Česká zemědělská univerzita v Praze
Technická fakulta

Návrh přechodu na IPv6 u komerčního poskytovatele připojení

Diplomová práce

Vedoucí bakalářské práce: **Ing. Zdeněk Votruba.**
Autor: **Zuzana Lebedová**

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra technologických zařízení staveb

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Lebedová Zuzana

Informační a řídící technika v agropotravinářském komplexu

Název práce

Návrh přechodu na IPv6 u komerčního poskytovatele připojení

Anglický název

Proposal for the transition to IPv6 commercial Internet service provider

---

Cíle práce

Cílem práce je navrhnout optimální řešení přechodu na IPv6 v komerční firmě poskytující internetové připojení. Podrobněji zpracovat problematiku routování a nastavení sítě na protokolu IPv6 a následně otestovat funkčnost na vybrané části sítě. Definovat základní předpoklady pro využití této služby a doporučení pro reálný provoz.

Metodika

Na základě literární rešerše posoudit vhodnost nastavení protokolu IPv6 v síti, sestavit metodiku testování a provést testy. Testy zpracovat a zobecnit. Na základě výsledků definovat doporučení pro reálný provoz.

Osnova práce

1. Úvod
2. Literární rešerše
3. Funkčnost sítě na IPv4
4. Protokol IPv6
5. Problematika rozvoje IPv6
6. Návrh přechodu na IPv6
7. Metodika testování
8. Výsledky testů a jejich zhodnocení
9. Doporučení
10. Závěr a ekonomické zhodnocení

Rozsah textové části
50 - 60 stran textu včetně příloh

Klíčová slova
počítačové sítě, routování, IPv4, IPv6

Doporučené zdroje informací

Wendell, O., Rus, H., Naren, M.: Směrování a přepínání sítí, CPress, 2009, ISBN:978-80-251-2520-5
Satrapa, P.: Internetový protol IPv6, CZ.NIC, 2008, ISBN: 978-80-904248-0-7
Healy, R., Odom, W., Mehta, N.: Směrování a přepínání sítí, CPress, 2009, ISBN: 978-80-251-2116-0
Keršláger, M., Horák, J.: Počítačové sítě pro začínající správce, CPress, 2008, ISBN: 978-80-251-3176-3

Vedoucí práce
Votruba Zdeněk, Ing.

Termín zadání
listopad 2013

Termín odevzdání
duben 2015

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
-3-
TECHNICKÁ FAKULTA

doc. Ing. Miroslav Přikryl, CSc.
Vedoucí katedry

prof. Ing. Vladimír Jurča, CSc.
Děkan fakulty

V Praze dne 3.2.2014

Čestné prohlášení:

Prohlašuji, že jsem diplomovou práci vypracovala samostatně, na základě informací získaných z uvedené literatury a po odborných konzultacích s vedoucím diplomové práce.

V Praze dne ……. Podpis……

Poděkování:

Děkuji vedoucímu diplomové práce Ing. Zdeňkovi Votrubovi za věcné připomínky, za možnost psát práci na toto téma a za vedení mé práce. Dále děkuji firmě LASCO s.r.o. za poskytnutí všech informací potřebných k dokončení mé práce a za možnosti provedení praktické části. V neposlední řadě bych chtěla poděkovat svému otci za vysvětlení některých pojmů a poskytnutí praktických ukázek nastavení.

Abstrakt:
Cílem této práce je návrh přechodu na protokol IPv6 v reálných podmínkách u poskytovatele internetu. Jedním z úkolů je provést analýzu současného stavu sítě a na základě teoretických informací vytvořit návrh a adresní plán s ohledem na budoucí rozvoj sítě a ekonomické zatížení. Dalším úkolem je sestavit metodiku testování, následně nastavit všechna potřebná zařízení a provést všechny testy průchodnosti a funkčnosti nasazení protokolu IPv6. Výsledkem této práce je zhodnocení testů, doporučení pro reálný provoz a ekonomické zhodnocení.

Klíčová slova: Počítačové sítě, routování, IPv4 a IPv6

Abstract:
The aim of this work is to design the transition to IPv6 in real terms at the ISP. One of the tasks is to analyse the current state of the network and on the basis of theoretical information to draft a plan to address with regard to future network development and economic burden. Another task is to compile testing methodology, then set all the necessary equipment and perform all tests throughput and functionality deployment of IPv6. The result of this work is to evaluate the tests, recommendations for real and economic evaluation.

Keywords: Computer networks, routing, IPv4 and IPv6

1 Úvod

Internet se neustále rozšiřuje a každý den je připojeno velké množství nových zařízení, které musí být jasně identifikovány. Pro tuto identifikaci slouží internetová adresa, kterou používá protokol IPv4 nebo novější protokol IPv6. Adres, které se používají v IPv4 protokolu, je jen omezené množství a bylo nutné vymyslet způsob, jak tuto situaci v budoucnu řešit. Nejprve vznikl překlad adres, který umožnil využívat určitý rozsah adres ve více sítích a tím se velmi zpomalil rozvoj nového protokolu. Následně byl rozvíjen protokol IPv6, který se postupně začíná používat.

Celosvětový správce IP adres IANA přerozděluje adresy pěti regionálním registrům a ty pak dále jednotlivým poskytovatelům služeb a koncovým uživatelům. Na začátku února v roce 2011 došlo k přidělení posledního bloku IPv4 adres. Pět měsíců na to došly adresy u regionálního registru APNIC, který spravuje region jihovýchodní Asie, Austrálie a Pacifiku. Dále následovaly i další regiony. To znamená, že žádný poskytovatel služeb již nedostane žádné IPv4 adresy pro svou infrastrukturu a zákazníky. Tato situace velmi komplikuje rozvoj současných služeb a připojování nových zákazníků.

Díky tomuto rozvoji techniky, internetu a rozdělení všech IPv4 adres bylo nutné tuto situaci řešit. Překlad adres NAT už také postupně přestává dostačovat, tak jedním ze zásadních řešení by byl přechod na verzi IPv6. Velice důležité bylo, že velcí poskytovatelé obsahu jako Google, Facebook, Yahoo a další se spojili a 6.6.2012 spustili své služby na protokolu IPv6 a tím odstartovali přechod i pro další firmy.

Rozvoj tohoto protokolu je velmi pozvolný a přechod bude ještě delší dobu trvat. Domnívám se, že hlavním a největším důvodem pomalého přechodu je finanční náročnost obměny síťových zařízení. Další možností je využít některý z přechodových mechanismů, které však nejsou tak spolehlivé. Firmy a poskytovatelé postupně budou přecházet spolu s rozvojem infrastruktury sítí.

Horší je situace pro poskytovatele připojení, pro něž je nasazení IPv6 výrazně komplikovanější záležitost, protože všechny prvky sítě musí tento protokol

podporovat, od páteřních spojů až ke koncovým uživatelům, a to může být opět velmi nákladné.

