Česká zemědělská univerzita v Praze

Technická fakulta

Novinky v problematice routování moderních služeb v rámci počítačových sítí

Bakalářská práce

Vedoucí bakalářské práce: **Ing. Zdeněk Votruba.**

Autor: **Ladislav Hüttl**

Česká zemědělská univerzita v Praze | Technická fakulta

Katedra technologických zařízení staveb | Akademický rok 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ladislav Hüttl

obor Informační a řídící technika v agropotravinářském komplexu

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 16 určuje tuto bakalářskou práci.

Název práce: **Novinky v problematice routování moderních služeb v rámci počítačových sítí**

Osnova bakalářské práce:

1. Úvod
2. Cíl práce a metodika
3. Literární rešerše
4. Routování prostřednictvím PC
5. Routování prostřednictvím specializovaných zařízení
6. Rozšiřující služby na routerech
7. Problematika přechodu na IPv6
8. Závěr
9. Seznam literatury
10. Přílohy

Rozsah hlavní textové části: 30 - 40 stran

Doporučené zdroje:

Kallay, F., Peniak, P.: Počítačové sítě a jejich aplikace, 2. vydání, Grada, 2003, ISBN 80-247-0545-1
HEŘMAN, J., TRINKEWITZ, Z., a kol.: Elektrotechnické a telekomunikační instalace, 2006, Verlag Dashofer, ISBN 80-86897-06-0
VELTE, T., VELTE, A.: Síťové technologie Cisco, CPress, 2003
SPORTACK, A.: Směrování v sítích IP, CPress, 2004
WERNER, F.: Encyklopedie počítačových sítí, SYBEX, 1998

Vedoucí bakalářské práce: **Ing. Zdeněk Votruba**

Termín zadání diplomové práce: listopad 2009

Termín odevzdání bakalářské práce: duben 2011

.....
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
TECHNICKÁ FAKULTA
-3-

.....
Děkan

V Praze dne: 30. 11. 2009

Čestné prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě informací získaných z uvedené literatury a po odborných konzultacích s vedoucím bakalářské práce.

V Praze dne ……. Podpis……

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Zdeňkovi Votrubovi za rady, připomínky a metodické vedení práce.

Novinky v problematice routování moderních služeb v rámci počítačových sítí

New issues in advanced routing in computer network

Abstrakt:

Cílem této bakalářské práce bylo zhodnocení situace řízení síťového provozu v minulosti a budoucí trendy v tomto oboru. Porovnal jsem platformy, které se dnes běžně používají pro routing, jejich přednosti i slabiny. V další kapitole byl popsán velmi populární Mikrotik RouterOS. Předposlední kapitolou je problematika přechodu na IPv6 protokol, jeho přednosti a možné problémy se kterými se můžeme setkat při migraci jak z pohledu systému, tak z pohledu síťové infrastruktury. Poslední kapitola ukazuje praktické nasazení RouterOS do běžných podmínek firemní sítě a sítě poskytovatele služeb internetové sítě.

Klíčová slova: WAN, LAN, BGP, OSPF, MPLS, routing, Mikrotik, RouterOS, QoS.

Summary:

The aim of this work was to evaluate situation of network traffic engineering in past years and future trends in this branch. I draw a comparsion between today used routing platforms, their strenghts and weaknesses. Next chapter contains a description of very popular and widely used Mikrotik RouterOS. Semi-final chapter contains questions about IPv6 transition, weaknesses and strenghts of this new protocol and any problems that IT department may encounter. Last chapter contains practical deployment of Mikrotik RouterOS in general company use and service provider use.

Key words: WAN, LAN, BGP, OSPF, routing, Mikrotik, RouterOS, QoS

Obsah

1 Úvod

Síťové propojení, zvláště pak internetové se dnes stává dalším z běžných prostředků, jako se v minulosti stalo zavedení elektřiny nebo spuštění radiového vysílání. Výhodou oproti minulosti je možnost obousměrné komunikace v reálném čase což uživatele staví do role možnosti aktivně spoluvytvářet obsah internetové sítě.

Celý tento ekosystém v průběhu let od svého vzniku v roce 1962 prodělal překotný vývoj zvláště zavedením protokolu IPv4 v roce 1980, a komercializací v roce 1985. Následné zavedení prohlížení sítě pomocí WWW browseru Mosaic v roce 1993 znamenalo poslední krůček k masovému rozšíření internetového připojení. [1]

Dále již jen uvedu hlavní milníky z pohledu provozovatelů sítí v Československé a později České republiky:

- 1991 - První pokusy s internetovým propojením Praha ČVUT <> Rakouský Linec komutovaným propojením. [2]
- 13.2.1992 - Slavnostní připojení CESNETu k internetové síti trvalým propojením o rychlosti 64 kbit vedoucím z Pražského ČVUT do Rakouské Vídně. [2]
- Přelom roku 1995/1996 - vstup konkurenčních subjektů na pole poskytování internetového připojení, konec monopolu na poskytování datových služeb firmou Eurotel. [2]
- Léto rok 1996 - vznik českého peeringového uzlu Neutral Internet eXchange (NIX)
- 1999 - Vznik bezdrátové normy WiFi 802.11b (11 Mbps, 2.4 GHz) [3]
- 3.10.2002 - Provoz peeringovým uzlem NIX.cz přesáhnul 1 Gbps [4]
- 17.2.2003 - Zavedena možnost peerovat pomocí IPv6 v českém NIXu [4]
- 7.12.2005 -Provoz peeringovým uzlem NIX.cz přesáhnul 10 Gbps [4]
- 27.10.2009 - Provoz NIXu přesáhnul hranici 100 Gbps [4]

Jak je z postupu času vidět provoz v českých sítích se přibližně zdesetinásobí každé 3 až 4 roky. Celkově je jasné, že se tento trend bude prodlužovat v důsledku saturace majoritních last-mile propojení a tím je dnes ADSL; 802.11x a CATV.

2 Cíl práce a metodika

Cílem bakalářské práce bude z teoretického a částečně praktického hlediska zhodnotit vhodnost použití routovacího systému Mikrotik RouterOS pro nasazení v domácích, firemních i velkých síťových prostředích s ohledem na co nejlepší poměr cena/výkon.

V první části bakalářské práce se krátce podíváme na stav vyžití routingu z pohledu velikosti sít í před a po roce 2000 s náčrtem využívání služeb.

3 Literární rešerše

Cílem této kapitoly bude popsat, v jakém stavu nasazení se nachází sofistikovanější routingové systémy včetně výhledu do budoucnosti.

3.1 Před rokem 2000

V této kapitole se zaměřím na užití routingu před rokem 2000 v rozdělení domácí sítě, kde zaměřím na domácí prostředí. Malé sítě pak hodnotím z pohledu firemních sítí, střední sítě a velké sítě z pohledu ISP.

3.1.1 Domácí sítě:

Doba před rokem 2000 se vyznačují tím, že penetrace osobních pc nebyla příliš vysoká. S tím souvisí i otázka připojení k internetu. Majoritním způsobem přístupu k internetu bylo vytáčené připojení po analogové lince (Dial-UP) nebo po digitálním okruhu (ISDN) které dosahovalo rychlostí desítek kilobitů za sekundu. Ceny nebyly také vůbec nakloněné k využívání internetu "na doma", ale spíše k pracovním účelům. Pokud již někdo doma měl, PC a chtěl připojení k internetu tak jasná volba byla klasické Dial-UP připojení kvůli relativně nízké ceně a účtování dle připojeného času. Tehdejší rychlosti bez problémů dostačovaly na procházení webu s občasným stažením souboru přes HTTP, FTP či stahování elektronické pošty POP3 nebo IMAP protokolem. Využívání připojení k realizaci komunikace aplikací, které vyžadovaly nízkou odezvu (VoIP, hraní her apod.) bylo téměř nemožné zvláště u připojení přes analogovou linku, u ISDN toto již nebyl problém. V některých místech se již běžně dalo připojit pomocí rozvodů CATV, kde se rychlosti pohybovali v rámci stovek kilobitů za sekundu s cenou nesrovnatelně lepší, než vytáčené spojeni. Pravidlem bylo, že v celé domácnosti byl pouze jediný počítač, nebylo tedy nutné nijak řešit routing.

3.1.2 Malé sítě LAN do 50 pc (školní, firemní)

U těchto malých sítí před rokem 2000 převládalo také vytáčené připojení k internetu, většinou realizováno jako v domácím prostředí pomocí dial-up modemu či ISDN, několika málo případech řešené pomocí CATV či fixního připojení . Sdílení taktového připojení aspoň z vlastní zkušenosti bylo povětšinou realizováno pomocí web proxy serveru, tzn internet ze sítě šel použít pouze pro procházení webu a stahování souborů přes FTP pokud proxy server měl tuto podporu . Jiné další služby internetu nebylo prakticky možné využívat, důvody byly především zabezpečení lokální stě . Použití proxy serveru bylo jednoduché jednalo se o levný software, který nevyžadoval žádné větší znalosti a poskytoval základní zabezpečení spolu s antivirem na stanicích. Z vlastní zkušenosti mohu říci, že takovéto řešení jsem viděl např. ve školství realizované projektem Internet do škol (INDOŠ), kde jako připojení bylo jednokanálové ISDN (64 kbit) pro celou počítačovou učebnu.

3.1.3 Střední sítě

Do této kategorie se před rokem 2000 řadili s velké části lokální ISP či vznikající czfree sdružení, kteří nabízeli připojení např. pro jedno větší sídliště. Tyto sítě využívaly ke své existenci několik málo routerů. Díky tehdejším cenám profesionálních routerů (např. od Cisco systems) byly hojně využívány klasické osobní počítače s modifikovaným Linuxem s několika síťovými kartami. Jediné místo, kde byl "lepší" router bylo místo odběru konektivity pro síť ISP. Použití Linuxových pc jako routerů sebou neslo také spoustu nevýhod, např. velmi častou nestabilitu a nefunkčnost uzlů. Důvodem bylo použití open source software pro routing, který měl v té době své mouchy. Ve většině případů bylo v této síti použito statického routování. V některých případech i několikanásobného překladu, což způsobovalo nefunkčnost některých služeb či programů, které s překladem nepočítaly ve svém komunikačním protokolu. V těchto sítích už nasazení proxy serveru bylo nemyslitelné, celé sdílení internetu bylo realizováno překladem NAT 1:N.

3.1.4 Velké sítě

Velkých sítí před rokem 2000 bylo velmi málo, do této kategorie se dají zařadit pouze velcí poskytovatelé konektivity se sítí po celém území ČR nebo alespoň z velké části území s vlastní nebo pronajatou zahraniční konektivitou. Takto velké firmy neměly většinou problém s použitím dražších routerů specializovaných na tuto funkci. I když se v jádru někdy stále jednalo i klasickou x86 PC architekturu v zmenšeném provedení (embed) do 19“ racku. Bylo použito buď RIP před rokem 1998 nebo OSPFv2 po roce 1998, který měl nahradit již zastaralý RIP. Výhodou dynamického routingu oproti statickým routám bylo to, že síť ISP mohla být stavěna do kruhu. V případě výpadku jednoho spojení se automaticky přesměroval provoz jiným propojením. Tato vlastnost byla u takto velkých sítí nutností z pohledu spolehlivosti (redundance).

3.2 Po roce 2000

Charakteristické pro tuto etapu je velký rozmach připojení pro domácnosti s tím spojené otázky bezpečnosti. Popis jednotlivých částí je shodný jako u předchozí kapitoly.

3.2.1 Domácí sítě

V průběhu let zvyšování penetrace a snižování ceny internetového připojení se s tímto trendem začal zvyšovat i počet PC v jedné domácnosti. Dnes není zvláštností 3 a více PC na jednu domácnost. Především v době netbooků a podobně levných mobilních zařízení. Domácnosti jsou připojené k internetové síti většinou pomocí xDSL , DOCSIS případně nějakou variantou ethernetu (ETTH,FTTH, 802.11x). Spojeni realizováno buď na cílovém počítači, nebo případně odstíněné routerem realizujícím NAT 1:N za jedinou IP adresou. Je ovšem nutné podotknout, že poměrně hodně se využívá překlad maškarádou i u ISP, např. v Austrálii dostáváte neveřejnou adresu již na WAN port routeru u běžných "consumer" přípojek. Vzniká tak dvojitý překlad, který může mít neblahý vliv na některé služby. Celý důvod použití neveřejných adres je jasný, blížící se den kdy již nebudou volné žádné IPv4 adresy. Ke dni 17.11.2010 zbývá dle webu Hurricane Electric pouze 11 z celkových 256 rozsahů /8 . Velký nástup moderních služeb naprosto vyloučil použití proxy serverů, využití sítě se u domácích uživatelů stává pomalu téměř nutností. Hlavní služby, které domácnosti využívají, se pomalu transformují od prostého stahovaní informací k opačné myšlence, kdy domácí uživatel je ten kdo generuje obsah.

