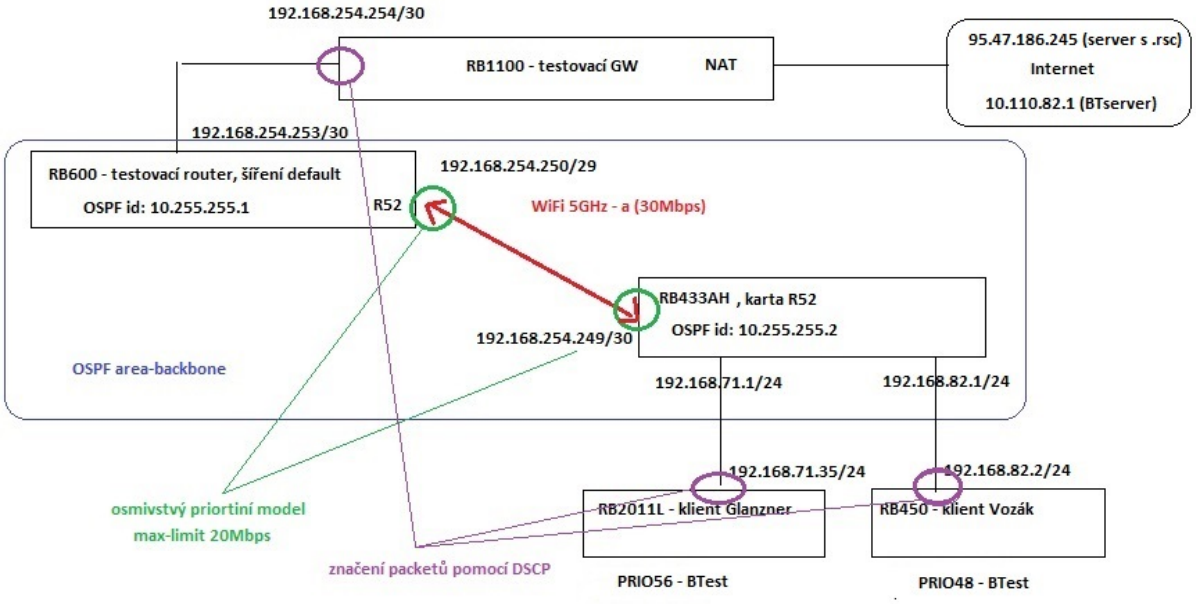
Po spuštění skriptu *loop.sh* došlo k naplnění databáze (viz Obrázek číslo 47) a zapsání hodnot do .rrd souborů. Grafický výstup je uveden v příloze číslo 2 (Uživatelský manuál).

ID_Dohled	ID_Pop	Zarizeni	IP_Zarizeni	SNMP_name	SNMP_description	SNMP_uptime	ICMP_odezva	ICMP_dostupnost	CPU_zatez	Typ	Dohled	Funkce
55	78	SP-Ales-vysilac	192.168.71.202	RouterOS OmniTIK U-5HnD	Ales-vysilac	326 days, 16:25:16.00	2.73	TRUE	0	2	TRUE	0
220	78	Bezinky-spoj-Vysluni	10.110.250.170	RouterOS RB711-5Hn-u.FL	Bezinky-spoj-Vysluni	50 days, 5:18:11.00	2.66	TRUE	1	2	TRUE	0
267	5	Bozkov	10.110.174.1	RouterOS RB433UAHL	Bozkov_RB433AH-vysilace	289 days, 19:17:12.00	2.23	TRUE	2	2	TRUE	4
266	9	Bytovka-router	192.168.72.1	RouterOS RB2011L	Bytovka-router	157 days, 14:02:05.00	2.71	TRUE	3	2	TRUE	3
30	78	SP-Bytovka-RB600-vysilace5G	192.168.72.201	RouterOS RB600A	Bytovka-Vysilace	157 days, 15:00:21.00	2.75	TRUE	12	2	TRUE	0
56	9	SP-Bytovka-vysilace24	192.168.72.202	RouterOS RB532A	Bytovka-vysilace_2,4GHz	157 days, 14:57:29.00	3.61	TRUE	2	2	TRUE	0
28	78	Chlum-spoj-Kysice	10.109.165.253	RouterOS RB433UAHL	Chlum-spoj-Kysice	87 days, 14:22:06.00	7.01	TRUE	9	2	TRUE	0
25	78	Chlum-spoj-Kostel	10.110.249.241	RouterOS RB433AH	Chlum_RB433AH_Trasy	187 days, 0:18:12.00	4.48	TRUE	20	2	TRUE	0
26	78	Chlum-RB433AH-vysilace	10.110.165.201	RouterOS RB433AH	Chlum_RB433AH_Vysilac	241 days, 18:03:44.00	5.5	TRUE	38	2	TRUE	0

Obrázek 47: Naplnění DB pomocí skriptu loop.sh

6.2 Řízení datových toků

Na ovlivňování datového provozu nebylo možné využít infrastrukturu sdružení PlzenecNET. Pro tyto účely byla sestavena testovací síť, která svým zapojením korespondovala se zepojením prvků občanského sdružení (GW, router, OSPF area, bezdrátový spoj). Byly použity desky RB1100, RB600, RB433AH, RB2011L a RB450. Schéma zapojení je zobrazeno na Obrázku číslo 48.