Tento protokol není zcela běžně podporován na firemních sítích, a tak jsem se rozhodla toto téma použít pro mou práci, zjistit více informací o tom, jak protokol a síť s tímto protokolem funguje v praxi.

V této práci jsem se rozhodla zhodnotit jednotlivé možnosti přechodu na IPv6 u poskytovatele internetového připojení. Součástí práce je i nasazení protokolu na části sítě, otestování průchodnosti od koncového počítače až na internet a zhodnocení tohoto testování.

Toto zhodnocení by mělo následně sloužit pro kompletní nasazení protokolu v celé síti, a také možnost poskytnout služby klientům prostřednictvím IPv6. Zabývám se i ekonomickým zhodnocením jednotlivých variant s ohledem na současný stav sítě a rozvoj v budoucnu.

První část této práce se zabývá protokoly IPv4 a IPv6, jejich rozdíly, variantami přechodu na IPv6 a dalšími teoretickými znalostmi. Druhá část se zaměřuje na problematiku návrhu a nasazení IPv6 v reálném prostředí firemní sítě. Následuje poslední část celé práce zhodnocení všech testů, doporučení a ekonomické zhodnocení.

2 Literární rešerše

Ze statistik lze zjistit, které státy mají podporu IPv6. Na stránkách www.ipv6-test.com v záložce Stats (statistika) lze zjistit 25 států, které jsou na tom nejlépe. Probíhají testy a na základě testů je sestavena tabulka s procentuálním hodnocením podpory obou protokolů. Nejlépe je na tom stát Monako, který má 100% podporu pro IPv4 a 80% pro IPv6, pro tento stát však proběhlo pouze 10 testů, výsledky tedy nejsou úplně autentické. V této tabulce je Česká republika umístěna na 18. místě a celkový počet testů je přes 3000. Podpora pro IPv4 je na 98% a IPv6 na 58,5%.

Další z možností je tabulka ukazující rozvržení unikátních veřejných adres a v tomto testování je Česká republika na 10. místě (Obr.1). Opět bylo provedeno přes 3000 testů a vyšlo necelých 51% pro unikátní adresy v rámci IPv4 a 49% pro unikátní adresy v rámci IPv6. Z těchto testů lze zhodnotit, že i pro IPv4 je u nás hodně používaný překlad adres NAT, díky kterému není potřeba všechny adresy mít veřejné. Oproti tomu pro IPv6 máme unikátní adresy skoro v 50%, což je dobrý výsledek.

Obr. 1 Rozvržení unikátních adres

Top 25 countries for IPv6 support (unique addresses, Mar 2015)

	Country	Test count	IPv4	IPv4 %	IPv6	IPv6 %
1.	Suriname	29	8	29.6%	19	**70.4%**
2.	Puerto Rico	240	37	38.5%	59	**61.5%**
3.	Luxembourg	385	102	40.6%	149	**59.4%**
4.	United States	90,748	22,958	42.7%	30,784	**57.3%**
5.	Netherlands	11,271	2,615	47.0%	2,951	**53.0%**
6.	Norway	1,962	592	49.9%	594	**50.1%**
7.	U.s. Virgin Islands	10	4	50.0%	4	**50.0%**
8.	Guatemala	31	14	50.0%	14	**50.0%**
9.	Switzerland	2,998	823	50.0%	822	**50.0%**
10.	Czech Republic	3,079	897	50.9%	865	**49.1%**

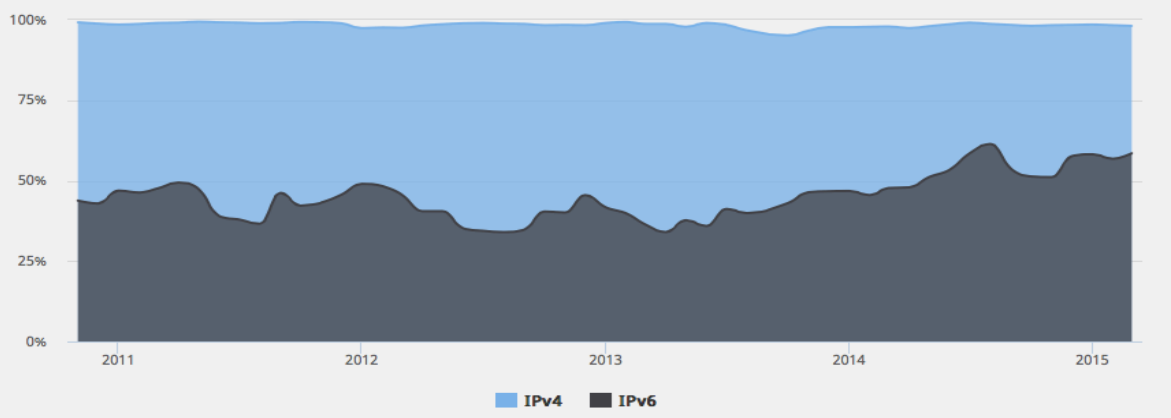
Zdroj: www.ipv6-test.com [10]

Na těchto stránkách jsou zobrazené i grafy, kde je porovnání obou protokolů. Z posledních naměřených hodnot na konci února 2015 vyšlo měření podpory protokolu IPv6 na 45% celosvětově. Můžeme předpokládat, že se postupně dostaneme zhruba na polovinu celosvětové podpory IPv6.

Z dalšího grafu je možné zjistit procento podpory IPv6 v případě, že jsou k dispozici oba protokoly (tzv. Dual stack). Prohlížeč má implicitně nastaven protokol IPv6 i v případě, že jsou oba dostupné. Někdy se však může stát, že zůstává výchozí IPv4 díky tunelování. Procento podpory v prohlížečích je necelých 71%.

Na těchto stránkách také lze vyhledat statistiky přímo pro Českou republiku včetně poskytovatelů připojení. V grafu je vidět rostoucí tendence IPv6 v ČR, v současné době je na 58,5%.

Obr. 2 Podpora IPv6 adres



Zdroj: www.ipv6-test.com [11]

Je možné tam také najít i nástroj pro otestování a validaci webových stránek, kde se zadá doménové jméno a validátor vygeneruje kód. Po uložení tohoto kódu na webové stránky se zobrazí malé tlačítko s nápisem IPv6, slouží jako identifikace, že webové stránky podporují IPv6. Tento validátor je na stejných stránkách jako předešlé statistiky, jen v záložce website. Jediný problém je, že server, na kterém webové stránky jsou uložené, musí mít podporu IPv6 a doména musí mít záznam v DNS, který umožní překlad IPv6 adresy a doménového jména.

Dle zjištěných materiálů a informací se IPv6 jeví jako rychlejší protokol, bezpečnější a s řadou dalších výhod. Zda poskytovatel internetu má podporu IPv6 lze snadno zjistit z webových stránek www.test-ipv6.cz nebo www.ipv6-test.com, kde lze zjistit i rychlost připojení.

Pro uživatele je tento protokol velkým přínosem, pro poskytovatele internetu to však znamená problémy spojené s návrhem a nastavováním.