3.2.2 Malé sítě

Dostupnost levnějších sofistikovanějších routerů způsobila to, že i v takto malých sítích se nasazoval routing, kdy se například ve školní sítí oddělí síť studentských počítačů na kolejích a připojených přes WiFi od zbytku školní sítě, kde jsou počítače v kabinetech a školních učebnách. Důvod tohoto oddělení je především bezpečnost. Využívá se statického nebo v několika málo případech dynamického routování spojením s VLAN . Použití proxy serveru v studentské části sítě je nahrazeno sofistikovanějším firewallem, kde se přísně odladí, jaké služby jdou či nejdou použít směrem do internetu. V části školní sítě, kde jsou ostatní školská zařízení, je použití proxy serveru vynuceno pro většinu komunikace do internetu. Proxy server tak slouží jako kontrolní bod pro průchozí provoz, použití s firewallem stejně jako u studentské sítě se dostáváme na základní zabezpečení proti útoku z internetu. Hlavním problémem, se kterým se správci takovýchto sítí museli potýkat, bylo především pomalé internetové připojení, které mnohdy velmi těžce mohlo poskytnout takovou propustnost, jaká byla vyžadována z lokální sítě. Hlavní využívané služby byly především kvůli bezpečnosti omezeny na HTTP/HTTPS a FTP přenos. U studentské části sítě pak podobně nastaveným firewallem pro bezpečnost.

3.2.3 Střední sítě

Tuto kapitolu zastupují především lokální ISP a různá czfree sdružení. V průběhu let se v těchto sítích odehrál stejný vývoj jako v počátcích internetu. Zpočátku používaný statický routing začal být nahrazován nejčastěji OSPF. Důvody byly podobné jako u velkých ISP, tím byla možnost konstrukce kruhových sítí s možností redundance. Co se týče využití BGP tak jsem viděl nasazené pouze u czfree sdružení, které takto routují mezicloudový provoz. Zdárným příkladem takového peeringového uzlu ,kde se hojně využívá BGP je sdružení NFX nebo NIX a pak také mezi sítěmi jednotlivých ISP. Z počátku existence těchto sítí nebylo nutné nijak řídit provoz, všechno bylo zařízeno shapováním zákazníku na rychlosti, které v součtu nedosahovaly rychlosti páteřních propojení. S postupem času začal provoz v sítích ISP narůstat, je to důsledek nástupu výměnných sítí architektury peer-to-peer (P2P) z počátku rozvoje internetu v ČR a velký hlad po internetovém připojení. Důsledkem těchto rychlých změn znamenalo ze strany ISP zavedení měsíčních limitů na přenesená data.

3.2.4 Velké sítě

Do této kapitoly se řádí především sítě "velkých" ISP. V takto velkých sítích, které svojí rozlohou pokrývají několik států, se již od počátku používá dynamický routing. Uvnitř sítě hojně využívané OSPF, které dnes již naráží na své limity a svým určením se posunulo níže na okraje sítě, které většinou tvoří lokální ISP. Uvnitř takto velkých sítích se posledních pár let nasazuje technologie MPLS/VPLS. Důvody přesunu k MPLS jsou na dnešní dobu celkem jasné, provoz v rámci takovýchto sítí dosahoval desítek až stovek gigabit za sekundu a zde již staré konvenční způsoby routingu nestačily. MPLS umožňuje enkapsulaci libovolných protokolů, hlavní výhodou oproti klasickému OSPF je ta, že LSR (Label Switching Router) není nucen prohlížet celý paket, ale pouze přečte tento index a podle něj se řídí a pošle jej dále. Síťový routing mezi jednotlivými sítěmi (AS) zařizuje BGP (Border Gateway Protocol). V takto velkých sítích je velké množství různorodého provozu, někteří ISP dávají přednost jistému provozu před jiným. Jedná se především o provoz, který je citlivý na latenci jako je např. VoIP nebo IPTV.

3.3 Výhled do blízké budoucnosti

Velký rozvoj připojení domácností k internetové sítí začal postupně ukazovat hlavní slabinu majoritně využívaného IPv4 protokolu a tím je jeho malý adresní prostor. Důsledkem toho na začátku února 2011 IANA rozdělila poslední adresní rozsahy lokálním registrátorům. Řešení problému nedostatku adresního prostoru je IPv6 které se zatím nasazovalo na testování pouze na páteřních sítích větších ISP. Podpora na straně domácích zařízení byla zpočátku prakticky nulová, ale to se již značně změnilo s koncem IPv4 a tedy podpora IPv6 je již implementována na zařízeních, které nejsou starší 2 let, případně se podpora dá doplnit prostým update firmware v zařízení. Postupně se tedy IPv6 dostává i na poslední míli ke koncovému zákazníkovi a tím je NAT technika. Z druhé stránky si troufám tvrdit, že hlavně z počátku bude pro domácí uživatele poměrně problémové

nasazování IPv6 z pohledu zabezpečení a funkčnosti. Doteď byl domácí uživatel před útoky z internetové sítě skryt za domácím routerem realizujícím NAT. S nasazením IPv6 tato ochrana úplně odpadne a všechna zařízení budou dostupná z celé internetové sítě. Bude tedy velmi záležet na tom jak se výrobci operačních systému a routerů k tomuto problému postaví. Nastane doba kdy odladěný firewall ať již v routeru nebo v počítači bude nutností pro základní zabezpečení. Podobný problém se bude řešit i na firemních sítích, kde se nasazování IPv6 posune na dobu kdy již hardware a software bude plně odladěn pro provoz na IPv6 protokolu.

4 Routování prostřednictvím PC

Užití klasických PC k routování vzniklo jako jedna ze služeb poskytovaných v rámci lokální sítě z "centrálního" serveru jako levná alternativa k profesionálním routerům, které byly pro menší subjekty finančně nedostupné. Z pohledu větších ISP byly a jsou PC routery využívány buď jako náhradní řešení nebo v případě malých ISP jako hlavní platforma pro routing především z důvodu ceny a možnosti softwarové rozšiřitelnosti o další služby jako firewall, traffic shaper a hardwarové rozšiřitelnosti hlavně co se NIC karet týče. Hlavní nevýhodou PC platformy pro routing je především nulová možnost jakékoliv akcelerace. Je to způsobeno univerzálností PC architektury, která byla koncipována pro velké množství použití. S tím souvisí fakt, že router je tak rychlý jak rychlý je nainstalovaný procesor a sběrnice na kterou jsou připojeny všechna síťová rozhraní a jejich počet. "Je udáváno, že na 1 kilobit čistého routovaného jednosměrného provozu je třeba 1 kHz výkonu procesoru." [5]. Pokud se k routingu přidá ještě traffic shaping, firewall a QoS tak výkon takovéhoto routeru se velmi rychle snižuje. Rychlost se přímo odvíjí od velikosti a množstvím paketů, které musí router zpracovávat a počtu pravidel které musí vykonat nad každým paketem. Z tohoto pohledu je jasné, že PC nelze používat pro routing velkého provozu. Dnešní běžné PC o konfiguraci 2 GHz CPU může obsloužit linku o rychlostech stovek megabit s jednoduchými pravidly ve firewallu. Výkon routeru se odvíjí také od jeho vlastní softwarové konfigurace. Existují speciálně upravené verze linuxu které jsou k tomuto účelu přímo určeny. Takové systémy jsou například komerční Mikrotik RouterOS nebo zdarma M0N0wall a jeho deriváty a případné jiné distribuce linuxu, které si člověk vytvoří sám. Celkově to lze shrnout tak, že PC router je vhodný do malých až středních sítí s malým provozem v režii desítek megabit nebo jednotek stovek megabit. Jeho hlavní nevýhodou je to, že každý paket musí projít od síťové karty přes sběrnici do procesoru, tam se provede dle pravidel jeho zpracování a pak jde zpět přes sběrnici do síťové karty a dále po sítí. Hlavním kladem tohoto řešení je především cena a dostupnost takovýchto řešení.

5 Routování prostřednictvím specializovaných zařízení

V této části popíši Mikrotik RouterBoard a RouterOS jakožto velice populární routovací platforma používaná ve velké míře lokálními poskytovateli připojení a také domácnostmi a menšími firmami.

5.1 Úvod

Systém Mikrotik RouterOS vzniknul v roce 1995 jako alternativa k systémům Cisco. První verze mikrotik RouterOS byly prostým embed linuxem s integrovanými open source nástroji pro řízení provozu. V průběhu času se hodně změnilo, již velká část routovací části systému není postavena na open source nástrojích, ale jsou komplet přepsány od základu. Tímto krokem se systém pomalu zbavuje problémů, které používání OSS přináší a nejsou zde problémy s licencováním.

5.2 RouterBoard

V této kapitole se lehce nahlédnu do nabídky boardů určených pro provoz RouterOS. Nabídka zařízení se dělí na 3 hlavní větvě. První z nich jsou boardy čistě pro nasazení do páteřních ethernetových sítí, jejich hlavní výhodou je vysoký výkon v nasazení routeru, QoS provozu a je u nich možná instalace do 19" racku. Díky integrovanému AES/3DES akcelerátoru je možné použít i jako vytížený VPN koncentrátor. Nevýhodou je absence možnosti přídavných karet formátu miniPCI či PCI. Do této kategorie se řadí RB série 1000 a vyšší (Obr 1).

Obr. 1 Mikrotik RouterBoard 1000 (1a) a provedení 19“ rack (1b)

1a

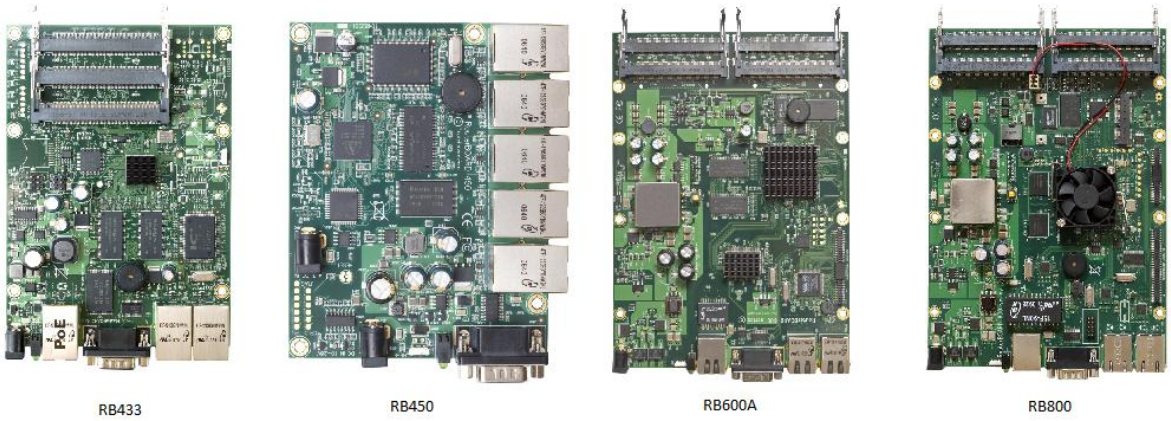
1b

Zdroj: www.routerboard.com

Zařízení z druhé větve je určeno především na prvky, které se nalézají na přístupové síti. Jedná se především RB řady 433, 450, 600, 800 (Obr 2.). Řada 433 je vhodná pro budování místních přípojných bodů (Access Pointů) díky většímu počtu miniPCI slotů. Řada 450 je určena jako čistě ethernet router vhodný např. pro připojení menšího panelového domu. Řada 600 je určena jako vysokorychlostní přístupový bod nebo

jako základ pro P2P spojení pomocí protokolu Nstreme nebo NV2. Řada 800 je vhodná pro kombinované nasazení jako ethernet a přístupový bot spolu s P2P spojením.

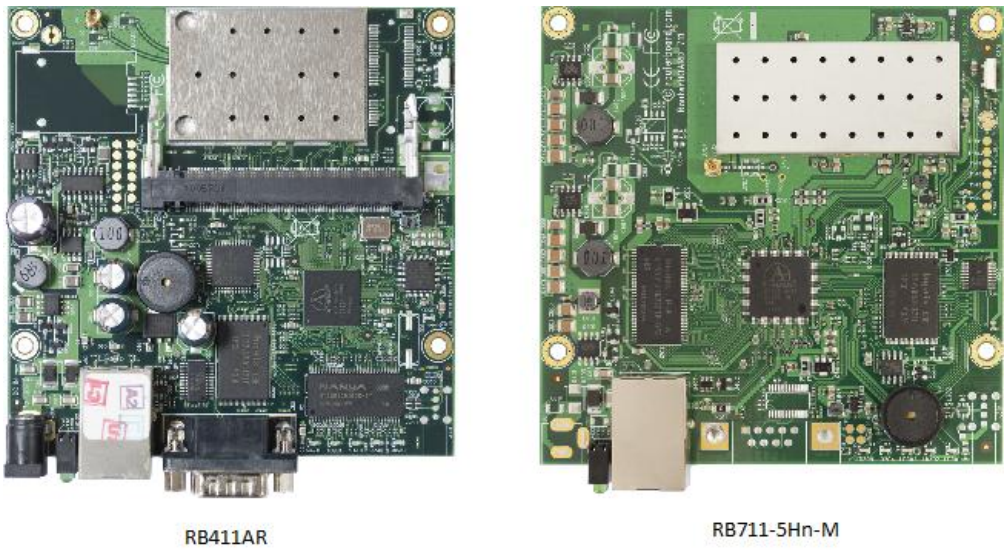
Obr. 2 Řady RouterBoardy vhodné pro přístupovou síť



Zdroj: www.routerboard.com

Poslední řada je určena především jako zařízení pro bezdrátové koncové zákazníky (CPE). Jsou jimi RouterBoardy řady 411 vhodné pro bezdrátové instalace v pásmu 2,4 GHz a 711 vhodné pro instalaci bezdrátových klientů v pásmu 5 GHz (Obr 3.). Jejich výbavou bývá už na boardu integrovaný WiFi modul případně další přídavný slot pro miniPCI či miniPCI-E kartu a jeden či dva ethernet porty. Specialitou RB411U a RB411UAHR je přítomnost SIM slotu pro realizaci datového spojení přes mobilní síť GSM operátorů po vložení 3G/2,5G modemu do miniPCI-E slotu. Některé další RB mají k dispozici i USB nebo slot pro vložení paměťové karty typu USB FLASH nebo MicroSD.