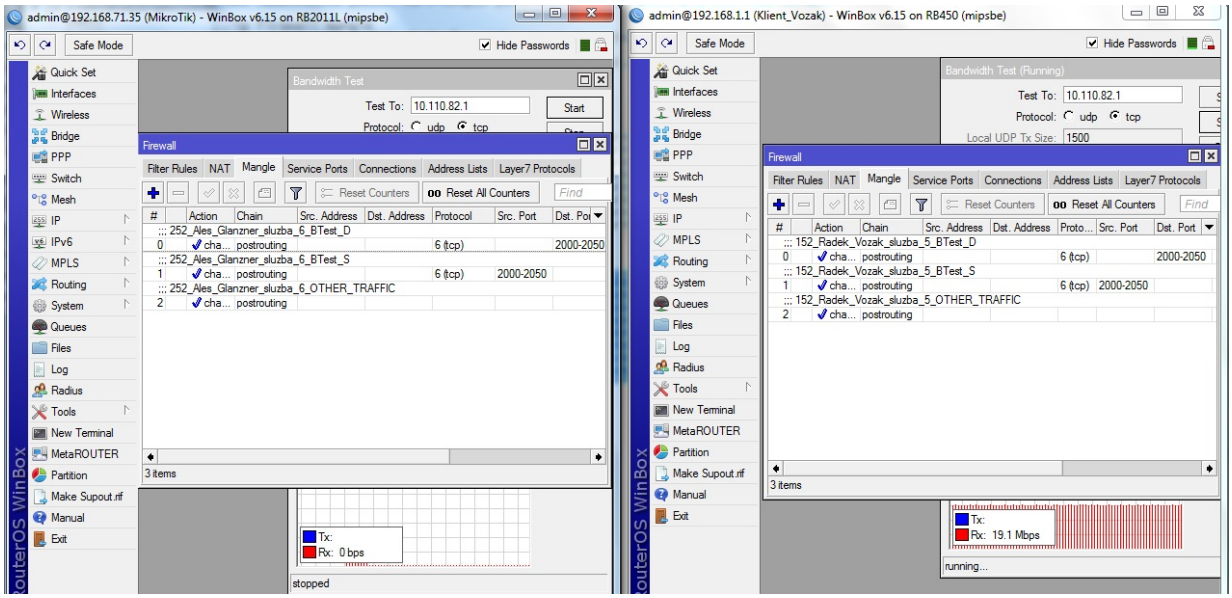
Obrázek 48: Schéma sítě pro testování řízení datových toků

Test byl proveden za následující konfigurace:

- RB1100 - GW s pravidly pro značkování provozu, NAT
- RB600 - OSPF router, který do sítě šíří default route, bezdrátový bod v AP módu, na rozhraní wlan1 nastaven prioritní model s frontou a limitem 20Mbps)
- RB433AH - OSPF router, bezdrátový bod v klient módu, OSPF šíří klientské sítě, na rozhraní wlan1 nastaven prioritní model s frontou a limitem 20Mbps)
- RB450 - klientský router uživatele Vozák. Služba BTest zařazena na úroveň 48.
- RB2011L - klientský router uživatele Glänzner. Služba BTest zařazena na úroveň 56.
- 95.47.186.245 - testovací server (generuje pravidla do .rsc souborů)
- 10.110.82.1 - Bandwidth Test server

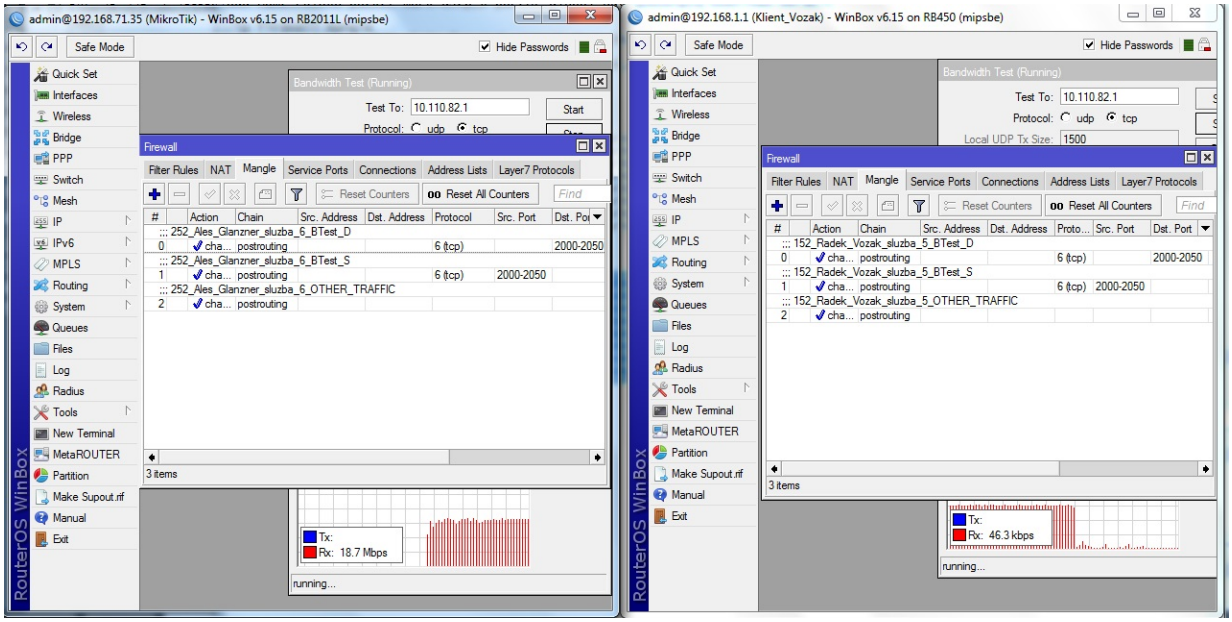
Kompletní konfigurační soubory jsou uloženy ve složce /network na datové disku, který je přílohou diplomové práce.

Prvním krokem testu bylo spuštění BTestu uživatele Vozák se zařazením služby do priority 48. Jak je patrné z Obrázku číslo 49, uživatel byl schopný využít celou přenosovou kapacitu 20Mbps.