3 Funkčnost sítě na IPv4

V současné době je přechod na IPv6 stále pozvolný, a tak je IPv4 stále hojně využíván. Pro pochopení rozdílů a využití je potřeba vědět, jak oba protokoly fungují. Nejprve je dobré říci, jaké jsou rozdíly v adrese.

Propojení počítačů v síti vyžaduje určitý druh adresování či identifikace uzlů v síti. Pro posílání dat v rámci sítě musíme znát identifikující IP adresu.

IP adresa verze 4 je 4 bajtové číslo, které se zapisuje jako čtveřice desítkových čísel oddělených tečkami. Obsahuje adresu konkrétní sítě a uzlu v této síti. Celkově lze rozdělit 2^{32} adres, což je cca 4 miliardy adres.

IP adresa verze 6 byla rozšířena na 16 bajtů a zapisuje se jako osmice hexadecimálních číslic. V přepočtu je to 2^{128} adres, což odpovídá počtu $5x10^{28}$ adres na každého obyvatele zeměkoule.

Jak je zřejmé, protokol IPv6 má mnohem větší adresní prostor, je tedy možné připojit každý počítač a směrovač na světě a ještě mnoho adres zbyde.

3.1 IP paket

Obr. 3 IPv4 paket

Zdroj: www.wikimedia.org [12]

První položkou paketu je verze, ve které se udává, o jaký jde protokol. Ve verzi IPv4 je číslo 4. Následuje položka délka hlavičky, která určuje celkovou velikost hlavičky od 20 do 60 bajtů. Další položka je typ služby, který měl dle původních plánů sloužit pro účely směrování podle priority paketu a požadavků paketu.

Identifikace slouží pro identifikování paketu. Každý paket má jednoznačný identifikátor, který je využit při fragmentaci, kdy se paket rozdělí a podle identifikátoru lze určit, které části patří k jednomu paketu.

Posun fragmentu určuje, zda se paket může fragmentovat, tedy rozdělit a poslat části zvlášť a také v jakém bajtu je paket rozdělen.

Životnost paketu je hodnota, která je nastavena na začátku před posláním paketu. Při průchodu routerem se sníží o jedničku a pokud se dostane na nulu, pak vyprší životnost paketu a paket je zahozen.

Další položkou je protokol, tato položka určuje protokol vyšší vrstvy, na který se má paket předat.

Kontrolní součet slouží pro kontrolu, zda nedošlo k chybě při předávání paketu. Provede se kontrolní součet a pokud souhlasí, paket je předán dál, pokud nesouhlasí, paket je zahozen.

Adresa odesílatele a cílová adresa určují IP adresy odkud se paket zasílá a kam. Poslední položka je volby, kde jsou různé rozšiřující informace nebo požadavky na paket.

3.2 Principy v IPv4

Ne všechny služby fungují na síti s protokolem IPv6 tak, jako s protokolem IPv4, proto je potřeba se podívat blíže na konkrétní principy, které v síti fungují pod protokolem IPv4.

3.2.1 Routování

Routování je předávání datových paketů v síti. Router má uloženou tabulku s adresami svých sousedů, případně sousedních sítí. Podle adres uložených v tabulce se rozhoduje, co s paketem provede. Směrování probíhá samostatně pro každý procházející paket.

Naplnění routovací tabulky provádí routovací protokoly, jako např. RIP nebo častěji používaný OSPF. Tabulka se musí průběžně aktualizovat a toto naplnění může

probíhat staticky nebo dynamicky. Statické směrování pracuje s tabulkou, která se nemění a v případě změny adres v síti se musí přenastavit ručně.

Dynamické routování reaguje na změny v topologii a upravuje směrovací tabulku podle situace v síti. Toto řešení je výhodné ve větších sítích, ve kterých se nachází více routerů, a díky tomuto způsobu lze např. „obejít“ výpadek jednoho z nich. [3]

3.2.2 Princip routování

Obecně každá komunikace v síti je prováděna jako komunikace bod-bod. Pokud posíláme paket mezi různými dílčími sítěmi, probíhá vždy předávání paketu mezi jednotlivými sousedy. Router přijme paket a podle IP adresy v hlavičce ho porovná s údaji v routovací tabulce. Pokud IP adresa v hlavičce souhlasí s některým údajem v routovací tabulce, pak router paket odešle na příslušnou IP adresu. Není-li nalezena shoda v routovací tabulce, router zkontroluje, zda má nastavenou výchozí cestu. Pokud má, paket je zaslán na příslušné rozhraní (jiný router v síti), pokud nemá, paket je zahozen. Obecně platí, že každý router musí znát alespoň jednoho svého souseda, který je pro něj nadřazen (tzv. gateway). Sem pak posílá všechny pakety, které není schopný poslat některému ze známých sousedů. Routery tak vytváří stromovou hierarchickou komunikační strukturu. [3]

3.3 Služby na routerech

Router jako síťové zařízení propojující různé sítě musí mít možnost nastavení různých služeb. Mezi tyto služby patří DHCP, překlad doménových jmen DNS, firewall, překlad portů a překlad IP adres NAT aj.

3.3.1 DHCP

Jednou z těchto služeb je DHCP (Dynamic Host Configuration Protokol), protokol sloužící pro přidělování IP adres klientům a ke konfiguraci síťových uzlů. Je založen na komunikaci klient–server, klient zašle požadavek a server odpoví nabídkou možných konfigurací. Konfigurace může být automatická nebo dynamická. Automatická konfigurace spočívá v přidělení trvalých parametrů stanici nebo síťovému uzlu. Dynamická konfigurace umožňuje přidělit parametry jen na určitou

dobu. Tato doba může být různá a tato konfigurace se hojně využívá pro wifi připojení v kavárnách a pro připojení mobilních zařízení, která potřebují IP adresu jen na krátkou dobu.

3.3.2 DNS

Další služba je DNS (Domain Name System), systém doménových jmen má na starosti překlad jmen na IP adresy a naopak. Vyhledávání na internetu pomocí IP adres by bylo velmi složité na zapamatování a správu, proto vznikl překlad IP adres na doménová jména. Určitá skupina IP adres má přiděleno jedno doménové jméno, které je možné použít místo IP adresy. Každý uzel obsahuje data o své části jména, které je mu přiděleno a odkazy na své subdomény.

Např. stránky www.google.com mají IP adresu 173.194.66.106 a pro zapamatování by to bylo složité, proto DNS překládá IP adresu na doménové jméno. Nejvyšší doména je root, což je www. Nižší doména je tematická (.com, .edu) nebo národní (.cz, .com atd.) a ty se dále dělí na nižší a menší celky. V tomto příkladu je doménové jméno google a nižší doména je .com.

Existuje také reverzní DNS, které překládá doménové jméno na IP adresu. Toto si lze ověřit v příkazovém řádku zadáním příkazu tracert a doménového jména. Ukáže se seznam IP adres jednotlivých routerů, přes které dotaz jde, ale také IP adresa doménového jména.