Obr. 3 RouteBoardy řady 411 a 711



Zdroj: www.routerboard.com

Obecně lze říci, že každý RouterBoard kromě Řady 1000 má možnost napájení po ethernetu (IEEE 802.3af) tím jsou RB vhodné pro instalace na stožáry, kde ne vždycky je k dispozici napájení ze silové sítě.

5.3 RouterOS

Jak již bylo řečeno v úvodu, RouteOS je postaven na linuxovém jádře. To spolu nese jisté výhody z pohledu podpory hardwaru. V aktuální verzi RouterOS V5-RC je linuxové jádro verze 2.6.35. Podpora ethernetových karet se odvíjí od ovladačů přímo v kernelu linuxu. U WiFi karet je podpora pouze na chipsety Atheros a Prism. Systém se dále skládá z jednotlivých balíčků, které vykonávají vždy jen určitou část funkčnosti. Je tedy možné si v těchto mezích systém přizpůsobit danému nasazení a tím např. zredukovat nároky na hardware obecně. Systém funguje na platformách RouterBoard která je hlavním podporovaným hardwarem pro provoz systému RouterOS. Systém je též k dispozici pro platformu x86, kde nemá k dispozici některé součásti jako např. nový protokol NV2.

Tabulka 1 Balíčky RouterOS

Název balíčku v systému	Funkce
Advanced-tools	Nástroje pro ping, skenování a nástroj netwatch
Calea	Nástroj pro získávání dat (pouze v USA)
DHCP	Klient a server protokolu Dynamic Host Configuration Protocol
GPS	Podpora systému GPS
Hotspot	Nástroj pro vytváření hotspot přístupového bodu
IPv6	Podpora adresace protokolu IPv6
MPLS	Podpora Multi Protocol Label Switching
Muticast	Podpora IGMP proxy a PIM multicast
NTP	Klient a služba síťového času
PPP	Podpora klienta a serveru protokolu PPP, PPTP, L2TP, PPPoE, ISDN PPP
Routerboard	Přistup ke správě specifických vlastností routerboardů, umožňuje upgradovat BIOS na routerboardech
Routing	Podpora dynamických routovacích protokolů BGP, OSPF, RIP a nástrojů pro filtraci routovací tabulky
Security	Podpora IPSEC, SSH a bezpečného přihlášení winbox
System	Základní funkce routeru jako statické routování, management IP adres, telnet, queues, firewall, web proxy, DNS cache, TFTP, IP pool, SNMP, packet sniffer, Torch, network bridge, VLAN, VRRP a základní tunely EoIP, IPIP.
UPS	Podpora záložních zdrojů APC přes RS-232
User-manager	Management uživatelů Mikrotik
Wireless	Podpora bezdrátových karet Atheros a Prism
Wireless-tes	Testovací balíček pro bezdrátové karty, aktuálně např. protokol NV2
MPLS-test	Testovací balíček pro nové verze a opravy týkající se MPLS
Routing-test	Testovací balíček pro nové verze a opravy týkající se routingu

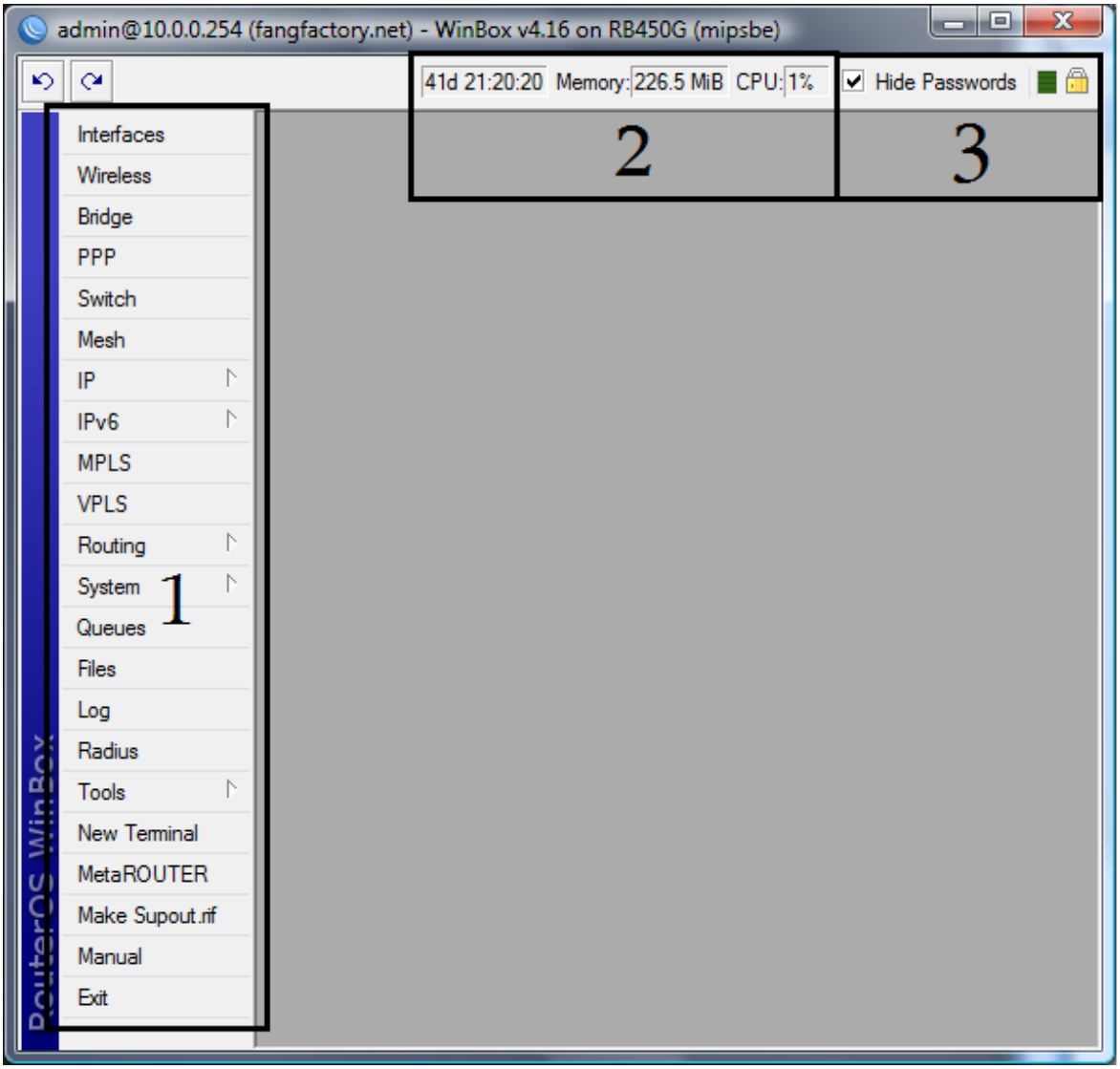
Zdroj: wiki.mikrotik.com, winbox

5.4 Možnosti managementu RouterOS

Hlavním nástrojem pro management Mikrotik RouterOS je od verze 2 Winbox, telnet a sériová konzole RS-232. Od verze 3.0 má RouterOS možnost omezené správy i přes webové rozhraní a plné správy přes SSH. Z podpory je evidentní, že hlavním management nástrojem je Winbox, který funguje pouze pod Windows. S různou úspěšností se podařilo tento nástroj rozchodit i pod Linuxem a MacOS, kde hraje roli použitý emulátor který je v případě Linuxu Wine a v případě MacOS DarWine. Z tohoto důvodu je v systému přítomna terminálová podpora přes Telnet, SSH a sériovou konzolu RS-232.

5.4.1 Management nástroj winbox

Obr. 4 Winbox management tool

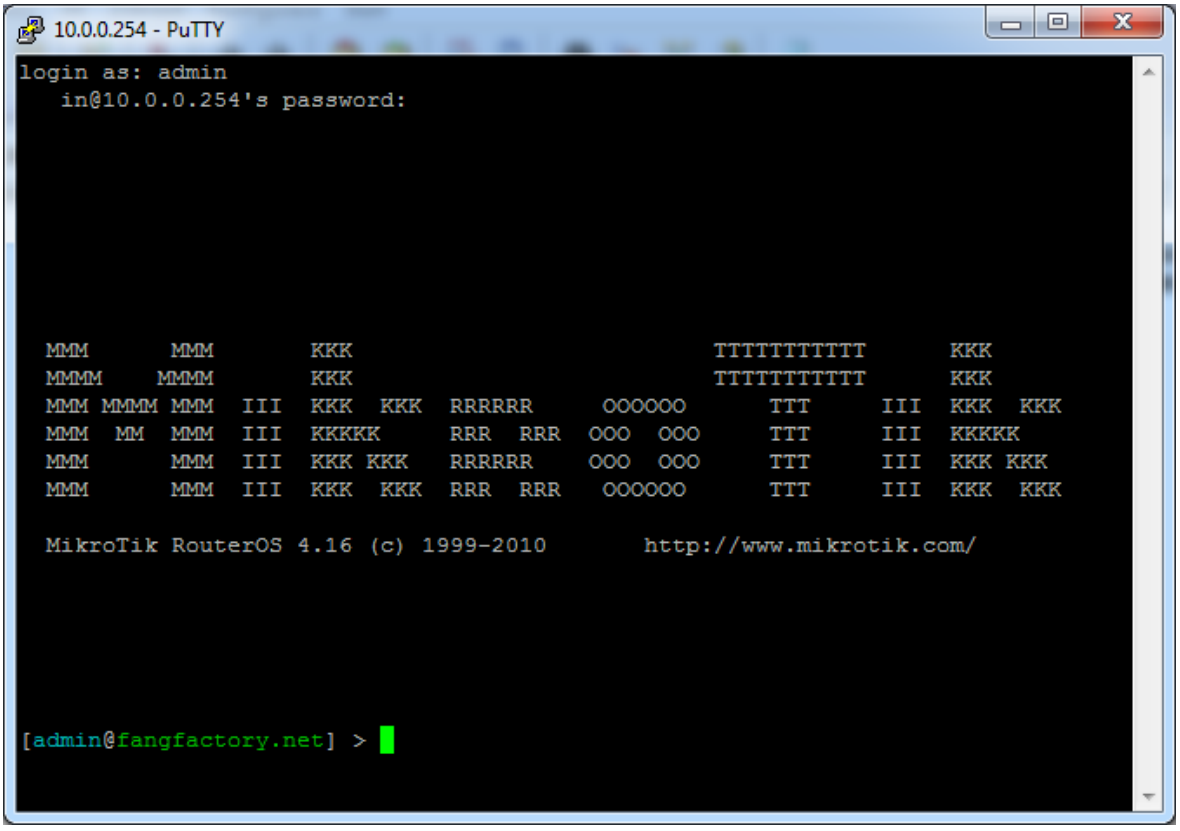


Hlavní okno winboxu se skládá z tří hlavních částí. První z nich představuje nabídku konfigurace routeru. Druhá sekce představuje aktuální stav zatížení CPU, volnou operační paměti RAM a celkovou délku provozu systému od posledního restartu. Třetí sekce indikuje další stavy systému, činnost a zabezpečení management spojení. Velká část položek obsažená v prvním bloku je shodná s počtem nainstalovaným a povolených balíčků. Pak tu jsou položky v menu, které jsou specifické na určitý hardware např. Switch, který dokáže jednotlivé ethernet porty na RB slučovat do hardwarového switche je k dispozici jen na nových RB kde je přítomen switch chip. U starších RB tuto funkcionalitu zastupovala možnost softwarového bridge, která byla pomalejší z důvodu toho, že switching realizoval procesor RB spolu s dalšími úlohami. Za zmínku stojí ještě položka New Terminal, která zpřístupňuje Telnet/SSH/RS-232 konzolu prostřednictvím okna ve winboxu. Hodí se to pro přístup k prvkům, které nejsou ve winboxu k dispozici. Jsou jimi např. možnost upgrade BIOSu RB nebo změna MAC adresy na ethernet portech apod.