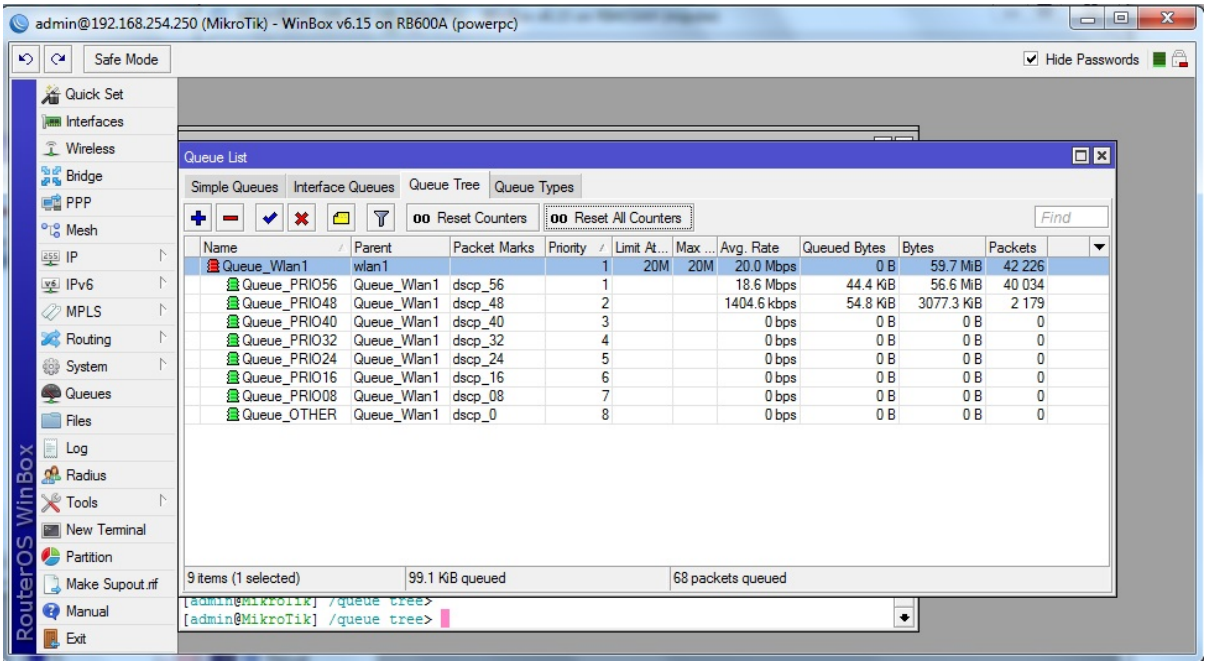
Obrázek 49: BTest uživatele Vozák, priorita 48

Následně byl spuštěn BTtest uživatele Glänzner se zařazení služby do priority 56. Na Obrázku číslo 50 je jasně zřetelné přesunutí datového toku na stranu tohoto uživatele.



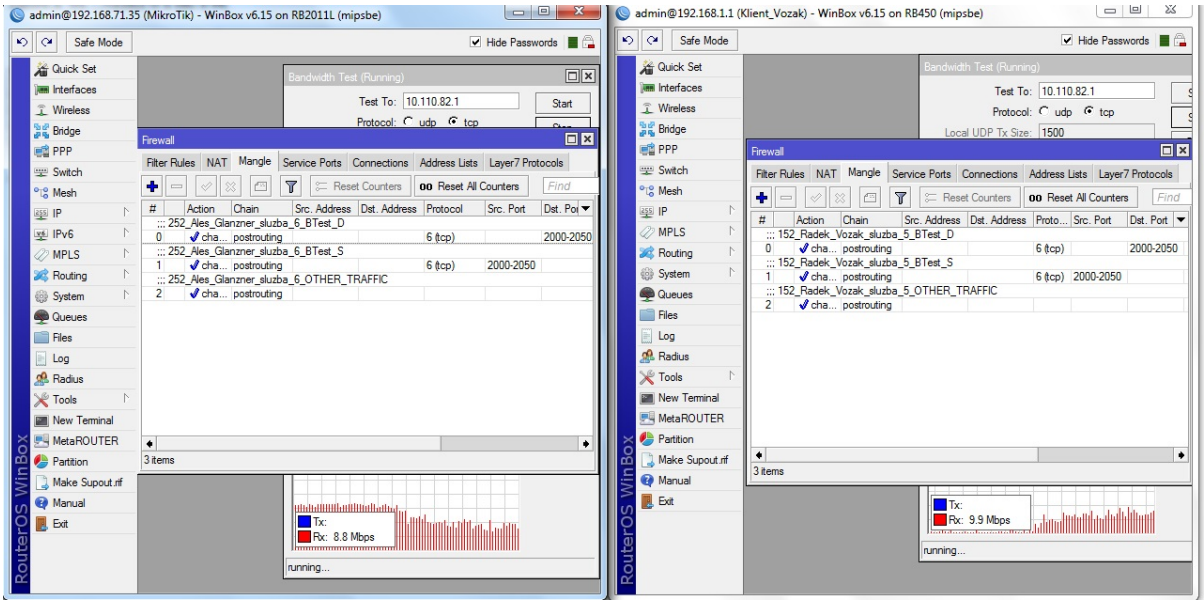
Obrázek 50: BTest uživatele Glänzner a Vozák, priorita 56 vs 48

Na Obrázku číslo 51 je vidět zatížení front na routerboardu RB600. Je patrné, že datový tok s prioritou 56 je upřednostňován před tokem s prioritou 48.



Obrázek 51: RB600 - využití front

Na posledním Obrázku číslo 52 je zobrazeno vyrovnání datových toků obou uživatelů, po přenastavení priority služby BTest u uživatele Vozák na hodnotu 56.



Obrázek 52: Vyrovnané datové toky uživatelů Vozák a Glänzner (stejná priorita 56)

7 Závěr

Teoretickou částí zadání bylo seznámit se se síťovými prvky od firmy Mikrotik RouterBoard, operačním systémem RouterOS a jeho možnostmi použití v oblasti monitorování síťového provozu a řízení datových toků. Tato část byla splněna bez větších problémů vzhledem k tomu, že prvky RouterBoard několik let aktivně používám i konfiguruji. Prvky od tohoto výrobce používá v aktuální době mnoho firem, proto není žádným problémem se s nimi potkat v praxi.

Realizace vlastního systému byla poněkud složitější. K úspěšnému zprovoznění nestačila znalost prvků RouterBoard a operačního systému RouterOS, ale bylo nutné přidat i znalosti operačního systému Linux, skriptování v Bashi, práci s databází MYSQL a také znalost programování ve frameworku Nette a PHP5. Ze všech těchto činností bych mezi ty problematičtější zařadil práci s Bashem. Skripty tvoří hlavní jádro systému a bylo potřeba je naprogramovat a nastavit tak, aby nedocházelo ke zbytečné procesorové režii nebo čekání na vstup. Toho bylo docíleno pomocí spuštění odpovídajícího množství procesů a na rychlosti skriptů se to projevilo v pozitivní míře.