3.3.3 Firewall

Další důležitá služba fungující na routeru je firewall. Jde o službu, která slouží k zabezpečení sítě. Definuje pravidla pro komunikaci mezi sítěmi, které odděluje. Měl by zabránit neoprávněnému přístupu zvenčí nebo naopak neoprávněnému přístupu zevnitř. Veškerá komunikace probíhající mezi sítěmi je kontrolována pomocí firewallu a zprávy, které nesplňují bezpečnostní požadavky jsou zablokovány. Existuje několik typů firewallu, paketový filtr, stavový paketový filtr a aplikační brána.

Prvním jmenovaným je paketový filtr. Pracuje na síťové vrstvě a jeho úkolem je kontrolovat všechny procházející pakety. Kontroluje každý paket zvlášť

a rozhoduje, zda se má zahodit nebo přeposlat dál. Paketový filtr nerozumí pravidlům ve vrstvě vyšší, než je síťová a nedokáže se jimi řídit, proto jsou rozhodujícími atributy zdrojová IP adresa, cílová IP adresa, adresa rozhraní odkud paket přišel, zdrojový a cílový port atd.

Druhým jmenovaným je stavový paketový filtr. Je velmi podobný jako jednoduchý paketový filtr, ale navíc má informace o povolených spojeních. Firewall má samostatnou stavovou tabulku, ve které jsou uložené informace o spojeních. Při průchodu paketu firewallem, rozhodne podle své tabulky, zda paket patří do povoleného spojení nebo zda má opětovně projít rozhodováním. Tento typ firewallu je rychlejší a účinnější, nemůže se stát, že by prošel paket, který by dopředu neprošel rozhodovacím procesem.

Třetím typem firewallu je aplikační brána, někdy také nazývána jako proxy firewall. Aplikační brána pracuje na aplikační vrstvě a chrání samotné aplikace. Komunikace probíhá prostřednictvím proxy serverů. Klient naváže spojení s aplikační bránou, která poté naváže spojení s proxy serverem. Brána dostane od serveru odpověď, kterou poté zašle klientovi zpět v původním spojení. Jde o poměrně vysoce spolehlivé zabezpečení, ale také velmi náročné na hardware. Aplikační brána zpracuje menší množství spojení než paketový filtr. [1]

3.3.4 NAT

Díky velkému rozvoji internetu a rozdělení adres mezi poskytovatele bylo nutné vyřešit problém s nedostatkem adres. Každý uživatel internetu nemůže mít veřejnou IP adresu, protože by velmi rychle došly. Velké řešení byl překlad adres NAT (Network Adress Translation). Umožňuje celou vnitřní síť ukrýt za jednu veřejnou IP adresu. Při směrování se v paketu změní adresa odesílatele z té vnitřní na adresu vnější a navenek tak tedy vypadá, že se pod tou jedinou veřejnou adresou skrývá jedno zařízení. Ve skutečnosti se za touto veřejnou adresou může schovávat skoro libovolné množství počítačů nebo celých sítí.

Velkou výhodou NATu je to, že se k vnitřním sítím nelze dostat zvenku. Tím, že se celé sítě jeví jen jako jedno zařízení pod jednou veřejnou adresou, není vnitřní síť

„viditelná“ a případný útočník neví přesnou strukturu vnitřní sítě. Tento mechanismus je jistou slabší formou zabezpečení před útoky hackerů.

Další velkou výhodou je to, že se stejné adresy mohou využívat v různých sítích a nebude to působit problém. Je tedy možné, že dva různí poskytovatelé internetu použijí úplně stejné vnitřní IP adresy ve svých sítích. Pro tyto účely jsou vyhrazeny rozsahy vnitřních adres, které nelze použít jako veřejné adresy.

3.3.5 PAT

S tím úzce souvisí překlad portů PAT (Port Address Translation), který je rozšířením pro NAT. Pro všechny počítače v jedné podsíti router použije jednu veřejnou IP adresu se kterou komunikuje ve vnější síti. Pro každý počítač v této podsíti „za routerem“ přidělí router svůj port. Ve vnější síti to vypadá, jako by komunikoval stále stejný počítač, ve skutečnosti to může být kterýkoliv v podsíti. Router má ve své tabulce MAC adresy, IP adresy a čísla portů všech síťových prvků ve své podsíti.

4 Protokol IPv6

Protokol IPv6 má spoustu výhod, jako je mnohem větší adresní prostor, veřejné IP adresy bez nutnosti překladu NAT, nebo také velká podpora mobilních klientů. Podpora IPv6 v operačních systémech je již dostatečně rozšířena, ale některé vlastnosti jsou ještě v experimentálním stádiu vývoje, jako například mobilita. Rovněž DHCPv6 není propracován tak dokonale, jak bychom očekávali podle zkušeností s DHCP ve verzi IPv4. [6]

4.1 IP paket

Obr. 4 IPv6 paket

Zdroj: www.ipv6.cz [9]

Na obrázku je vidět formát paketu IPv6. Paket vypadá oproti IPv4 jednodušeji, má však spoustu rozšiřujících částí. V protokolu IPv4 má paket stále stejné prvky, u IPv6 se používají pouze ty, které jsou v daný moment opravdu nutné. Tím se trochu zjednodušuje struktura paketu IPv6.

Vznikla základní hlavička, která má konstantní délku, a je velmi zjednodušena. Ostatní údaje byly přemístěny do rozšiřujících hlaviček, které slouží pro doplnění o položky, které mohou být přítomny, nebo mohou zcela chybět. Používá se zřetězení hlaviček a každá hlavička je samostatný blok, který navazuje na hlavičku předešlou. V každé hlavičce je uvedeno, která hlavička bude následovat. Tímto je možné zřetězit libovolný počet hlaviček do jednoto paketu. [14]

První položkou základní hlavičky paketu je Verze, která platí pro obě verze protokolu. Pomocí této položky se určuje, zda jde o paket v protokolu IPv4 nebo IPv6.

Další položkou je třída provozu, někdy také označována jako třída dat. Svou hodnotou uvádí, jakou prioritu paket má a kam má být zařazen. Tuto položku využívají routery, aby mohly rozlišit prioritu a důležitost paketu.

Následuje položka značka toku, což je nová položka u IPv6 protokolu. Tok může být nazván jako proud paketů, které mají společné vlastnosti, např. adresáta, odesílatele. Tento princip mohou využít routery ke směrování paketů, umožňují rozpoznat, do kterého toku paket patří.

Délka dat je další položkou v paketu. Obsahuje informace o délce paketu, tedy počet bitů, které následují za základní hlavičkou paketu.

Další hlavička specifikuje typ následující hlavičky. Existuje mnoho těchto hlaviček a v paketu se použijí jen ty, které jsou potřebné.

Následuje maximální počet skoků, což je hodnota, která určuje životnost paketu. Před odesláním paketu je v této položce uložena hodnota maxima skoků. Při průchodu směrovačem je tato hodnota snížena o jedničku, dokud se hodnota nedostane k adresátovi nebo na 0, pak je paket zahozen a odesilateli přijde zpráva, že byl paket zahozen. Obdobná položka je i v IPv4 paketu, jen se jmenuje Životnost (TTL-time to live).