5.4.2 Terminálové přístupy do RouterOS

Z předchozí kapitoly je zřejmé, že ovládání nástrojem winbox je poměrně rychlé a komfortní. V některých případech se může stát, že chybou konfigurace si odřízneme tuto možnost a jediná možnost jak se dostat zpět do systému je užití RS-232 sériové konzole nebo přístup přes SSH či telnet rozhraní.

Obr. 5 Konzole RouterOS připojena programem Putty



Práce s konzolou je velmi podobná ovládání ve winboxu. Pro porovnání uvedu přístup k pravidlům NATu ve firewallu přes winbox a terminálovou konzolu. Přistup do pravidel NAT firewallu je následující, IP -> Firewall -> Záložka NAT. V případě terminálu funguje stejná analogie. Po přihlášení stačí zapsat příkaz „ip firewall nat print“. Syntax, příklady a další návody lze nalézt na webové adrese wiki.mikrotik.com nebo na českém fóru www.ispforum.cz

6 Rozšiřující služby na routerech

6.1 VLAN

Virtual LAN je zkratka pro seskupování hostitelů i v případech kdy nejsou všichni zapojeni do stejného switche [6] . Podstata VLAN je označení L2 rámce o IEEE 802.1Q hlavičku která popisuje do které VLAN tento rámec patří. Podle tohoto popisu pak síťové prvky, přes které tento rámec prochází, s ním pak nakládají. Standardní L2 rámec je na Obr. 6 , 802.1Q označený rámec je na Obr. 7.

Obr. 6 Standardní L2 rámec

Délka	7 byte	1 byte	6 byte	6 byte	2 byte	46-1500 byte	4 byte	12 byte
Popis	Preambule	Začátek rámce	Cílová adresa	Zdrojová adres	Délka/Typ ethernet	DATA	Kontrolní s	Pauza mezi rámci

Obr. 7 Standardní s 802.1Q označením

Délka	7 byte	1 byte	6 byte	6 byte	4 byte	2 byte	46-1500 byte	4 byte	12 byte
Popis	Preambule	začátek rámce	Cílová adresa	Zdrojová adresa	802.1Q hlavička	Délka/Typ ethernetu	DATA	kontrolní součet	Pauza mezi rámci

Popis jednotlivých částí rámce:

- Preambule - sled 1 a 0 pro synchronizaci hodin
- Začátek rámce - 10101011 slouží k oznámení začátku rámce
- Cílová adresa - MAC adresa cílového hostitele
- Zdrojová adresa - MAC adresa zdrojového hostitele
- 802.1Q - VLAN označení (tag)
- Délka/Typ ethernetu - Pro ethernet II je zde uveden vyšší typ protokolu a pro IEEE 802.3 je zde délka datového bloku
- DATA - Blok obsahující samotná přenášená data
- Kontrolní součet - Obsahuje cyklický redundantní součet (CRC32), který slouží ke kontrole přenášených dat
- Pauza mezi rámci - Je pomlka mezi vysíláním dalšího rámce

802.1Q hlavička se skládá:

- VLAN protokol ID - Je zpráva která určuje, že 2 další bajty dat obsahují VLAN informace
- Priority Code Point - Obsahuje informace o prioritě rámce (IEEE 802.1p)

- Canonical Format Indicator - Říká v jakém pořadí je rámec přenášen, zda li jde o little endian (kanonický tvar) nebo o big endian. Hodnota je při přijmu znegována, znamená to tedy, že ¬0 je kanonický tvar
- VLAN Identifier - Identifikuje číslo VLAN, celkem 12 bitů znamená celkem 4096 VLAN. Dvě čísla jsou rezervována, k dispozici je tedy 4094 VLAN

Použití VLAN v praxi je celkem častě, ve firemních sítích se takto odděluje provoz např. VoIP telefonie která má díky možnosti VLAN nastavenu vyšší prioritu než ostatní provoz. Dále se takto mohou separovat i pracovníci jednotlivých oddělení. V sítích ISP se takto odděluje management jednotlivých routerů, spojení typu L2 VPN apod. Nevýhodou VLAN je to že přidává další informace, které snižují propustnost zvláště u pomalejšího 10 nebo 100 Mbps ethernetu. S postupem času tento problém pomalu začíná mizet díky nasazování gigabit ethernet sítí umožňující tzv. Jumbo rámce (Jumbo frame), které mohou být velké až 9000 byte. Některé síťové prvky umožňují jít s velikostí rámce ještě výše, ale pouze mezi stejnými prvky od jednoho výrobce. Podpora VLAN v RouterOS je přítomna a řeší se pomocí přidání nového virtuálního interface VLAN a přiřazením na jeden fyzický interface.

6.2 Multicast

V sítích fungujících na TCP/IP protokolu funguje několik typů vysílání. Nejběžnějším je tzv. unicast vysílání, které je určeno pro spojení mezi jednou zdrojovou a jednou cílovou stanicí. Tento typ spojení je nejčastěji využíván ve všech typech sítí. Dále tu je možnost vysílat je pro určitý počet cílových stanic. Anycast funguje tak, že data jsou odeslána k nejbližšímu uzlu, kde jsou replikována a zaslána klientům které je požadují. Opak těchto dvou selektivních vysílání je broadcast a multicast. Broadcast je určen především pro LAN sítě, podstatou brodcast paketu je rozeslání těchto dat všem stanicím, které se nalézají v rámci jednoho síťového segmentu. Pro tento účel slouží poslední adresa daná maskou sítě, např. pro 192.168.0.0/24 je broadcast adresa 192.168.0.255. Tuto vlastnost používají v hojné míře jmenovitě operační systémy Windows od Microsoftu k hledání ostatních stanic Windows na síti. Poslední z těchto technologií je multicast, který funguje stejně jako broadcast, ale s tím že je čistě v režii TCP/IP protokolu. Funguje na principu registrace stanic do skupin, mezi které je pak multicastové vysílání šířeno a to tak že každá stanice má u sebe na interface danou multicast adresu. S výhodou se této vlastnosti využívá při vysílání klasické televize po datových rozvodech (IPTV), kdy jeden vysílač posílá stejná data do více přijímačů. Pokud by pro každý přijímač bylo nutno posílat jako unicast tak by přenosové kapacity mezi vysílačem a přijímačem musely být obrovské zvláště dnes v případě HD videa s datovým tokem i několik desítek megabit. Multicast v tomto případě zařídí, že až k poslednímu routeru či switchi je datový proud pouze jeden. Switch či router pak tyto data replikuje a posílá na porty, u kterých je registrován přijímač (IPTV set-top-box).

Pro účely multicastu je u IPv4 vyhrazen blok adres 224.0.0.0/4 dle RFC5771 [7]. Uvedu jen nejčastěji využíváné bloky:

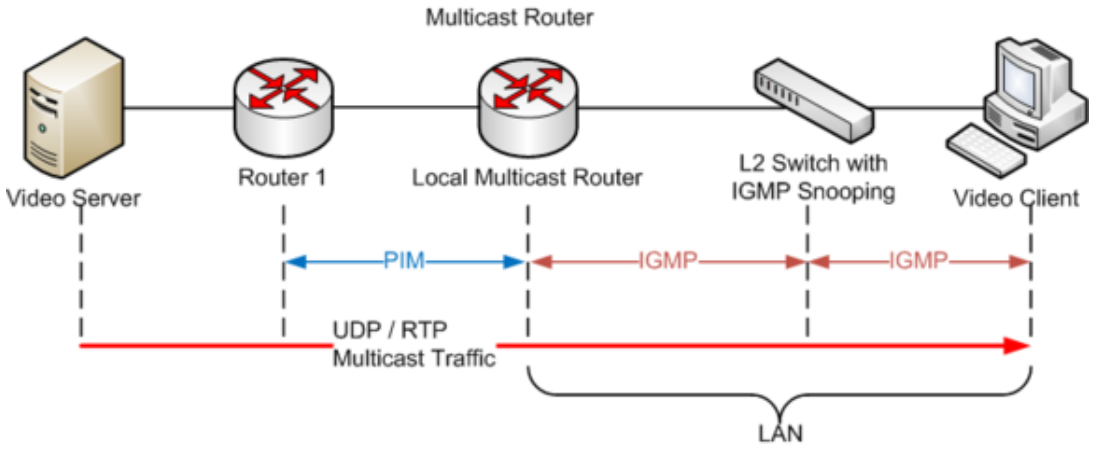
- 224.0.0.0/24 – Blok určený pro multicast v lokálních sítích
- 224.0.1.0/24 – Blok určený pro mezisíťový multicast (internetwork multicast). Lze použít v rámci veřejné sítě internet. Je používán např. pro synchronizaci času (224.0.1.1)
- 224.0.2.0 – 224.0.255.255 – AD-HOC blok číslo 1.
- 224.3.0.0 - 224.4.255.255 – AD-HOC blok číslo 2.
- 233.252.0.0 - 233.255.255.255 – AD-HOC blok číslo 3.
- 224.2.0.0/16 – Blok učený pro Session Annoucement Protocol, protokol určený k oznamování multicastového vysílání.

AD-HOC bloky jsou využívané pro aplikace, které nelze přiřadit do bloků pro lokální nebo mezi síťový multicast.

Multicast u IPv6 protokolu též podporován a je pro tento účel vyhrazen blok adres ff00::/8. Protože dnes je nasazování IPv6 velmi brzděno náklady s tím spojené není nasazování IPv6 multicastu příliš časté. Z tohoto důvodu se jím nebudu zabývat, v případě je možné se podívat do RFC2375 na webu ietf.org .

Podpora ze strany RouterOS je pomocí protocol independent multicast (PIM) ve variantě sparse mode (SM). Výhodou PIM protokolu je, že topologii sítě si staví z informací BGP nebo jiného dynamického routovacího protokolu. Znamená to tedy, že PIM je použit především mezi routery. Sparse mode zajišťuje centrální bod (rendezvous point) odkud je vysíláno k routerům které mají zaregistrovány nějaké klienty. V případě lokálních sítí se používá pro šíření multicast provozu internet group management protocol (IGMP). Je nutné, ale aby případnou podporu IGMP měly i síťová zařízení v lokální síti především tedy switche.

Obr. 8 Schéma použití PIM a IGMP protokolů



Zdroj: *http://www.answers.com/topic/internet-group-management-protocol*

6.3 QoS

Možnosti QoS v RouterOS reprezentuje modul nazvaný Queues (fronty, řady). Umožňuje limitovat rychlosti datových proudů procházejících přes systém s RouterOS definované:

- Rozsahem zdrojových nebo cílových adres, portů, protokolů.
- Priorizaci datových proudů nebo přímo některých paketů
- Umožňuje nastavení tzv. burst (dávek) pro zrychlení chvilkového přenosu
- V závislosti na čase
- Dynamické dělení rychlosti hlavního datového kanálu.

Implementace v RouterOS staví na tzv. Hierarchical Token Bucket (HTB), které umožňuje definovat strukturu a vztahy mezi jednotlivými frontami. Jednotlivé HTB struktury lze v RouterOS přiřadit do čtyř skupin:

- Celkový vstup (global-in) -Reprezentuje sumu veškerého vstupního provozu
- Celkový výstup (global-out) - Reprezentuje sumu veškerého výstupního provozu
- Celek (global-total) - Reprezentuje sumu vstupu a výstupu provozu
- Název sítového rozhraní (interface) - Reprezentuje síťové rozhraní přes které bude procházející provoz zařazen do HTB.

V RouterOS jsou 2 možnosti jak definovat fronty:

- Jednoduché fronty (simple queues) - Vhodné pro nasazení do velmi malých sítí např. malé firmy nebo domácí uživatelé. Limituje provoz jednotlivých klientů a provoz typu P2P.
- Stromové fronty (queue tree) - Pro nasazení do velkých sítí se složitou hierarchií řízení provozu. Umožňuje limitaci na základě označování paketů příznaky ve firewallu v záložce mangle.

6.3.1 Simple Queues

Jak již bylo zmíněno v předchozí části, SQ není vhodné pro nasazení ve velkých sítích. Jeho hlavní nevýhodou je to, že každý paket prochází každým pravidlem v SQ dokud nenarazí na odpovídající kritéria. Z toho plyne, že velký počet SQ může značně zpožďovat průchozí pakety i o stovky milisekund. Hlavní výhodou SQ je jednoduchá konfigurace a rychlá funkčnost.

6.3.2 Queue Tree

Výhodou oproti SQ je naprostá kontrola nad veškerým provozem. Nevýhodou oproti SQ je vyšší náročnost na výkon hardware při malých počtech pravidel. To je dáno především tím, že každý paket se označuje ve firewallu příznakem. Je nutné označovat oba směry a to příchozí i odchozí.