Přesto, že jsou funkce systému RouterOS velmi dobře zdokumentovány na webových stránkách, výrobce už neuvádí problémy jednotlivých verzí operačního systému. Dobrým a nutným zdrojem pro tyto účely posloužilo ISP fórum, kde mnoho lidí řeší velmi podobné záležitosti ohledně skriptování, SNMP a priorizace. Nutno však podotknout, že ve verzi RouterOS 6.15, na které jsem priorizaci testoval, jsem neobjevil žádný problém. Opakem bylo testování dohledu pomocí protokolu SNMP, kde například verze RouterOS 6.13 nebyla schopná odpovědět na dotazy serveru pomocí snmpwalk.

Téma této práce je v současné době velice aktuální. Stále dochází k rozšiřování datových sítí menších bezdrátových poskytovatelů a všichni se snaží zajistit svým klientům kvalitní služby, které by mohly konkurovat profesionálním internetovým poskytovatelům.

Hlavním cílem práce bylo naprogramovat základní monitorovací systém s podporou řízení datových toků v síti. Toho se podle mého názoru podařilo docílit. Bez sebemenších problémů by bylo možné systém rozšířit o další monitorovaná data, která budou administrátora zajímat a přizpůsobit prioritní model požadavkům jakékoliv sítě. Po doplnění systému o administrační záležitosti a systém plateb, bude systém nasazen v testovacím režimu v síti občanského sdružení PlzenecNET, o.s.

Literatura

[1] Web mikrotik http://www.routerboard.com

[2] http://www.routerboard.sk

[3] http://www.mikrotik.com

[4] http://www.root.cz/clanky/mikrotik-jak-funguji-site/

[5] http://home.zcu.cz/ hliboka/

[6] http://www.earchiv.cz/a96/a632k150.php3

[7] http://www.earchiv.cz/a92/a225c110.php3

[8] http://tools.ietf.org/html/

[9] http://wiki.mikrotik.com/wiki/Manual:API

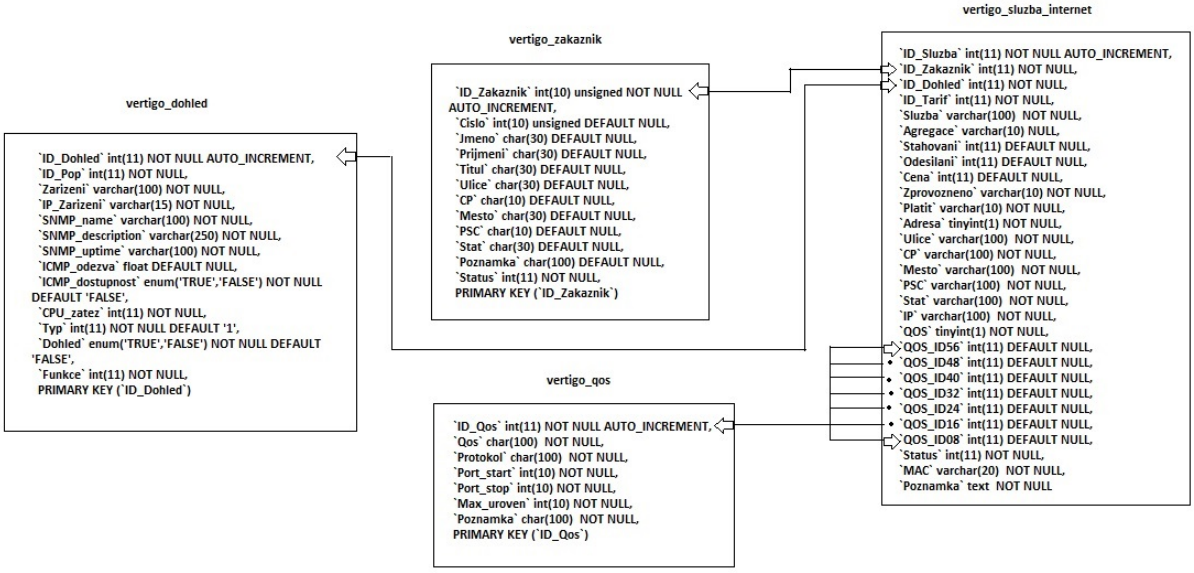
[10] http://www.adminblog.org/2013/06/11/snmp-trap-receiver-with-ubuntu/