Adresa odesilatele a cílová adresa jsou dvě položky základní hlavičky, které mají uložené IP adresu odesilatele a IP adresu, kam se má paket doručit. Oproti IPv4 je adresa 4x delší, ale funkce zůstává stejná.

4.2 Adresy v IPv6

Principy adresace sítí a zařízení zůstaly zachovány jako u protokolu IPv4, jen adresa se zvětšila na čtyřnásobek, tedy na 128 bitů. Zapisuje se jako osmice čtyř hexadecimálních číslic oddělených dvojtečkami. V adrese často bývají uvedené řetězce nul, které se dají nahradit dvojtečkami, tím se adresa zkrátí.

Například adresa fbae:9a8d:843::42/64 by v úplném zápisu vypadala takto: fbae:9a8d:0843:0000:0000:0000:0000:0042/64.

Tím, že se pro oddělení číslic používá dvojtečka, stejně tak se používá i pro použitý port, je někdy matoucí, zda jde ještě o adresu nebo o přidělený port, proto se adresa uvádí v hranatých závorkách.

Například adresu a port 80 bychom zapsali [fbae:9a8d:843::42]:80. Takto lze adresu zapsat třeba i do URL ve webovém prohlížeči (http://[fbae:9a8d:843::42]:80).

V některých případech může adresa obsahovat i IPv4 adresu. Zapisuje se posledních 32 bitů tak, jak jsme byli zvyklí u IPv4, například ::ffff:147.251.54.47. Takový zápis pro IPv6 adresy se často objevuje v operačních systémech, které oba typy adres vnitřně ukládají do stejných struktur. [14]

Za lomítkem na konci adresy se používá délka prefixu sítě, která je zapsána v desítkové soustavě. Prefix sítě určuje poskytovatel připojení a slouží pro identifikaci o kterou síť se jedná. Velké firmy poskytující internetové připojení dostávají od svého nadřízeného poskytovatele služeb prefixy 48 bitů, koncové sítě pak 64. Rozdělení sítí a adres v nich si pak určuje každý poskytovatel sám. Tento prefix také označuje pouze jednu konkrétní adresu.

4.3 Typy adres

U protokolu IPv6 se používají tyto základní typy adres a to globální, linkové, skupinové.

4.3.1 Linkové

Linkové adresy se používají pouze v lokální síti, nesmí se směrovat a poznají se podle prefixu fe80::. Bývají automaticky generované, a pro použití je nutné specifikovat rozhraní, přes které se dá k adrese dostat.

4.3.2 Globální

Globální adresy jsou celosvětově unikátní a jednoznačné. Velký rozsah adres u novějšího protokolu dovoluje plně využívat těchto globálních adres a není tedy

nutnost schovávat více adres za jedinou, tak jak tomu je u IPv4. Díky absenci NAT jsou globální adresy dostupné odkudkoliv a přímo.

Zrušení NATu je obecně bráno jako velký přínos, má to však i stinné stránky, jako například nutnost zlepšení firewallu a dalších obranných mechanismů proti nelegálnímu přístupu a proti napadení, zejména koncových počítačů zákazníků či firem. Tím, že jsou adresy veřejné a kdokoliv je tedy může zjistit, jsou sítě náchylnější k útokům hackerů.

4.3.3 Skupinové adresy

Skupinové adresy představují samostatný typ adres v protokolu IPv6 a slouží k adresaci určitých skupin zařízení. Jestliže se zasílají nějaká data na tuto skupinovou adresu, pak dorazí na všechny členy skupiny. Skupinové adresy se používají mimo jiné i pro šíření obrazového a zvukového signálu v reálném čase, jako např. videokonference. U skupinových adres platí, že se dané adresy nesmí objevit jako odesílatel, ale jen jako adresát.

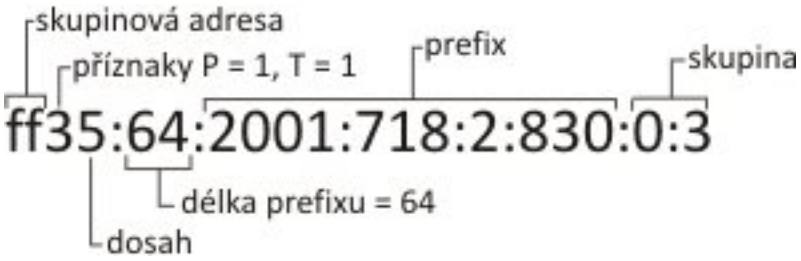
První část adresy tvoří položka, která slouží k určení, zda jde o skupinovou adresu, je to prvních osm bitů, které jsou nastavené na jedničku. Následují čtyři bity, které pomocí příznaku určuje volby dané adresy. První příznak je označen P a T. Příznak P je použit u skupinových adres, které jsou odvozené z individuálních globálních adres. Pokud je hodnota jedna, pak skupinová adresa vychází ze síťového prefixu a následující hodnota musí být také jedna. Pokud je hodnota P nula, pak adresa nevychází ze síťového prefixu. Příznak T slouží k určení, zda bylo přidělení adresy trvalé nebo pouze na nějakou dobu. Trvalé přidělení adres zajišťuje IANA a poskytovatelé připojení. Pokud je hodnota T nula, adresa je přidělena trvale, pokud je T nastaveno na jedna, adresa je pouze dočasná.

Dále následuje položka dosah, která má čtyři bity a určuje, jaká je maximální povolená vzdálenost mezi členy ve skupině. Takto je definováno šestnáct skupin dosahu.

Dalšími položkami je délka prefixu a samotný prefix, který určuje poskytovatel připojení a může jednotlivým sítím přiřadit vhodný prefix dle velikosti sítě.

Poslední položkou skupinové adresy je skupina, která slouží k identifikaci.

Obr. 5 Formát IPv6 adresy



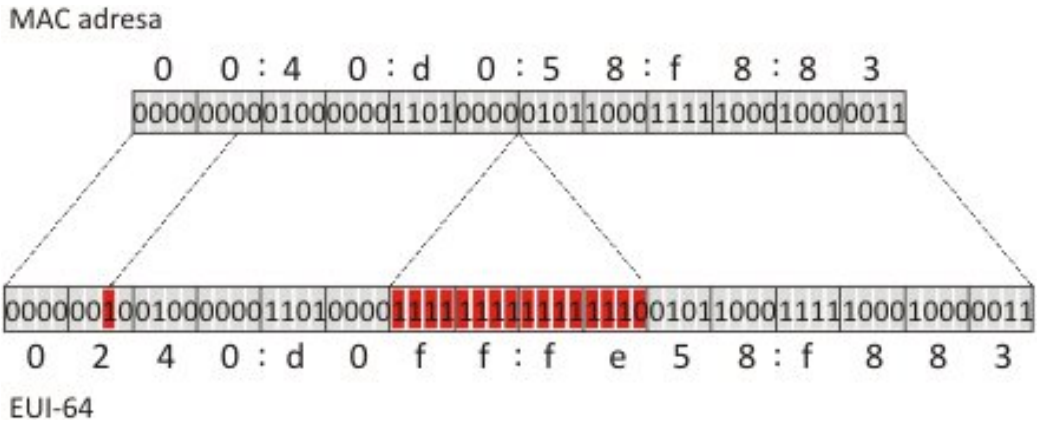
Zdroj: access.feld.cvut.cz [7]

4.4 Získání IPv6 adresy

U protokolu IPv4 se adresy konfigurovaly ručně nebo pomocí DHCP. V protokolu IPv6 lze adresu také nastavit ručně, pro svou délku a složitost se však doporučuje autokonfigurace. Tento mechanismus umožňuje automaticky získat globální adresu pro každý uzel a počítač připojený do sítě.