6.3.3 Hierarchial Token Bucket

Umožňuje budování hierarchií typu parent-child a child-child. Jakmile má jedna fronta jeden child stává se z ní inner queue, všechny fronty bez child jsou označeny jako Leaf. Inner queue jsou odpovědné za distribuci provozu, zatímco všechny leaf jsou samotní konzumenti provozu. V RouterOS je nutné označit relaci parent pro přiřazení dítětem (child) k frontě. [8]

V RouterOS lze HTB limitovat 2 způsoby:

- CIR (commited information rate) – (limit-at) datový tok dostane tolik, kolik specifikuje nastavená hodnota. Jinými slovy, každá queue dostane tolik kolik má nastaveno
- MIR (maximal information rate) – (max-limit) datový tak dostane kolik je nastaveno, pokud je zde parent queue která má volnou kapacitu.

Jde vlastně o agregaci, kdy se u parentů nastaví maximální přípustný provoz a u child queues se přiřazují rychlosti jednotlivým uživatelům v agregační skupině.

6.3.4 Značkování paketů pro Queue Tree

V RouterOS k tomuto účelu slouží část firewallu nazvaná Mangle. Je to funkce, která je platná pouze v rámci jednoho systému s nainstalovaným RouterOS. Znamená to, že tyto značky nejsou posílány dále po síti. Ve chvíli, kdy paket dojde k pravidlu, které mu odpovídá s ním lze provést tyto akce:

- accept - Přijme paket, který dále nepokračuje k dalším pravidlům
- add-dst-to-address-list - přidá cílovou adresu do specifikovaného seznamu (lze nastavit timeout)
- add-src-to-address-list - přidá zdrojovou adresu do specifikovaného seznamu (lze nastavit timeout)
- change-dscp - změní differentiated services code point (DSCP, náhrada za ToS)
- change-ttl - změní hodnotu time to live
- jump - odskočí na definované pravidlo ve firewallu (číslo)
- log - Přidá výpis do systémového logu
- mark-connetion - označí danou konexi definovaným příznakem
- mark-packet - označí daný paket definovaným příznakem
- mark-routing - označí daný paket definovaným příznakem, vhodné pro pravidla routingu (policy routing)

- passtrough - na paketu neprovede žádnou akci a paket pošle k dalšímu pravidlu, vhodné pro statistické účely
- return - vrátí paket na pravidlo odkud odskočilo (jump).
- set-priority - nastaví prioritu pokud data prochází přes síťové rozhraní podporující priority (VLAN u Ethernetu nebo WMM u WiFi)
- strip-ipv4-options - odebere z hlavičky IPv4 protokolu přidané option (možnosti)

Pro účely značkování se používají především mark-connection, mark-packet pro provoz od koncových klientů. V RouterOS je ještě jedna možnost jak označovat datové proudy a to přímo protokoly na sedmé vrstvě (L7). Pro tyto účely je nutné ve firewallu v záložce layer 7 protocols mít vyplněnou alespoň jednu položku obsahující název protokolu a tzv. regexp. Regexp definuje řetězec, který je společný pro každý paket. V podstatě se jedná o vzor každého paketu. Seznam možných vzorů pro jednotlivé protokoly lze získat na adrese http://l7-filter.sourceforge.net. Použití této metody je hodně výpočetně náročné z důvodu hloubkové inspekce datové části (payload) paketů a % úspěšnosti detekce se liší dle použitého protokolu. V případě manglování s detekcí L7 protokolů se u pravidel v záložce advanced vybere předdefinovaný vzor a dle něj se pak detekce řídí.

6.4 Dynamické routování

Nejdříve je vhodné popsat, jak je routování organizováno. V rámci internetu existují tisíce sítí, které svou funkčností představují celky tzv. autonomní systémy (AS - Autonomous System). AS jsou unikátní číselná označení těchto nejmenších bloků, přidělují se na žádost organizace Internet Assigned Numbers Authority (IANA). Do nedávna před přechodem IPv6 bylo toto číslo maximálně 16 bitové, to představovalo celkem 65536 AS. Odečtením vyhrazených bloku je toto číslo ještě nižší, použitelných pro veřejný internet jsou AS 1–54271. S příchodem IPv6 je rozsah rozšířen až na 32 bitů, čemuž se rovná cca 4 miliardám možných AS. V praxi AS reprezentují jednotlivé sítě poskytovatelů internetu (ISP) nebo dalších organizací, které tvoří internetovou síť, jako jsou např. internet exchange uzly apod.

V základu se dynamické routovácí protokoly dělí na dvě hlavní skupiny:

- IGP (Interior Gateway Protocol) - Protokoly pro routing uvnitř AS
- EGP (Exterior Gateway Protocol) - Protokoly pro routing mezi jednotlivými AS

IGP se dále dělí na protokoly řízené stavem linek (link-state) a řízené vektorovou vzdáleností (distance-vector). Rozdíl mezi těmito skupinami je naplňování routovací tabulky hodnotami. V případě distance-vector protokolů router nemá informace o kompletní topologii sítě a svou tabulku si konstruuje tak, že přijímá a vysílá na ostatní routery své síťové vzdálenosti k jiným routerům. U těchto protokolů dochází při komunikaci k přenosu kompletní routovací tabulky.

U link-state routovacích protokolů si každý router staví svou routovací tabulku ze známosti topologie. Z té si kalkuluje nejlepší cestu k dalším cílům v síti. Komunikace mezi těmito routery probíhá tak, že si předávají pouze informace o stavech jednotlivých linek v síti.

Mezi IGP distance-vector protokoly se řadí:

- Routing Information Protocol (RIP) - dnes již velmi zastaralý, téměř nepoužívaný
- Interior Gateway Routing Protocol (IGRP) - proprietální vyvinutý firmou Cisco jako reakce na omezení RIP, dnes je považován za již překonaný
- Enhanced Interior Gateway Routing Protocol (EIGRP) - Vylepšená verze předchozího IGRP, též vyvinutí firmou Cisco

Mezi IGP link-state protokoly se řadí:

- Open Shortest Path First (OSPF) - nejčastěji využívaný
- Intermediate system to intermediate system (IS-IS)

Mezi EGP distance-vector protokoly se řadí:

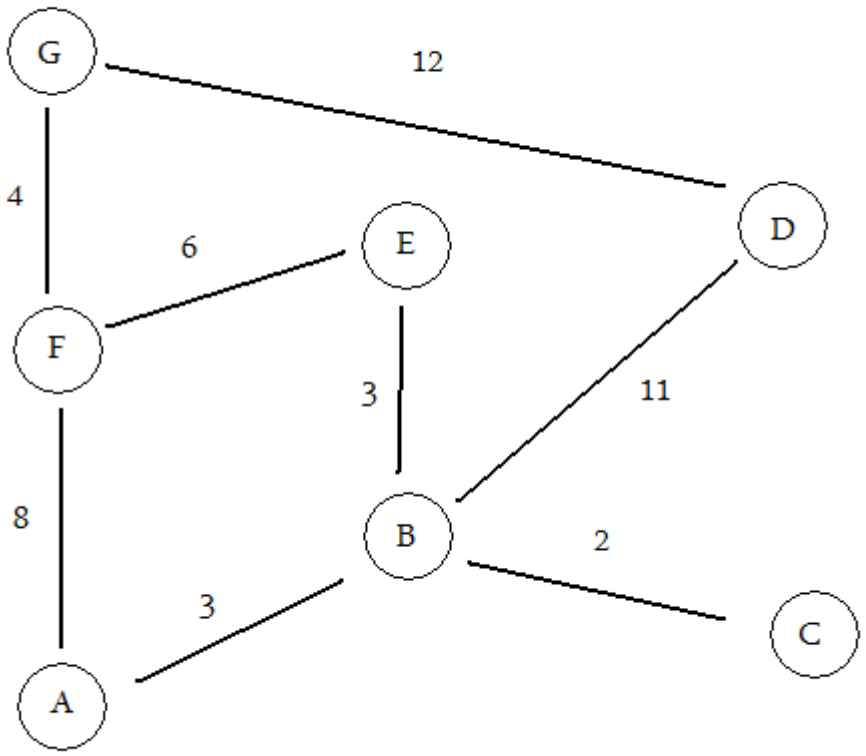
- Border Gateway Protocol (BGP) - nejvyužívanější

V dnešní realitě internetové sítě jsou nejpoužívanější Border Gateway Protocol pro routing mezi jednotlivými AS. Jeho nasazení je tedy určeno na hraničních routerech sítí ISP a v internet exchange uzlech. Pro routing uvnitř AS se dnes nejvíce používá Open Shortest Path First (OSPF), který nachází uplatnění v menších sítích. U velkých sítí (high-performance), kde již OSPF nestačí, se používá specifická kombinace routingu nazvaná Multi Protocol Layer Switching (MPLS) kterým se budu zabývat v samostatné kapitole.

6.4.1 Open Shortest Path First (OSPF)

Jak již bylo řečeno, OSPF patří do skupiny link-state IGP dynamických routovacích protokolů. Jednotlivé routery si staví routovací tabulku na základě stavů linek v celé síti. To se děje pomocí Dijkstrova algoritmu který staví z informací přímo připojených routerů síť s ohodnocenými spojeními tzv. váhou (cost), která udává váhu propojení v rámci sítě. Na obr. X je uveden ohodnocený graf, písmena A-G označují routery a čísla u propojení jsou costy. Pokud se chceme dostat z routeru B do routeru G, jsou zde k dispozici 3 cesty, prostým sečtením costů dostáváme váhu celé trasy. První cesta přes router D má váhu 23. Druhá cesta přes router E a F má váhu 13 a třetí cesta přes routery A a F má váhu 15. Rozhodnutí, skrze kterou cestu se data vydají je dána nejnižší vahou celé trasy a cílovou adresou v každém paketu. V našem případě je to cesta přes router E a F s váhou 13.

Obr. 9 Ohodnocená síť vahami

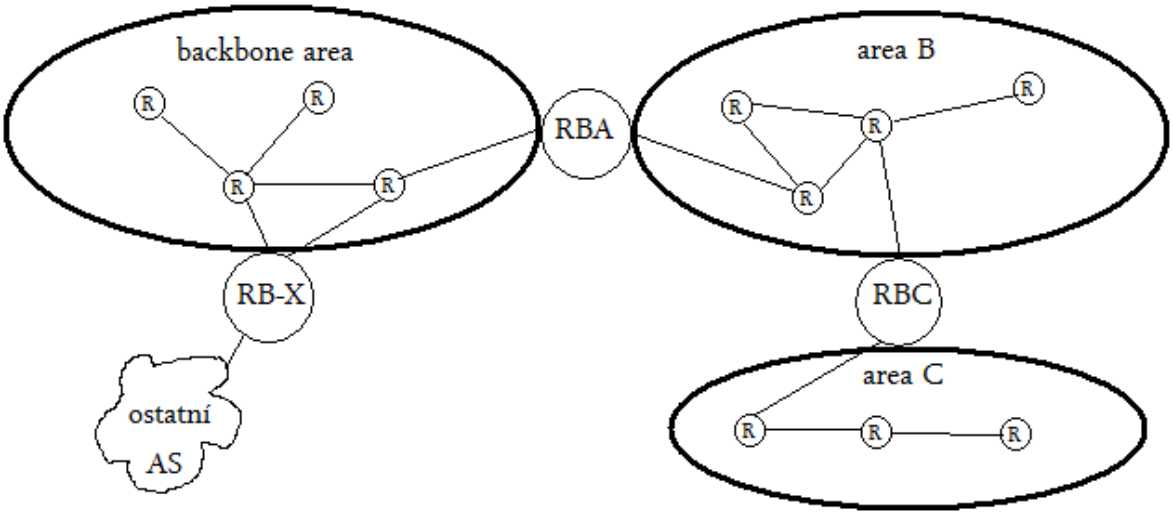


V případě dvou a více cest se shodnými costy je nutné určit která cesta má přednost, často se to řeší tak, že se jedné cestě zvedne cost o jednu nebo se pomocí podrobných pravidel určí, kudy mají data téct, lze např. nastavit pro každý směr jinou trasu. Nastavení odpovídajících costů v síti je alfou a omegou správné funkce celé sítě. Jak pomůcku při kalkulaci se používají např. reálné vzdálenosti v Km nebo propustnost jednotlivých linek v

megabitech apod. Je nutné, aby postup kalkulace costů v celé sítí (v rámci AS) byl pokud možno stejný.

Z důvodu administrativních a také výkonových (velikost routovacích tabulek) se sítě postavené na OSPF mohou dělit na menší celky nazvané Area (oblast). V každé instalaci OSPF musí být přítomna area backbone, která tvoří jádro celé sítě. Ostatní oblasti lze pak libovolně pojmenovat. Z důvodů správné funkce OSPF je nutné aby každá oblast měla přímé spojení s oblastí backbone. V reálném nasazení není vždy možné mít fyzické propojení s hlavní oblastí proto OSPF podporuje tzv. virtual links. Virtual links jsou už dle názvu virtuální propojení určené pro případy kdy, není technicky možné mít přímé spojení do backbone area. Lze tímto realizovat např. scénář na obr. 10, kde area C není přímo spojena s backbone.