[11] http://www.kiv.zcu.cz/ ledvina/Prednasky-PSI-2007/qos-text.pdf

[12] https://ispforum.cz/

Přílohy

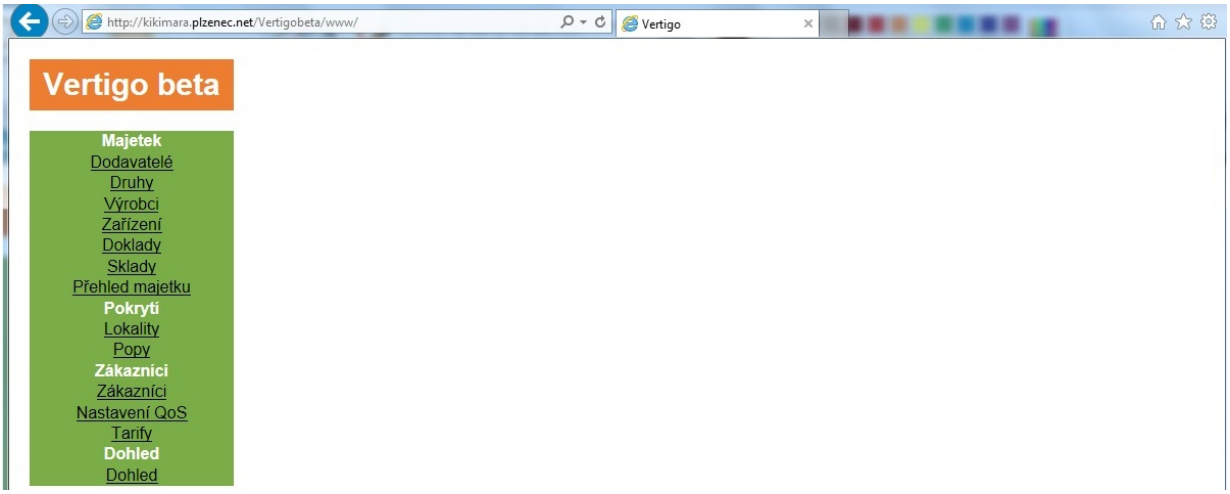
Příloha č.1 ERA model



Obrázek 53: ERA model

Příloha č.2 Uživatelský manuál

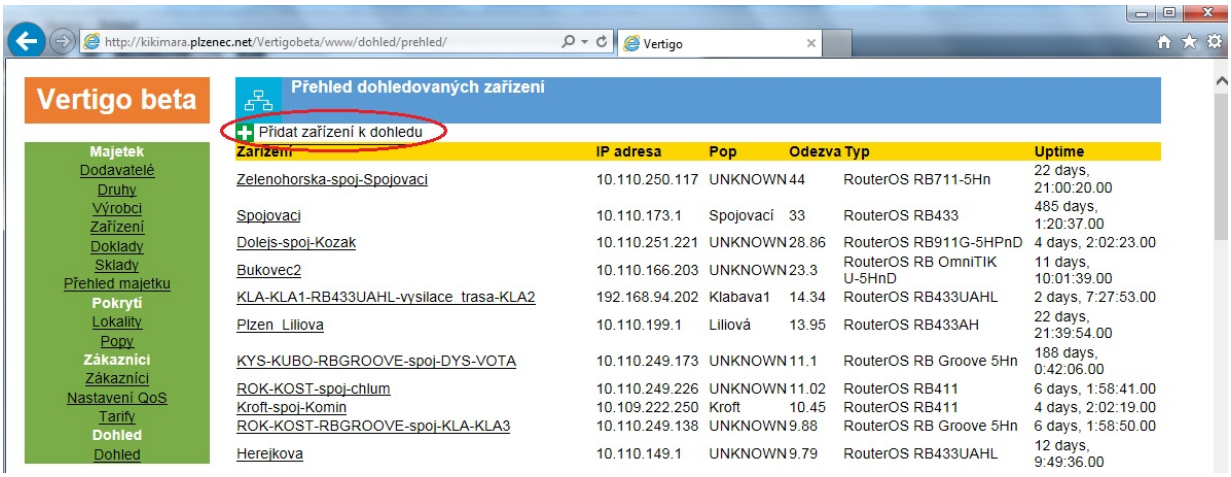
Celý systém je dostupný na adrese: *http://kikimara.plzenec.net/Vertigobeta* s uživatelským jménem a heslem: *diplomka/diplomka*. Po úspěšném přihlášení se zobrazí úvodní obrazovka systému (viz Obrázek číslo 54).



Obrázek 54: Přihlášení do sytému

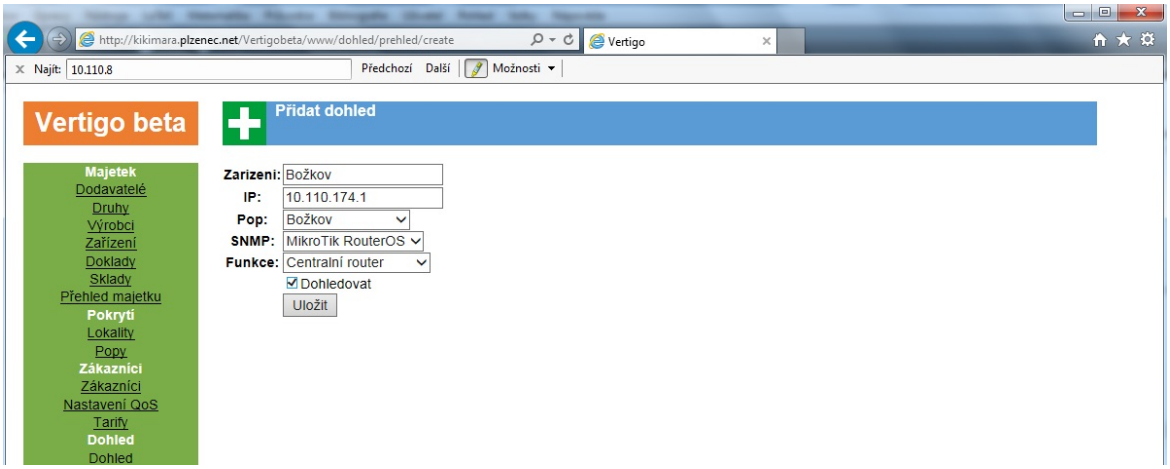
Přidání zařízení do dohledu

Přidání nového zařízení do dohledu je možné provést pomocí odkazu *Dohled* v levé části systému. Po jeho stisknutí se vypíšou aktuálně dohledovaná zařízení. V horní části je odkaz na přidání nového zařízení: *Přidat zařízení k dohledu* (viz Obrázek číslo 55).



Obrázek 55: Přidání zařízení do sytému

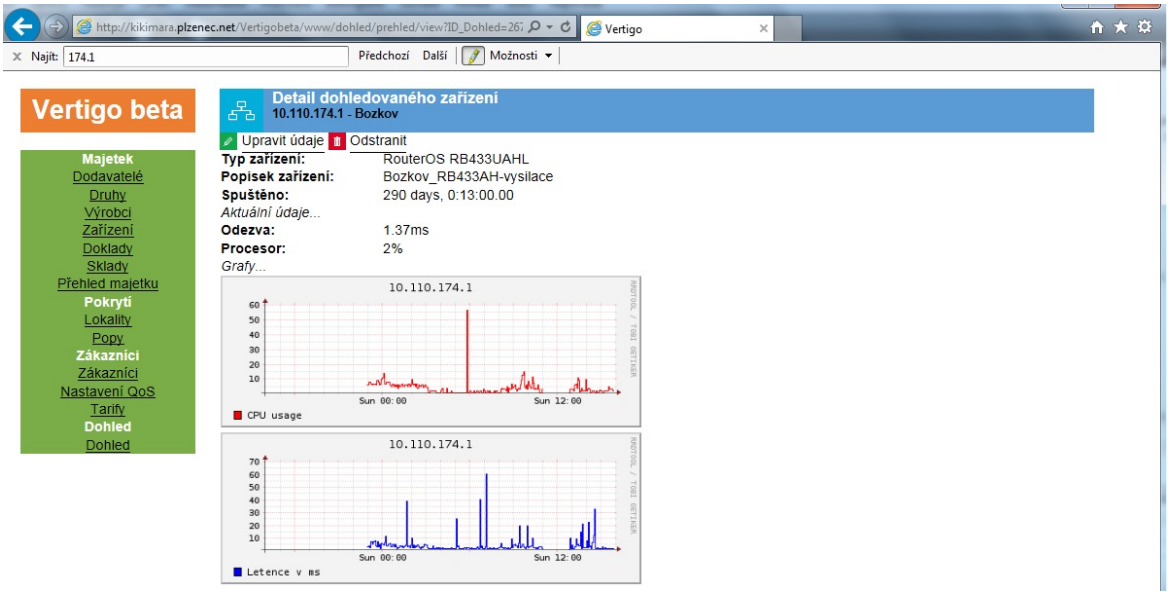
Pro úspěšné zařazení mezi monitorované routery je potřeba vyplnit popis, IP adresu, přiřadit zařízení k fyzickému místu Pop (lze použít UNKNOWN), vyplnit typ SNMP: MikroTik RouterOS, zvolit funkci: Centrální router a zatrhnout políčko *Dohledovat*.