Jedním ze způsobů získání IP adresy je použití modifikovaného EUI-64, což je mechanismus, který využívá pro získání IP adresy MAC adresu síťového rozhraní. Nejprve se vezme MAC adresa a upraví se na požadovaný počet bitů 64. Úprava se provede tak, že se mezi třetí a čtvrtý bajt MAC adresy vloží dva bajty o hodnotě fffe a vznikne tak 64 bitová adresa. Poté se musí sedmý bit od začátku adresy invertovat a tím vznikne modifikovaný EUI-64. Tímto způsobem lze z jakékoliv MAC adresy vytvořit platnou a unikátní IPv6 adresu.

Obr. 6 EUI-64



Zdroj: access.feld.cvut.cz [8]

4.5 ICMPv6

Protokol ICMP není úplnou novinku, ale je velmi přepracovaný. V IPv4 se tento protokol ICMP také objevuje, ale nebyl tak důležitý jako v IPv6. Spoustu mechanismů v rámci protokolu IPv6 staví na tomto protokolu ICMPv6, je tedy nutné, aby všechna zařízení podporující IPv6 podporovala také ICMPv6.

Protokol ICMPv6 je používám hlavně pro výměnu provozních informací, testování dosažitelnosti a pro hlášení chybových stavů. Je také používán pro objevování sousedů a podporu skupinových adres. Tyto výsledné zprávy jsou předávány pomocí paketů protokolu IPv6.

Existují dvě skupiny těchto zpráv. Jednou skupinou jsou informační zprávy a druhou skupinu tvoří chybové zprávy. Chybové zprávy mohou informovat o nedosažitelnosti, kdy cílová adresa je nedosažitelná, o nadměrnosti datagramu, kdy se na přenosové cestě objevuje uzel, který nemůže předat paket dál kvůli jeho velikosti. Může se také objevit odpověď o vypršení životnosti paketu, kdy nebyl paket doručen na cílovou adresu a hodnota TTL se dostala na nulu. Mezi informační zprávy lze zařadit známý příkaz ping pro zjištění dostupnosti a dalších parametrů sítě nebo uzlu.

Do protokolu ICMPv6 byly zabudovány některé bezpečnostní prvky, které definují např. minimální časovou prodlevu mezi jednotlivými zprávami nebo přidání šifrovacího mechanismu do zpráv. [4,5]

4.6 Objevování sousedů

V rámci protokolu IPv6 je nový mechanismus pro objevování sousedů v síti, tzv. ND (Neighbor Discovery). Obdobným mechanismem je v protokolu IPv4 protokol ARP, který překládá IP adresu a MAC adresu síťového rozhraní.

Systém objevování sousedů slouží ke zjišťování adres uzlů ve stejné lokální síti, k aktualizaci routovacích tabulek, ke zjišťování parametrů sítě a dalších údajů pro automatickou konfiguraci.

Pro svou funkci využívá pět druhů ICMP zpráv, a to ohlášení a výzva sousedovi, výzva a ohlášení routeru a přesměrování. Pro objevování sousedů využívá skupinové adresy. Na tuto skupinovou adresu odešle zařízení ICMP zprávu typu *výzva sousedovi* a pokud je zařízení aktivní a danou zprávu přijme, pak na ni odpoví ICMP zprávou *ohlášení souseda*. Tímto způsobem si routery uchovávají aktuální routovací tabulky s adresami svých sousedů. Pokud dojde ke změně, může zařízení vyslat ICMP zprávu s údaji, které se změnily. Tato zpráva dorazí všem uzlům s danou síťovou adresou, ty uzly, které mají uloženou původní adresu, si změní údaje ve své tabulce. Ostatní zařízení zprávu ignorují. [14]

V rámci objevování sousedů se systém snaží o průběžnou kontrolu dostupnosti sousedů, se kterými zařízení komunikuje. Toto probíhá pomocí ICMP zpráv rozesílaných na sousedy a pokud soused odpoví, pak je jasné, že je dostupný.

5 Problematika rozvoje IPv6

Díky překladu NAT je přechod na IPv6 velmi pozvolný a vzhledem k nekompatibilitě IPv4 a IPv6 nedochází ani k přechodu pouze na IPv6. Během vývoje tohoto protokolu vznikaly různé přechodové mechanismy, které by měly umožnit přechod na nový protokol za použití toho staršího.

5.1 Dual stack

Jedním z těchto mechanismů je tzv. Dual stack, což je v překladu dvojí zásobník, který umožňuje chod obou protokolů současně. Všechna zařízení v síti tak mají přidělenou IPv4 i IPv6 adresu a oba protokoly mohou být používány současně. Výběr verze protokolu je ponechán na konkrétním uzlu sítě dle preferencí.

Tento mechanismus je podporován u všech operačních systémů i zařízení, kde je samotná podpora protokolu IPv6. Patří k nejčastěji používaným přechodovým mechanismům a často se používá i s některým z tunelovacích mechanismů.

5.2 Tunelovací mechanismy

Pokud jsme v síti, kde funguje pouze IPv4, pak je potřeba použít tunelovací mechanismus. Tunel je způsob zabalení dat z jednoho protokolu do jiného, pro přechod na IPv6 je několik variant.

5.2.1 6in4

Pro tunelování se používá komunikace bod-bod a je potřeba oba body nakonfigurovat. IPv6 paket je zabalen, je přidána IPv4 hlavička a do verze protokolu se uloží hodnota 41.

Tento mechanismus je celkem jednoduchý, ale problém nastává při překladu NAT. Někdy také bývá blokován firewallem.

5.2.2 6to4

Tento tunel patří v dnešní době k nejrozšířenějším a jeho konfigurace probíhá automaticky. Používá adresy obsahující IPv4 adresu hraničního routeru sítě.

Využívá vyhrazeného prefixu 2002::/16, za který se připojí 32 bitů včetně IPv4 adresy routeru v dané síti, tímto vznikne prefix o délce 48 bitů, který lze použít pro adresování v síti. Tím pádem v síti lze používat IPv6 a hraniční router tuneluje provoz do IPv4.