Obr. 10 Příkladová síť OSPF s oblastmi



Další prvek, který je OSPF nutné rozlišovat jsou jednotlivé typy routerů v OSPF síti. OSPF routery se označují číselně podobně jako IPv4 adresa např. 0.0.0.0 nebo 0.0.1.2 nemají, ale s IPv4 adresným rozsahem vůbec nic společného. Na obr. 10 jsou vidět routery, které spojují jednotlivé oblasti a také routery, které spojují celý autonomní systém s jiným. Routery realizující spojení mezi oblastmi se nazývají Area Border Router - ABR (RBA a RBC). Jejich význam je snižovat počet rout distribuovaných do jednotlivých oblastí. Výsledkem toho je, že routery v backbone area nemusí znát všechny routy z ostatních oblastí a obráceně. Připojování celé OSPF sítě k jiným realizuje tzv. Autonomous System Border Router - ASBR (RB-X), který dělá velmi podobnou práci jako ABR, ale pro celou OSPF síť. Znamená to tedy, že tyto hraniční routery slouží k především celkové redukci počtu distribuovaných rout dále do sítě, čímž se snižují nároky na paměť a rychlost procesoru routerů. Je celkem časté souběžně provozovat na ASBR routeru kromě zakončení OSPF routingu také BGP, které funguje pro distribuci routovacích informací dále do internetové sítě.

Komunikace mezi jednotlivými OSPF routery probíhá pomocí multicast vysílání. Pro tento účel má OSPF rezervované multicast adresy 224.0.0.5 a 224.0.0.6 pro IPv4 a FF02::5, FF02::6 pro IPv6, používaných u síťových rozhraní disponující broadcastem jako např. Ethernet. Informace z těchto adres se nesmí routovat mimo dotčené síťové rozhraní. V nasazeních, kde se používají non-broadcast síťová média je nutné ručně nastavit protější routery. Takové případy jsou např. VPN propojení nebo point to point spoje s maskou /31. Komunikace a detekce u broadcast sítích probíhá periodickým posíláním tzv. hello paketů, které zjišťují funkčnost síťového propojení a zjišťují okolní OSPF routery. Samotná výměna informací vzdálenějších OSPF routerů funguje pomocí aktualizací o stavech linek (link state update). Autentizace mezi routery je možná pomocí MD5 hashe předsdíleného klíče u IPv4 varianty. OSPFv3 má pro autentizaci použité IPsec.

Podpora OSPF v RouterOS je plná pro IPv4 (OSPFv2) tak i IPv6 (OSPFv3) od verze 4.0 výše.

6.4.2 Border Gateway Protocol (BGP)

S růstem internetové sítě se začalo projevovat nedostatky tehdejšího síťového uspořádání sítě na třídy A, B, C a nedostatků routovacího protokolu RIP a EGP. Hlavním přínosem BGPv4 bylo zavedení tzv. Classless Inter-Domain Routing, které v praxi zavádí masku jako hlavní prvek při definici velikosti sítě. Další zavedenou novinkou bylo zavedení tzv. route aggregation umožňující na základě CIDR definic zmenšovaní počtu položek (rout) v routovací tabulce.

Router pro komunikaci s ostatními využívá port 179/TCP a konečný automat s celkem 6 stavy:

- v klidu (idle)
- připojeno (connect)
- aktivní (active)
- otevřeno pro odeslání (opensent)
- otevřeno pro potvrzení (openconfirm)
- spojeno (established)

Tabulka 2 - Classless Inter-Domain adresace

IP/CIDR	Poslední adresa	Maska Podsítě	počet adres k dispozici (všech)	Použitelných adres pro síť
0.0.0.0/32	0.0.0.0	255.255.255.255	1	0
0.0.0.0/31	0.0.0.1	255.255.255.254	2	0
0.0.0.0/30	0.0.0.3	255.255.255.252	4	2
0.0.0.0/29	0.0.0.7	255.255.255.248	8	6
0.0.0.0/28	0.0.0.15	255.255.255.240	16	14
0.0.0.0/27	0.0.0.31	255.255.255.224	32	30
0.0.0.0/26	0.0.0.63	255.255.255.192	64	62
0.0.0.0/25	0.0.0.127	255.255.255.128	128	126
0.0.0.0/24	0.0.0.255	255.255.255.0	256	254
0.0.0.0/23	0.0.1.255	255.255.254.0	512	510
0.0.0.0/22	0.0.3.255	255.255.252.0	1 024	1 022
0.0.0.0/21	0.0.7.255	255.255.248.0	2 048	2 046
0.0.0.0/20	0.0.15.255	255.255.240.0	4 096	4 094
0.0.0.0/19	0.0.31.255	255.255.224.0	8 192	8 190
0.0.0.0/18	0.0.63.255	255.255.192.0	16 384	16 382
0.0.0.0/17	0.0.127.255	255.255.128.0	32 768	32 766
0.0.0.0/16	0.0.255.255	255.255.0.0	65 536	65 534
0.0.0.0/15	0.1.255.255	255.254.0.0	131 072	131 070
0.0.0.0/14	0.3.255.255	255.252.0.0	262 144	262 142
0.0.0.0/13	0.7.255.255	255.248.0.0	524 288	524 286
0.0.0.0/12	0.15.255.255	255.240.0.0	1 048 576	1 048 574
0.0.0.0/11	0.31.255.255	255.224.0.0	2 097 152	2 097 150
0.0.0.0/10	0.63.255.255	255.192.0.0	4 194 304	4 194 302
0.0.0.0/9	0.127.255.255	255.128.0.0	8 388 608	8 388 606
0.0.0.0/8	0.255.255.255	255.0.0.0	16 777 216	16 777 214
0.0.0.0/7	1.255.255.255	254.0.0.0	33 554 432	33 554 430
0.0.0.0/6	3.255.255.255	252.0.0.0	67 108 864	67 108 862
0.0.0.0/5	7.255.255.255	248.0.0.0	134 217 728	134 217 726
0.0.0.0/4	15.255.255.255	240.0.0.0	268 435 456	268 435 454
0.0.0.0/3	31.255.255.255	224.0.0.0	536 870 912	536 870 910
0.0.0.0/2	63.255.255.255	192.0.0.0	1 073 741 824	1 073 741 822
0.0.0.0/1	127.255.255.255	128.0.0.0	2 147 483 648	2 147 483 646
0.0.0.0/0	255.255.255.255	0.0.0.0	4 294 967 296	4 294 967 294

Z tabulky je viditelné, že /32 a /31 nelze použít pro celou síť ale pro jednoho nebo dva konkrétní hostitele. Síť /30 se nejčastěji používá u propojení typu point-to-point. Typické nasazení rozsahů /29 až /26 je jako bloky adres pro klienty velkých ISP. Bloky, které jsou větší, buď zahrnují enterprise klienty velkých ISP nebo slouží jako adresní bloky pro malá data centra. Blok adres /8 je přidělován organizací ICANN lokální registrátorům jako je evropské RIPE, které tyto bloky dále dělí na menší a poskytuje žadatelům, jimiž jsou ISP.

Každý BGPv4 router má informační základnu rout složenou z několika informačních bází:

- Adjacent Routing Information Base incomming (Adj-RIB-in) - je báze složená z rout přijatých od jiných BGP routerů
- Local Routing Information Base (Loc-RIB) - Hlavní báze určená pro přímé vkládání rout do routovací tabulky routeru
- Adjacent Routing Information Base outgoing (Adj-RIB-out) - je báze složená pro odeslání k dalším BGP routerům v síti.

Struktura těchto tří tabulek není viditelná pro ostatní routery. Předávání informací z Adj-RIB-in do Loc-RIB závisí na konkrétních nastavených pravidlech a konkrétní softwarové implementaci BGP. Z Loc-RIB informací se posílají routy do routovací tabulky která má hlavní význam při rozhodování cesty každého paketu. Informační báze Adj-RIB-out je složena z Loc-RIB báze a z informací získaných z lokální routovací tabulky jako jsou přímo připojené sítě. Update tabulky ostatní BGP routery dostávají pomocí tzv. Network Layer Reachability Information (NLRI) aktualizace, která obsahuje informace z Adj-RIB-out.

Router pro komunikaci s ostatními využívá port 179/TCP a konečný automat s celkem 6 stavy:

- v klidu (idle)
- připojeno (connect)
- aktivní (active)
- otevřeno pro odeslání (opensent)
- otevřeno pro potvrzení (openconfirm)
- spojeno (established)

Při klidovém stavu router uzavře příchozí port 179/TCP a inicializuje všechny systémové zdroje. Dále se pokusí připojit na všechny routery definované v peers na portu 179/TCP a otevře svůj port 179/TCP. Pokud všechno proběhne v pořádku tak router přechází do stavu připojeno, jinak se router vrací do stavu klid. Stav připojeno pokračuje vyjednáním TCP spojení a zašle všem ostatním routerům, že přechází do stavu otevřeno pro odeslání. Pokud dojde k chybě tak i přes to přechází do stavu aktivní. V aktivním stavu pokud dojde k chybě vyjednávání TCP spojení tak router spojení zkusí vyjednat znovu, pokud ani poté neuspěje, vrací se do stavu v klidu. Stav otevřeno pro odesílání router odešle ostatním zprávu o tom, že se nachází v tomto stavu. Pokud routeru přijde od ostatních routerů stejná zpráva, přejde do stavu otevřeno pro potvrzení. Stav otevřeno pro potvrzení je stav, při kterém router může přijímat tzv. keepalive pakety od ostatních routerů. Pokud přijme tento paket v definovaném časovém intervalu, přejde do stavu spojeno, pokud dříve tento časovač vyprší, přejde do klidového stavu. Stav spojeno znamená, že router správně navázal všechna spojení a může začít výměna routingových informací. Pokud v tomto stavu dojde k chybě je danému routeru odeslána zpráva o chybné

informaci a router přechází do klidového stavu. To samé platí pro keepalive zprávy, pokud tedy v stavu spojeno dojde k vypršení časovače, router se pak vrátí do klidového stavu.

Nevýhodou BGP oproti OSPF je nutnost nastavit do každého BGP routeru adresy všech ostatních routerů v rámci AS. Routery tímto tvoří tzv. mesh sít. V podmínkách dnešních velkých sítí by to byl nadlidský úkol si udržet přehled. Proto v rámci BGP protokolu jsou možnosti jak tento problém obejít. Existují dvě techniky, Route Reflection (RR) a BGP confederation. Route reflection (zrcadlení rout) je komponenta sítě sloužící jako proxy server pro spojení mezi jednotlivými routery. Komunikace probíhá výhradně přes tento bod, na BGP routerech stačí komunikační kanál nastavit na tento proxy server.

Druhou popisovanou komponentou je BGP confederation (spolek), slouží k rozdělení jednoho AS na několik logicky menších. Zmenšuje se velikost celé mesh sítě a tím se redukuje počet routerů, které musí být v rámci mesh sítě přímo spojeni. Tyto techniky nemají žádný dopad na propagaci AS oproti ostatním AS.

Nevýhodou těchto technik může být zvýšená doba reakce při změnách v sítí, která může znamenat několikaminutovou nedostupnost některých cílů v síti. I přes tyto nevýhody je dnes BGP hlavním prostředkem, který udržuje internetovou síť při životě. BGP je dnes jediný protokol, který je schopný obsluhy sítě velikosti internetu, další výhody jsou především v dostupnosti hardwarově akcelerovaných prvků a možností škálovatelnosti.

Podpora BGP v RouterOS je pro IPv4 tak i pro IPv6 včetně podpory route reflection a confederation.

6.5 MPLS

Odklon od spojovaných sítí (circiut switched network) k čistě routovaným sítím ukázal slabiny takto konstruovaných sítí. Náročnost klasického routování se odvíjí od počtu průchozích paketů za jednu vteřinu. Ve velkých sítích se postupem času ukázalo, že routery mají s velkým počtem paketů za vteřinu problém. Důvodem delšího odbavení byla nutnost prohlížet celou IP hlavičku každého paketu. Tento stav způsoboval prodlužování doby, kdy paket čeká na odbavení v paměti routeru. Z pohledu běžného uživatele to znamenalo prodlužování odezvy. Do jisté hranice lze tento stav tlumit výkonnějším hardwarem nebo load balancováním mezi několik routerů. Tyto důvody vedly firmu Ipsilon Networks k zavedení tzv. IP Switching fungujících podobně jako v minulosti využívané spojované sítě. Nevýhodou této implementace byla funkčnost pouze na ATM síti. Tento hendikep způsobil úpadek a v roce 1998 odkoupení Ipsilon Networks firmou Nokia. Idea přepínání paketů přetrvala. Chopila se jí firma Cisco, která upravila funkčnost tak aby přepínání paketů fungovalo na jiných topologiích než jen na ATM. Výsledkem práce Cisca bylo tzv. Tag switching, které bylo přejmenováno na Label Switching a předáno jako návrh IETF. Výsledkem připomínkového řízení od ostatních výrobců síťového hardware byl vznik MultiProtocol Label Switching techniky.