Obrázek 56: Přidání zařízení do sytému - detail

Zobrazení grafů

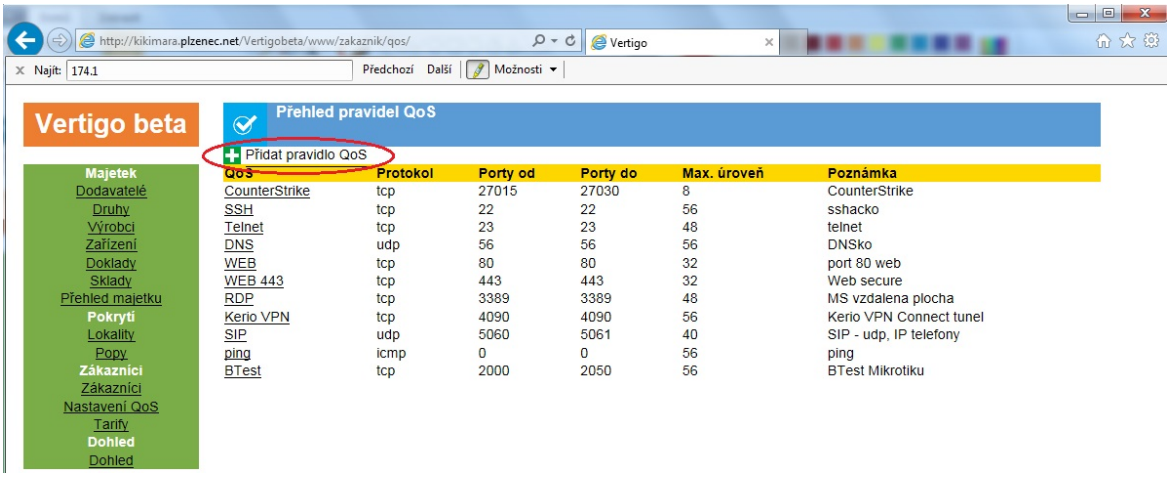
Po cca 15 minutách se u přidaného zařízení začnou generovat grafy, ve kterých jsou dostupné hodnoty 25 hodin zpětně. Pro zobrazení těchto grafů stačí v sekci dohled kliknout na příslušný router. Podrobné informace a grafy se zobrazí jako na Obrázku číslo 57.



Obrázek 57: Podrobné informace o monitorovaném zařízení

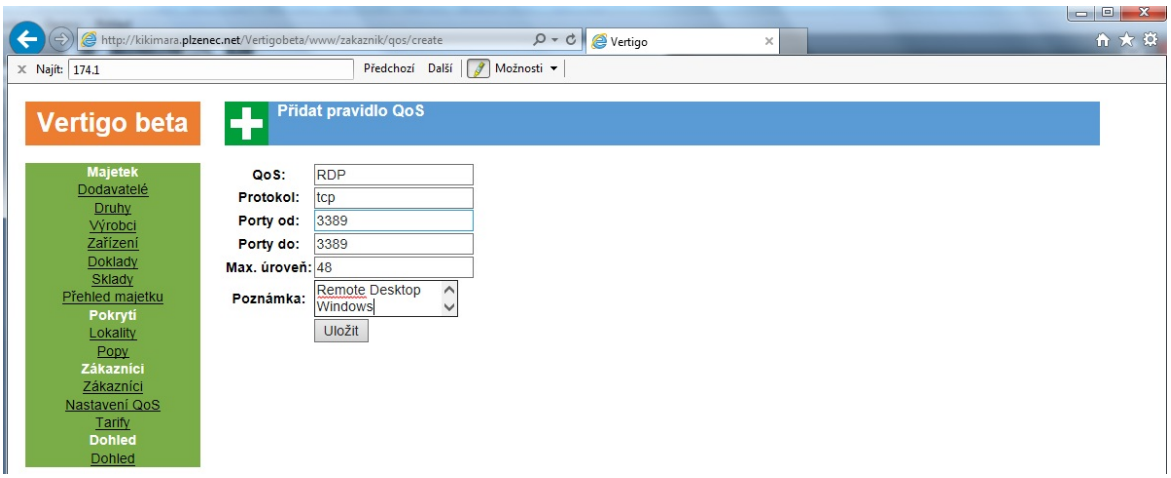
Přidání služby QoS

Přidat službu, kterou bude následně možné zařadit do priorizačního modelu uživatelských služeb, lze provést v sekci *Nastavení QoS* po kliknutí na odkaz *Přidat pravidlo QoS* v horní části (viz Obrázek číslo 58).