Pro směrování do IPv6 sítí je zapojen zprostředkující router, který má podporu IPv4 i IPv6. Tyto routery mají nastavenou IPv4 adresu 192.88.99.1, aby byla zajištěna automatická funkčnost a IPv6 adresu 2002:c058:6301::.

5.2.3 ISATAP

Další z možných tunelovacích mechanismů je ISATAP, který slouží pro komunikaci uzlů na lokální síti, která nepodporuje IPv6.

V tomto mechanismu nefungují standardní mechanismy jako u IPv6, není tedy možné poslat oznámení routeru a tím i zaniká možnost objevování sousedů. Výzvy router zasílá na adresy potenciálních routerů, které může získat ruční konfigurací, z DHCP nebo DNS.

Uzel se pokouší od svých DNS záznamů získat IPv4 adresu. IPv6 adresu pak uzel vytvoří z prefixu podsítě připojením 16 nulových bitů a na konec 32 bitů své IPv4 adresy, ale jen v případě, že jde o neveřejnou adresu. V případě, že jde o veřejnou IPv4 adresu, pak dojde ke změně sedmého bitu, místo 0000 se dosadí 0200. Zbylých 16 bitů obsahuje konstantu 5efe.

5.2.4 Teredo

Tento mechanismus je poloautomatický. Na straně klienta je nutné nastavit adresu Teredo serveru, ten slouží k automatické konfiguraci. Tento server poskytne klientovi základní 64 bitový prefix, který se skládá z prefixu 2001::/32 a IPv4 adresy serveru.

Není potřeba veřejných IPv4 adres, je tedy skvěle využitelný pro sítě s překladem NAT. S ohledem na náročnost překonávání NATu při navazování každého spojení je Teredo zamýšleno až jako poslední řešení, když není žádná jiná cesta k IPv6.

5.3 Bezpečnost IPv6

Je také důležité nezapomenout na bezpečnost v rámci IPv6. Díky tomu, že nefunguje NAT a zároveň většina adres je veřejně přístupných, celá síť je tak náchylnější k útokům.

Jedna varianta bezpečnostního opatření je nastavení firewallových pravidel na hraničním routeru sítě. Lze nastavit pravidlo takové, aby zařízení v síti mohla přistupovat libovolně na zařízení ven ze sítě, ale ne zvenku dovnitř.

Další variantou je možnost použít NAT64, který lze použít pouze v případě, že je na síti nastaven některý z tunelovacích mechanismů. Funguje na podobném principu jako u IPv4, brána do vnějšího internetu je router s IPv4 adresou.

Je také možné pro zabezpečení použít protokol IPSec, který zajišťuje autentizaci a šifrování přenášených dat s využitím kryptografie. Podpora mechanismu IPSec je povinně požadována jako součást protokolu IPv6.

5.4 Zhodnocení

Prozatím všechny služby ani všechna zařízení nepodporují protokol IPv6. V operačních systémech Windows, kterým disponuje velká většina lidí, je tento protokol standardně vypnutý. V případě, že tedy někdo bude chtít vyzkoušet funkčnost tohoto protokolu, musí nejprve povolit protokol IPv6 a tam nastává první problém, jakou adresu zvolit, jak přesně si počítač nastavit. Pokud poskytovatel internetu má podporu IPv6, pak může klientovi rovnou přidělit IPv6 adresu. V případě, že podporu nemá, je potřeba zvolit některý z přechodových mechanismů.

Další problém nastává pro poskytovatele internetu, jakou variantu přechodu, případně tunelovacího mechanismu použít, jak zvolit adresní plán a také zařízení, která budou podporovat IPv6. Podpora IPv6 na routerech je v dnešní době jedna z největších překážek nasazení v domácích sítích.

Díky pomalému přechodu ani poskytovatelé služeb nebo správci webových stránek nepospíchají s podporou IPv6, tím pádem na hodně stránek stále nelze

přistupovat přes IPv6. Někdy jsou jen části na cestě podporující IPv6 a ostatní části nemají podporu vůbec nebo používají některý z přechodových mechanismů.

Jedním z dalších problémů při přechodu je bezpečnost IPv6, kdy je nutné si pohlídat firewall a pro poskytovatele to znamená na hlavním routeru nastavit pravidla tak, aby nešlo přistupovat do sítě a na počítače zvenku.

6 Návrh přechodu na IPv6

Testování jsem prováděla ve firmě LASCO s.r.o. Tato firma je poskytovatelem internetu v okrese Praha-východ, a v její síti je připojeno kolem 200 zákazníků. Všichni mají ve své domácnosti pro připojení k internetu použitý router Mikrotik, což umožňuje rychlou a bezproblémovou správu všech routerů v síti na dálku pomocí programu Winbox. [2]

6.1 Podmínky přechodu

Pro přechod na IPv6 je potřeba mít přidělený rozsah adres od nadřízeného poskytovatele. V tomto případě jsou adresy přidělené od GTS Novery. Další podmínkou přechodu musí být podpora protokolu IPv6 na všech zařízeních v síti. V případě, že některá zařízení nepodporují, je třeba je vyměnit nebo uvažovat o jiném řešení. V tomto případě je celá síť postavena na platformě Mikrotik, tzn. všechny routery v síti podporují protokol IPv6 a není tedy potřeba je měnit. Jako další zařízení je nainstalovaný linuxový server, který rovněž IPv6 podporuje. S prvky sítě tedy není problém a nebude potřeba vynaložit úsilí a finance na obměnu.

Další bod k zamyšlení je varianta přechodu, je nutné rozmyslet, zda lze použít paralelní chod obou protokolů současně nebo zvolit jinou variantu. Celá síť se musí konfigurovat za plného provozu a přechod je nutné vymyslet tak, aby konfigurace nenarušila provoz sítě. Je to síť provozovatele a poskytovatele internetového připojení, kde koncoví zákazníci jsou soukromé osoby, tudíž nejvhodnější varianta je paralelní chod obou protokolů současně tak, abychom neomezili provoz sítě a zákazníci tak nebyli bez služeb. Vzhledem k různorodým možnostem zařízení, co se týká zákazníků, je nasazení paralelního chodu vhodné.

Jednou z podmínek je také možnost vytvořit testovací prostředí, kde by se dala funkčnost IPv6 ověřit bez zbytečné ztráty připojení a omezení funkčnosti.

V neposlední řadě je návrh adresního plánu celé sítě s ohledem na budoucí rozvoj sítě.

6.2 Analýza současného stavu sítě

V současné době je síť společnosti LASCO celá postavena na protokolu IPv4.

Páteřní soustavu sítě tvoří jeden centrální router Mikrotik RB1000, který je připojen k nadřazenému poskytovateli a dále pak tři routery Mikrotik RB600 a RB435, které tvoří 7 základních páteřních WiFi spojů vnitřní sítě do různých lokalit. Druhý konec každého z těchto 7 hlavních páteřních spojů tvoří další routery Mikrotik RB600 a RB435, které současně slouží jako jednotlivé připojovací uzly (APčka) pro WiFi připojení koncových klientských stanic u zákazníků na domě v dané lokalitě. Tyto klientské jednotky, které jsou také ve správě firmy, jsou typu RB411, RB711, RBSXT, ap., všechny rovněž od výrobce Mikrotik. [2]

V několika lokalitách jsou vytvořeny další vedlejší spoje pro lepší vykrytí některých dalších míst, vše opět na stejné technologii.