Hlavní důvody nasazování MPLS do velkých sítí jsou především možnost jak přepínání paketů, tak navazování spojovaných okruhů. To umožňuje naprostou nezávislost na layer 2 síti a tedy možnost nativního přenosu ATM, SONET a Ethernetových rámců. Pokud bychom měli MPLS zařadit do kategorií EGP či IGP tak se řadí do IGP protokolů. V rámci OSI modelu je MPLS chápáno jako mezistupeň mezi druhou a třetí vrstvou. Někdy proto bývá označována jako 2,5 vrstva v OSI modelu.

6.6 Princip funkčnosti

Z pohledu síťového uspořádání, je MPLS zařízení možné brát jako skupinu 2 speciálních switchů. Body na kterých dochází k zapouzdření (encapsulation) či odpouzdření (decapsulation) se v MPLS sítí nazývají label edge routers (LER). Zařízení starající se o další zpracování paketů v rámci MPLS sítě se nazývají label switch routers (LSR). LER a LSR si mezi sebou předávají informace o daných popisovačích (labels) pomocí label distribution protocol (LDP) a informace o dostupnosti jednotlivých MPLS bodů v síti. Tím si každý MPLS router staví obraz o celé MPLS síti. Pro distribuci těchto informací je nutné mít funkční IP komunikaci mezi LER a LSR - hojně se pro tento účel používá OSPF nebo BGP na neveřejných IP rozsazích.

Dalo by se to přirovnat např. k OSPF, které si obraz sítě staví z funkčnosti linek. Ve chvíli požadavku na spojení prostřednictvím MPLS sítě se vytvoří mezi LER tzv. label switch path (LSP). Tento „tunel“ umožňuje přenos libovolných dat nezávisle na přenosové síti. Toho se s výhodou používá např. při stálých VPN spojeních nebo pronájmu propojení z bodu do bodu. MPLS síť lze tedy chápat jako množinu přepínačů typu LER a LSR. Mezi jednotlivými LER se vytvářejí virtuální propojení prostřednictvím LSR. Další výhodou je, že MPLS sít nepotřebuje ke svému fungování veřejné adresy v rámci internetu. Platí to pro LSR, u LER je nutné mít alespoň jednu adresu přítomnu.

6.7 Hlavička MPLS

Obsahuje celkem 4 položky, které se souhrnně nazývají label stack (popisová halda či blok). Obsahuje následující položky:

- číslo popisovače (label value) - s délkou 20 bitů
- třída provozu - lze chápat jako nastavení QoS priority a značku ECN (Explicit Congestion Notification), která umožňuje informovat koncové LER o přetížení uzlů bez zahazování paketů. Délka jsou 3 bity
- konec popisové haldy (bottom of stack) - Pokud je tato informace nastavena na logickou 1 pak routeru oznamuje, že již další popisovače nejsou přítomny. Délka je 1 bit
- životnost (time to live) - životnost daného paketu, při průchodu LSR se hodnota zmenší o 1 nebo o jinou definovanou hodnotu. Pokud je hodnota nulová, paket se zahodí. Funkčnost je stejná jako u IP protokolu, který tuto informaci také obsahuje.

6.8 Podpora v RouterOS

MPLS bylo do RouterOS implementováno od verze 3.4. Dokončená implementace by měla být ve všech verzích 4.X. Některé funkce nejsou dosud implementovány jako je podpora BGP pro LDP a stavba MPLS sítě čistě na IPv6.

7 Problematika přechodu na IPv6

Obecně lze říci, že postupem času začíná být otázka IPv6 čím dále tím více palčivá jak pro poskytovatele obsahu, tak pro domácí uživatele. Hlavním důvodem vývoje nového protokolu bylo především vyřešit problém nedostatku síťových adres. V průběhu vývoje se kromě tohoto cíle začalo uvažovat i dalších změnách ohledně fungování a uspořádání sítě, které by lépe vyhovovalo modernímu využívání.

První významnější rozdíl oproti IPv4 je formát adres. IPv4 je adresa složena s 4 bloku číselných hodnot od 0 do 255 oddělených čtyřmi tečkami např. 156.145.2.3. V případě IPv6 je adresa složena s osmi bloků složených z hexadecimálních hodnot např. 2002:0da8:face:0000:0000:0000:1528:5756. Z běžného pohledu je jasné, že zapamatovatelnost takovýchto adres bude velice složitá. Tím dále roste významnost DNS. Další věcí je možnost zkracování adres, bloky s 0000 lze nahradit takto 2002:0da8:face:0:0:0:1528:5756. Takto zkrácenou adresu lze dále zkracovat a to tak, že prvky s nulou lze nahradit dvěma dvojtečkami např. 2002:0da8:face::1528:5756. Jediným omezením je možnost pouze jedné dvojice dvojteček. Dalším rozdílem mezi IPv4 a IPv6 je přidělování adres. U IPv4 se o přidělování adres staral DHCP server, kdežto u IPv6 je nově zavedena tzv. bezstavová konfigurace fungující v routovaných sítích. Přidělování adres je čistě automatická záležitost, která se realizuje pomocí ICMPv6 datagramu poslaným multicastem, který plně nahrazuje broadcast. Router, který zachytí tuto zprávu, pošle datagram obsahující nastavení sítě. Nevýhodou tohoto řešení je, že se nedistribuuje nastavení DNS, čímž je prakticky toto řešení nepoužitelné pro podmínky domácích a firemních sítí. Proto v pozdějších fázích vývoje bylo definováno DHCPv6. Je dobré zmínit, že zatím není příliš mnoho funkčních implementací v domácích routerech. Výhodou DHCPv6 oproti bezstavové konfiguraci je, že v informačním paketu obsahuje i informace o použitelném prefixu v síti klienta. Tato funkčnost velmi usnadňuje přidělování adres v lokální síti klienta.

7.1 Podpora a možnosti IPv6 v systému RouterOS

Systém RouterOS ve verzi 4.16 umožňuje přidělování adres pomocí bezstavové konfigurace. Implementace DHCPv6, IPSECv6, PPPv6 je plánována v nadcházející verzi 5. V době psaní této práce byla verze 5 ve stavu release candidate 11 (RC11). Dále umožňuje statické routování, firewall s možností filtrování, manglování a connection tracking jako u IPv4. Dynamické routování zajišťuje BGP+, OSPFv3 a RIPng. O shaping se stará stejná komponenta (queues) jako v případě IPv4. Podpora MPLS a multicast routingu zatím není implementována.

7.2 Možnosti klientských systémů

7.2.1 Systém Windows [9]

První pokusy o implementaci IPv6 započal Microsoft již v roce 1998, kdy poprvé zkoušel první implementace IPv6 ještě na Windows 95 a Windows 98. Další pokusy Microsoft učinil v krátce po vydání Windows 2000, kdy uvolnil balík nazvaný "Technology preview", který měl poskytnout první vodítka pro vývojáře aplikací. Tento balík nikdy nebyl určen pro nasazení do produkčního prostředí, některé zdroje uvádějí chybně Windows 2000 jako IPv6 ready systém. Dle mého názoru to může být z části pravda, ale spíše se přikláním k názoru, že Windows 2000 nejsou systém připravený pro provoz v IPv6 only sítích.

V době vydání přelomových Windows XP v roce 2001 systém měl podporu na úrovni developer preview jako u Windows 2000. Tato situace se změnila s příchodem prvního Service Packu v prosinci 2002. Microsoft zahrnul kompletně přepracovaný TCP/IP v6 kód, který standardně nebyl nainstalován, ale musel se ručně u síťového adaptéru nainstalovat. Konfigurovat jej šlo pouze přes příkazový řádek pomocí nástroje "netsh". Další nevýhodou byla absence funkčnosti základních služeb jako je DNS nebo Sdílení souborů a tiskáren v sítích Microsoft. V červenci roku 2003 Microsoft uvolnil "Advanced networking pack for Windows XP", který přidal možnost filtrování IPv6 paketů pomocí integrovaného firewallu. Dále umožňoval tunelování IPv6 provozu přes IPv4 síť pomocí 6to4, ISATAP. Teredo tunel umožňoval připojení nativní IPv6 konektivity prostřednictvím tunelového serveru a to i při NATovaném spojení. V srpnu roku 2004 Microsoft uvolnil druhý Service Pack pro Windows XP, který obsahoval kompletní networking pack uvolněný dříve jako volitelná součást. Tím Microsoft dokončil integraci IPv6 do svého klientského systému. Další systémy jako Windows Vista a Windows 7 měly podporu IPv6 již při prvním vydání na trh s dalšími vylepšeními jako byla grafická konfigurace.

Stejná situace panovala v případě Windows Serveru. Podpora IPv6 byla plně přidána u Windows serveru 2003 v podobě integrovaného Advanced networking packu už při prvním vydání. Kompletní zahrnutí IPv6 do systému bylo prakticky totožné jako u Windows XP v době vydání Service Packu 2. U Windows serveru 2008 a 2008 R2 byl IPv6 protokol plně přítomen jíž při prvním uvedení včetně možnosti grafické konfigurace.

7.2.2 Systém Linux

Experimentálně se IPv6 objevilo již v linuxovém kernelu verze 2.1.8 v roce 1998. Do běžného nasazení se mohl linux představit až v roce 2005 ve verzi kernelu 2.6.12. V průběhu vývoje IPv6 kódu vzniklo za tímto účelem několik projektů, které si vzali za cíl implementaci IPv6 do linuxového kernelu. Těmito projekty jsou KAME a USAGI. Tyto projekty z velké části tvoří asijské a světové firmy či akademické subjekty zabývající se IPv6. První ze jmenovaných, projekt KAME, se zaměřil na implementaci IPv6 do BSD like systémů, byl uvolněn jako open source. Tento projekt oficiálně dokončil implementaci IPv6 v březnu roku 2006. Projekt USAGI je zkratka UniverSAl playGround for Ipv6 ve volném překladu znamená univerzální herní hřiště pro IPv6. Tento projekt měl za cíl implementaci IPsec a IPv6 protokolový stack pro všechny ostatní linux systémy. Na konec je dobré zmínit ještě 2 projekty, které se podílely na vývoji IPv6, jsou jimi TAHI a WIDE projekty. Tyto dva projekty měly za cíl testování implementací praktickými benchmarky a reálným nasazením.

7.2.3 Mac OS X

Informací ohledně implementace IPv6 do Mac OS X je velmi málo. Známo je jen to, že Mac OS X si převzal implementaci IPv6 od KAME projektu v průběhu roku 2006. IPv6 pak bylo dostupné od verze Mac OS X 10.4.8, kde bylo jako běžná součást systému.

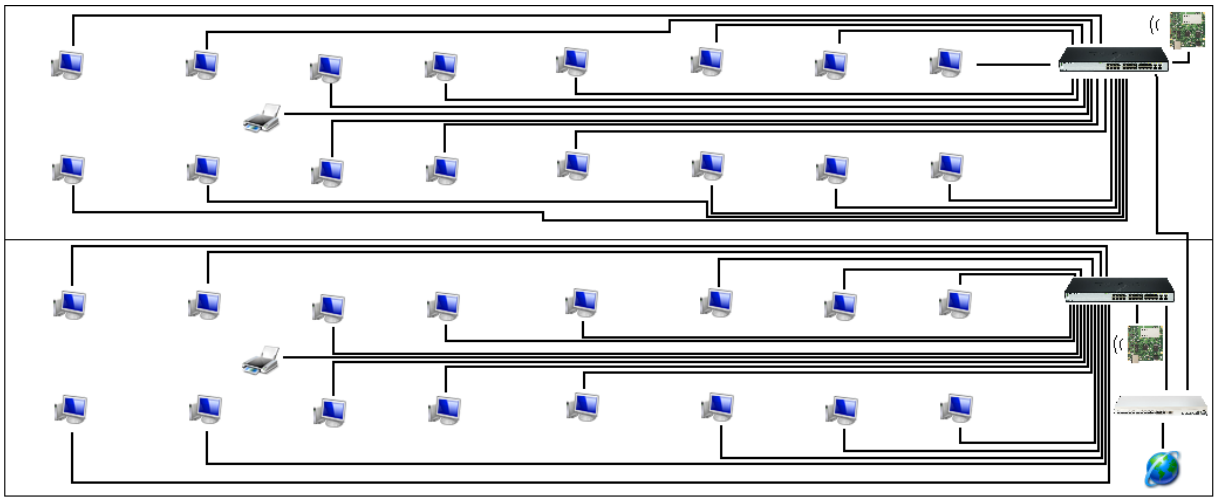
8 Příkladové nasazení Mikrotik RouterBoard a RouterOS

8.1 Brána ve střední firmě

8.1.1 Popis případu

Nasazení bude ve firmě využívající internetovou přípojku k běžné činnosti, VoIP, IPsec VPN a telekonferencím, firma podniká v oboru outsourcingu 3D modelování. Předpokládaný provoz ve špičkách bude 40 Mbps v obou směrech přibližně stejně, s cca 30000 paketů za vteřinu. Přípojka do internetu je zakončena RJ-45 konektorem, přenosovým médiem je FTTB konvertovaná na 1000BASE-T Ethernet. Pro tento účel jsem zvolil Mikrotik RouterBoard 1100 s 13 gigabit porty. Jako switche pro přístupovou firemní síť jsem zvolil typ D-Link DGS-1224TP s podporou PoE pro IP Telefony. Firma je umístěna v dvoupatrové budově, v každém patře je 16 počítačů. Celkem 32 klientských stanic, na každé patro jedna síťová tiskárna. Celkem spotřeba portů na patro 17 + uplink port. IP telefonie a běžná pc komunikace je oddělena VLAN, kde VoIP telefony mají přednost. V hlavní místnosti je umístěn serverový stojan XtendLan 18U/600x600. V prvním patře je umístěn nástěnný rozvaděč XtendLan 4U/600x435 umístěný na zdi. Hlavním stojanu je umístěn intranetový server a RB se Switchem. Zálohování napájení (UPS) má server vlastní, pro RB1100 a switch je zde druhá UPS TRIPPLITE 500VA/300W. Stejná UPS je použita v prvním patře na zálohování druhého switche. Ke každému pracovišti vede jeden pár kabelů, zásuvky jsou dvouportové. V každém patře bude umístěno jedno WiFi AP postavené na RB411-Hn-M pro bezdrátový přístup mobilních zařízení.