Obrázek 58: Přidání služby QoS

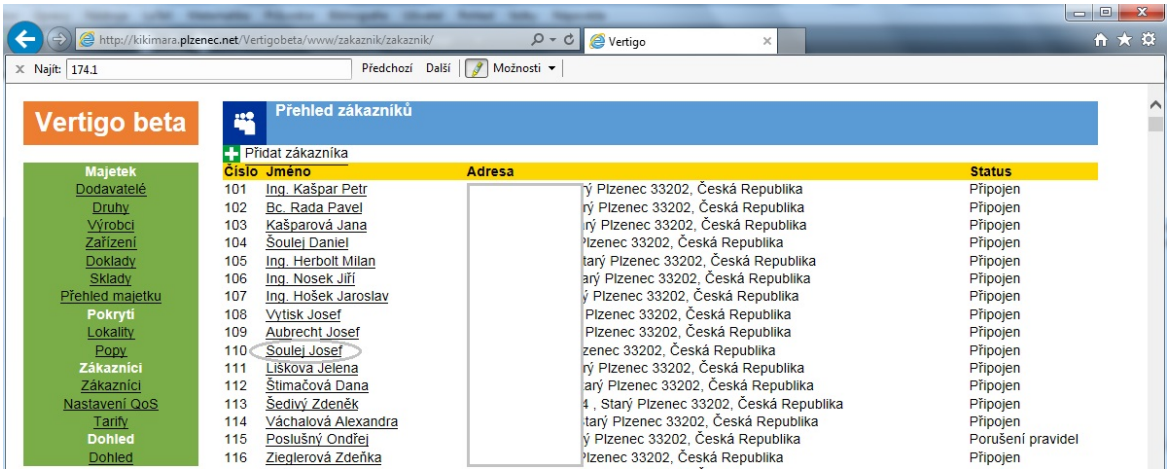
Pro úspěšné přidání služby je potřeba vyplnit protokol (podporováno tcp,udp), rozsah portů (pokud jsou porty stejné, jedná se o jeden port), maximální úroveň zařazení služby (jak vysoko půjde služba zařadit v prioritním modelu) a popis služby (viz Obrázek číslo 59)



Obrázek 59: Přidání služby QoS - detail

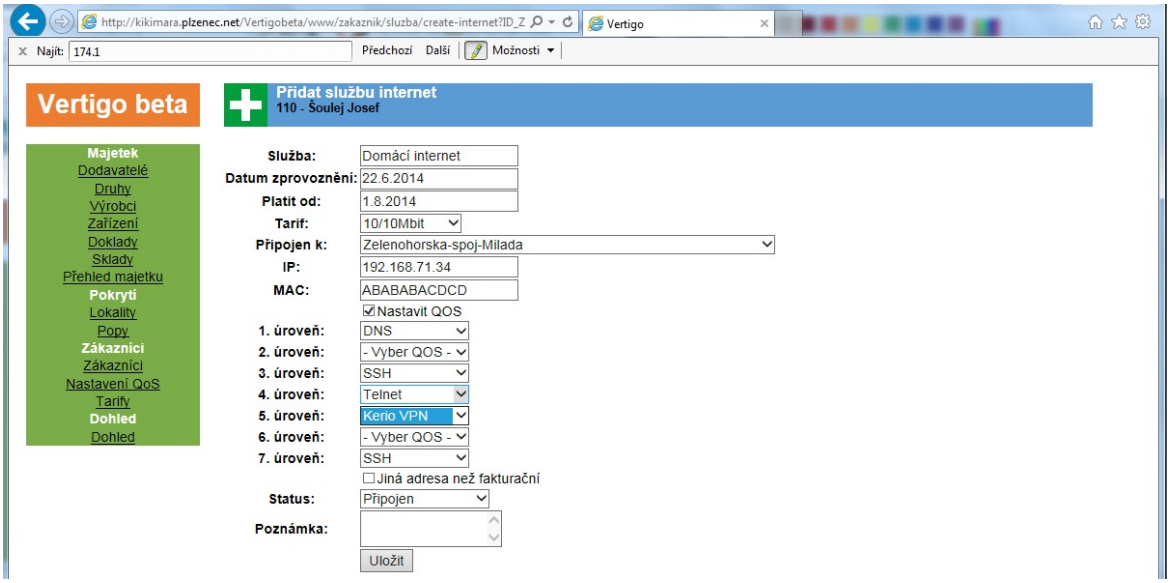
Přidání uživatelské služby

Přidání nové služby je spojeno se zákazníkem. V sekci *Zákazníci* proto zvolíme jméno uživatele, kterému chceme službu přidat kliknutím na jeho jméno (viz Obrázek číslo 60).



Obrázek 60: Vybrání zákazníka

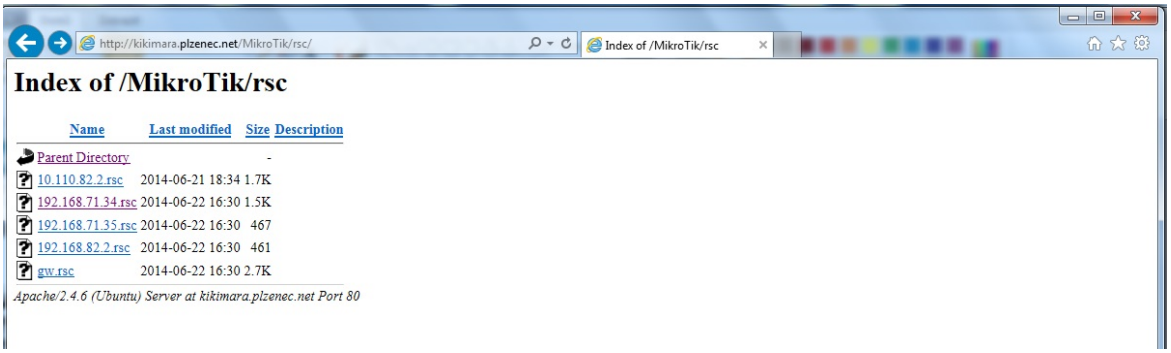
Následně se zobrazí informace o uživateli a je potřeba se přepnout na seznam jeho služeb pomocí tlačítka *Služby* v horní části. Stisknutí *Přidat službu internet* vyvolá formulář, v kterém je možno založit novou službu. Po označení políčka *Nastavit QOS* je možné nastavit 7 úrovní služeb, které je potřeba danému uživateli priorizovat (viz obrázek číslo 61).