Obr. 11 Nákres firemní sítě



Zdroj:www.dlink.com, www.routerboard.com

8.1.2 Cenová kalkulace

Tabulka 3 Kalkulace firemního nasazení

Název	počet	cena kusu [Kč]	celková cena
D-Link Switch DGS-1224TP	2	13000	26000
Mikrotik RouterBoard 1100	1	5900	5900
Kabeláž CAT.6 typ FTP, 1 metr = 1 kus	1020	11	11220
Lišty na kabely 40x40x2000	510	60	30600
Další instalační materiál (vruty, hmoždinky apod.) celková cena	1	1200	1200
UPS Tripplite 500VA/300W Line Interactive 1U	2	5300	10600
XtendLan 18U/600x600 stojanový,černý,skl.dveře,perf.záda-S	1	8890	8890
XtendLan 4U/600x435,na zeď, jednodílný, skleněné dveře	1	2100	2100
Zásuvky na zeď - 2 portové	110	34	3740
Patch panel 19", 24 portů CAT6 stíněný	4	1500	6000
Mikrotik Routerboard 711-5Hn-M	2	720	1440
Kryt pro RB711, vnitřní	2	250	500
Pigtail MMCX - Nfemale	2	130	260
Stropní všesměrová anténa Pacific Wireless	2	520	1040
Patch kabely pro klientské stanice délka 7m	16	105	1680
Patch kabely pro klientské stanice délka 10m	16	135	2160
Patch kabel 0,5 m, do racku	40	27	1080
Instalace	1	10000	10000
Cena celkem			124410

Ceny v tabulce jsou uvedeny v korunách bez DPH.

8.2 Malá regionální síť pro poskytování internetového připojení

8.2.1 Popis případu

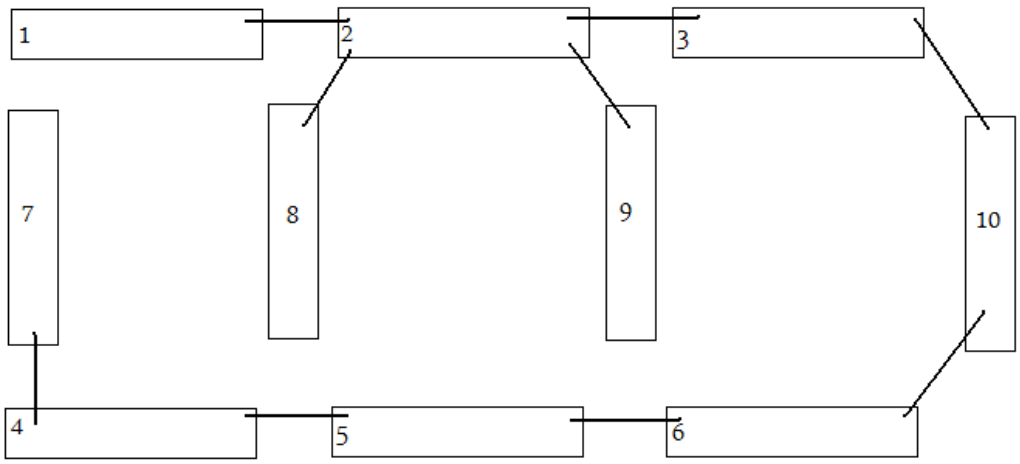
Mezi několika podnikateli padlo rozhodnutí zkusit podnikání jako poskytovatel internetového připojení (ISP). Portfolio poskytovaných služeb bude obsahovat internetové připojení, VoIP telefonii a IPTV. Pro první investici byl zvolen finanční strop 1 000 000 Kč. Záměrem je zasíťovat sídliště o 10 panelových domech. Jeden panelový dům má 7 pater, 2 vchody a v každém patře jsou 3 byty. Mezi jednotlivými panelovými domy budou nataženy optické převěsy, zálohované pomocí spanning tree protokolu. Délka mezi jednotlivými panelovými domy pro optický převěs je do 100 metrů. Kompletní natažení a navaření optických vláken bude provádět externí firma. Pro každých 5 panelových domů bude vyhrazen jeden router Mikrotik RouterBoard 1100 zastávající funkci shaperu, routeru, a DHCP serveru. Přenosovou soustavu bude tvořit v každém panelovém domě ethernet managed switch D-Link DGS-1210-48 s celkovým počtem 48 portů topologie

1000BASE-T a čtyřmi SFP šachtami osazenými dvěma WDM 1000BASE-LX simplex moduly. Na 3 panelových domech bude dále nainstalován WiFi access point postavený na RB433AH, rádiovou část tvoří karta R52Hn v počtu dvou kusů s připojenými sektorovými anténami Gainmaster 90°, zisk 17 dBi. V jednotlivých domech bude tato technologie umístěna v rozvaděči velikosti 6U. V hlavním rozvaděči bude zálohování napájení pomocí UPS APC Smart-UPS RT 2000XLI v provedení rackmount, v umístění přístupových switchů bude pouze přepěťová ochrana. Hlavní rozvaděč bude tvořit čtveřice RouterBoardů 1100, dvojice fiber switchů D-Link DGS-3100-24TG, optická vana 24 port a další podpůrná zařízení jako je accounting server, server pro IPTV, VoIP brána apod.

Rozdělení RouterBoardů bude následující:

- 2x RB1100 pro shaping, 2x 5 panelových domů, slučování VLAN
- 2x RB1100 , jeden jako hlavní a druhý záložní páteřní router, OSPF pro vnitřní síť, BGP pro vnější síť.
- 3x RB433AH , jako 2x WiFi AP na 3 panelových domech (1,3,5) , OSPF, shaper a DHCP pro WiFi klienty

Obr. 12 Nákres převěsů



8.2.2 Cenová kalkulace

Tabulka 4 Kalkulace nasazení ISP

Název	počet	cena kusu [Kč]	celková cena
Switch D-Link DGS-1210-48	10	13000	130000
Mikrotik RouterBoard 1100	4	5900	23600
Kabeláž CAT.6 typ FTP, 1 metr = 1 kus	4000	11	44000
Zásuvky na zeď - 1 portové	500	110	55000
Patch panel Cat 6 FTP 24 portů	20	1500	30000
Rozvaděč 32U/600x800 stojanový, černý, skleněné dveře-S	1	11300	11300
XtendLan rozvaděč 6U/600x550,na zeď, dvoudílný, skleněné dveře	10	3500	35000
mini GBIC SFP, SC, 1000Base-LX, 10km, WDM, TX1310nm/RX1490nm	40	1400	56000
19" rozvodný panel 7x230V, s nadproudovým jističem	10	1100	11000
APC Smart-UPS RT Rack-mount XL 2000XLI	1	24000	24000
D-Link DGS-3100-24TG, 8x 1000 Copper, 16x SFP	2	14000	28000
Mikrotik RouterBoard 433AH	3	2000	6000
MiniPCI R52Hn	6	800	4800
kryt pro RB433AH	3	350	1050
Pigtail MMCX - Nfemale	6	130	780
Anténa 5 GHZ Gainmaster 90°, zisk 17 dBi	6	2300	13800
Propojovací kabel k anténě 6 metrů Nfemale - Nmale	6	500	3000
Lišty pro rozvod po chodbách 40x20x2000	1260	45	56700
FO kabel, 9/125, 8c, samonosný, ocel. Lanko, 1 metr= 1 kus	2000	19	38000
Optická vana 8 port, 1U osazená SC konektory	1600	10	16000
Patch kabel optický SC-SC 1 metr	40	270	10800
Optická vana 24 port, 1U osazená SC konektory	1	1300	1300
Práce externí firmy, natažení, navaření, změření	1	75000	75000
Servery pro provoz VoIP, IPTV a accounting (dohromady)	1	250000	250000
Práce externí firmy, natažení metalické kabeláže a instalace rozvaděčů v panelových domech	1	60000	60000
Cena celkem			985130

Ceny v tabulce jsou uvedeny v korunách bez DPH.

9 Závěr

Cílem této práce bylo zmapovat základní techniky využívané v sítích a platforem umožňující routing. Řízení provozu, možností identifikace datových proudů a další funkce byly popsány v systému Mikrotik RouterOS. Dále byly popsány dnešní nejvyužívanější techniky dynamického routingu a nadcházejícího MPLS. Poslední kapitolou bylo popsání funkcí a změn nového protokolu IPv6 a podpory v klientských systémech Windows, Linux a Mac OS X.

Hlavním cílem nadcházejících let bude zavádění IPv6 protokolu. Nebude to bez strastí a problémů. V tomto kontextu si troufám říct, že IPv4 protokol tu bude přítomen ještě dlouhou dobu. Připravenost na IPv6 z pohledu nejpoužívanějších klientských systémů je dobrá, implementace v domácích prvcích je špatná. Tento stav by se měl brzy změnit, poslední IPv4 adresy se rozdělují již nyní. Výrobci tak budou mít důvod tyto funkce doplnit.

Spolu s navyšujícími rychlostmi bude IGP OSPF postupně odsunováno na okraje sítě a nahrazováno MPLS. Tento trend je dnes již viditelný v sítích velkých poskytovatelů internetu. Trendy v malých a středních sítích bude v nasazení OSPFv3 a kombinací BGP na hraničních routerech.

V době psaní tohoto závěru vyšla již finální verze 5.0 Mikrotik RouterOS, která obsahuje z velké části implementovanou funkční část IPv6. Stále chybí některé části, které jsou pro nasazení IPv6 v domácnostech velmi důležité např. DHCPv6 server a klient. Předpokládám, že během dalšího roku dojde k implementování těchto zbylých částí a RouterOS se tak stane plně IPv6 ready a tím bude schopen role profesionálního v6 routeru.

10 Seznam literatury

[1]. **Bartošek, Miroslav.** Krátce z historie Internetu. *UVTMU Zpravodaj.* [Online] 2. Únor 2011. [Citace: 17. Únor 2011.] http://www.ics.muni.cz/zpravodaj/articles/22.html.

[2]. **Chlad, Radim.** Historie Internetu v České republice. *www.fi.muni.cz.* [Online] 4. Únor 2011. http://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm.

[3]. **www.ieee.org.** IEEE 802.11™: WIRELESS LOCAL AREA NETWORKS (LANs). *www.ieee.org.* [Online] 7. Září 2007. [Citace: 12. Únor 2011.] http://cs.wikipedia.org/wiki/IEEE_802.11.

[4]. Neutral Internet eXchange. *Neutral Internet eXchange.* [Online] 7. Únor 2011. www.nix.cz.

[5]. **Švarc, Zdeněk.** ISPforum.cz. [Online] 7. Říjen 2005. [Citace: 14. Leden 2011.] http://www.ispforum.cz/viewtopic.php?f=16&t=2956.

[6]. **Sítí, Svět.** VLAN. *Virtual LAN - Svět Sítí.* [Online] 2. Duben 2003. [Citace: 27. Únor 2011.] http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=237&clanekID=238.

[7]. **Cotton, Michelle, Vegoda, Leo a Meyer, David.** Internet Engineering Task Force (IETF). *IANA Guidelines for IPv4 Multicast Address Assignments.* [Online] Březen 2010. [Citace: 4. Březen 2011.] http://tools.ietf.org/html/rfc5771.

[8]. Manual:HTB. *MikrotTik.* [Online] 14. duben 2010. [Citace: 9. Březen 2011.] http://wiki.mikrotik.com/wiki/HTB.

[9]. **Tulloch, Mitch.** IPv6 Support in Microsoft Windows. *WindowsNetworking.com.* [Online] 13. Duben 2006. [Citace: 21. Březen 2011.] http://www.windowsnetworking.com/articles_tutorials/IPv6-Support-Microsoft-Windows.html.

[10]. **Riekstins, Arnis a Tully, John.** About Mikrotik RouterOS. *Mikrotik RouterOS.* [Online] 2011. http://www.mikrotik.com/aboutus.php.

11 Seznam obrázků

12 Seznam tabulek