Obrázek 61: Založení služby internet

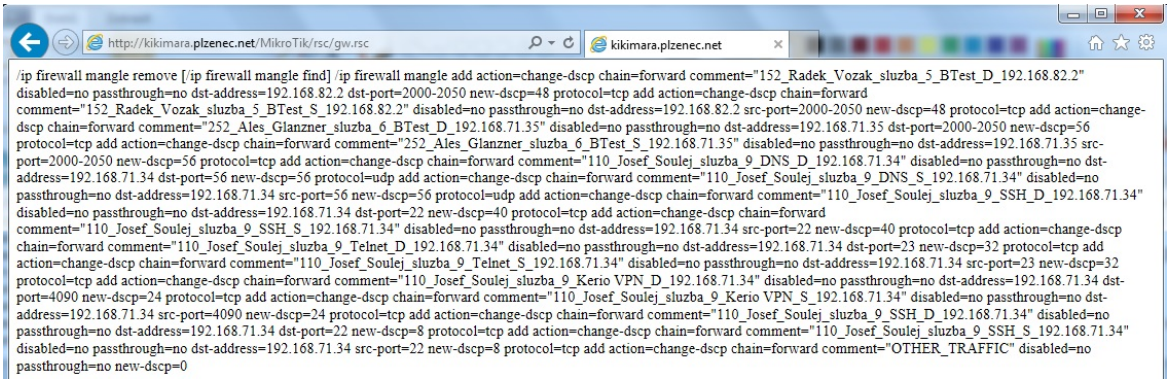
Zobrazení konfiguračních souborů

Po úspěšném založení služby a po spuštění skriptů plánovačem CRON se soubory pro klientská zařízení se zadaným prioritním modelem zobrazí na adrese: *http://kikimara.plzenec.net/MikroTik/rsc/* (viz obrázek číslo 62).



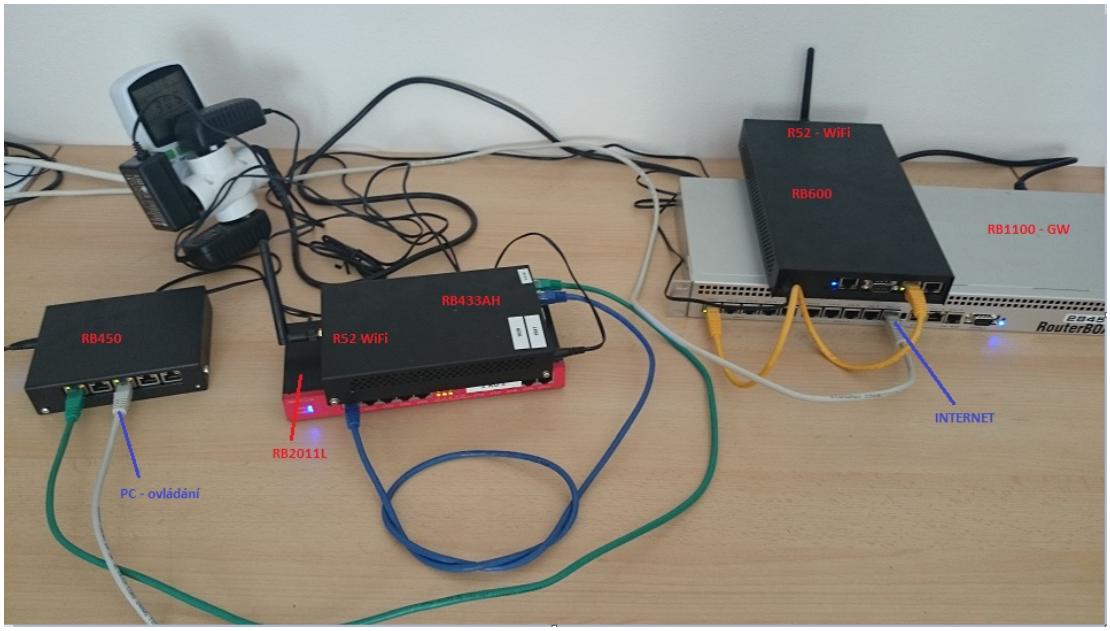
Obrázek 62: Soubory .rsc připravené pro klientské routery

V prohlížeči je možné daný .rsc soubor otevřít a zkontrolovat vygenerovaná pravidla. Detail souboru pro GW je zobrazen na obrázku číslo 63.

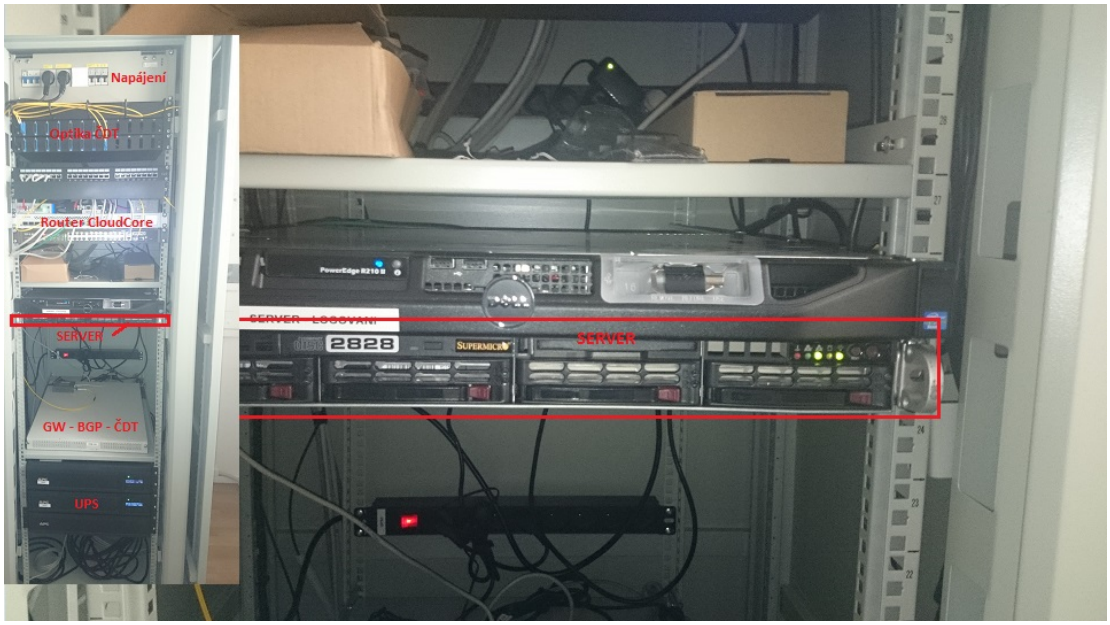


Obrázek 63: Detail .rsc souboru pro GW

Příloha č.3 Fotografie z testování



Obrázek 64: Testovací síť



Obrázek 65: Umístění serveru v racku PlzenecNET, o.s.