Routery v celé síti jsou vybaveny bezdrátovými WiFi kartami, které podporují bezdrátovou WiFi technologii v pásmu 2.4GHz a 5GHz podle specifikace IEEE802.11abgn a mají také podporu přenosového protokolu „nstreme" a „nv2", což je vlastní protokol vyvinutý firmou Mikrotik pro zvýšení datové propustnosti spojů.

Všechny páteřní spoje jsou bezdrátové typu WiFi, pracují v pásmu 5GHz-A/N s použitým protokolem nv2. Připojovací uzly v jednotlivých lokalitách pracují převážně v pásmu 5GHz-A/N nebo 5GHz-A s použitým protokolem „nv2", některé z nich ještě v pásmu 2.4GHz-B/G také s protokolem „nv2". [2]

Centrální uzel obsahuje také server s OS Linux (Centos 7), který pro celou síť a zákazníky zabezpečuje další velmi důležité služby. Jsou to zejména DNS server, který zajišťuje překlad IP adres na doménová jména, zejména pro doménu lasconet.cz a lasco.cz včetně překladů reverzních. Další službou je SMTP server, který umožňuje provoz odchozí elektronické pošty pro celou síť a zákazníky. Dále POP3 server, který poskytuje přístup k poštovním schránkám pomocí POP3 klienta. K tomu se váže další služba týkající se elektronické pošty a to IMAP server, který poskytuje přístup k poštovním schránkám pomocí klienta IMAP. Také obsahuje HTTP server, který umožňuje provoz informačních www stránek pro poskytování služeb zákazníkům.

6.2.1 Adresní prostor IPv4

Adresní prostor IPv4 je v síti použit následujícím způsobem.

Síť 10.0.0.0/8 je neveřejná a je určena pro připojování klientských stanic v jednotlivých uzlech. Je rozdělena na subnety s maskou /16 pro jednotlivá rozhraní routeru podle lokalit. Například: 10.61.0.0/16 nebo 10.62.0.0/16 pro klienty připojované v lokalitě 6 na rozhraní wlan1 a wlan2. Router má například přiděleny adresy 10.61.0.1/16 pro wlan1 a 10.62.0.1/16 pro wlan2 a tvoří bránu pro klienty. Klienti pak mají IPv4 nastavenu např. takto: 10.61.35.1/16, 10.62.74.1/16, ap., kde třetí byte udává identifikátor (35,74) z podpůrného databázového systému pro evidenci zákazníků. Je tak zabezpečena poměrně dobrá orientace v IP adresách zákazníků a routování subnetů tak probíhá pouze v místní síti.

Síť 192.168.0.0/16 je také neveřejná, je určena pro nasazení v páteřních a vedlejších spojích. Je rozdělena na subnety s maskou /30 pro spoje typu bod-bod (2 IP adresy). Například síť 192.168.55.4/30 tvoří 2 IP adresy 192.168.55.5 a 192.168.55.6, které jsou přiřazeny příslušnému rozhraní konkrétnímu páru routerů tvořících daný spoj. Routování probíhá pouze v místní síti.

Síť 192.168.10.0/24 je neveřejná, je určena pro každou koncovou klientskou jednotku a je nastavena na vnitřním rozhraní jednotky u zákazníka. IP adresa 192.168.10.1/24 tvoří bránu domácí sítě zákazníka. Zde routování probíhá pouze v domácí síti zákazníka. Je zde použit překlad adres NAT, například: 192.168.10.0/24 -> 10.62.74.1.

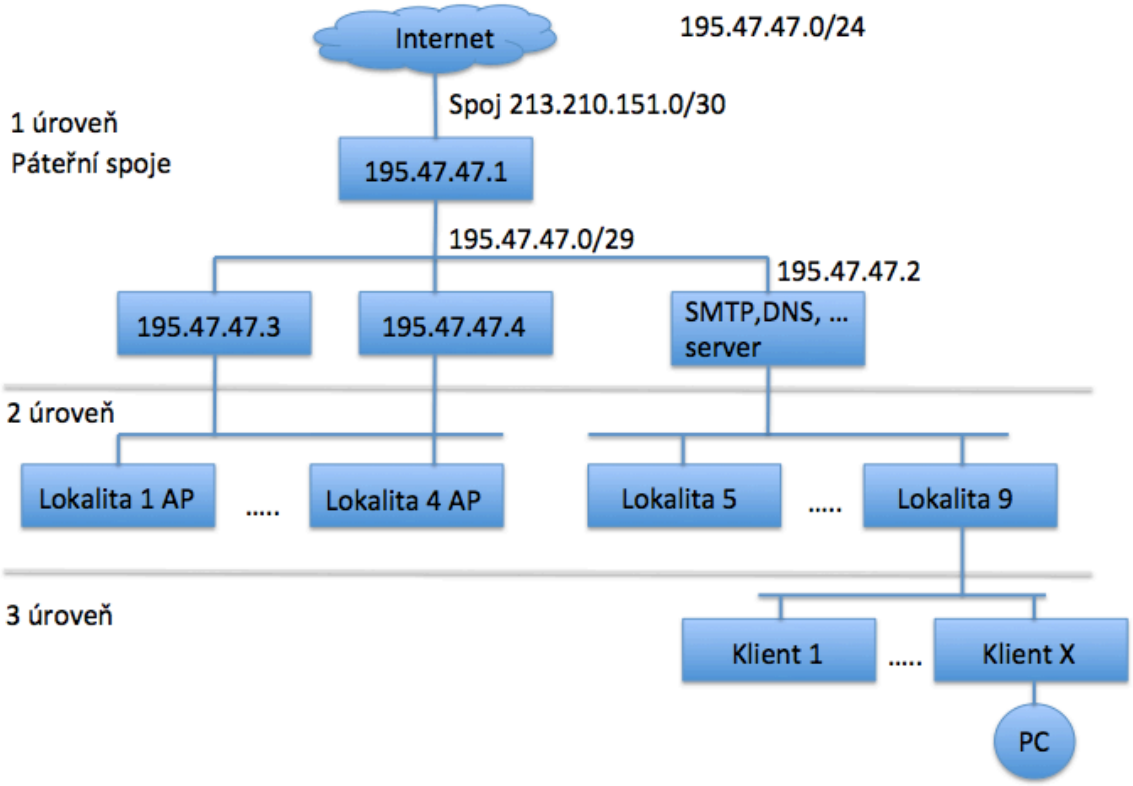
Síť 213.210.151.0/30 je veřejná, přidělená od ISP, určená pro konektivitu směrem k ISP. IP 213.210.151.1 je na spoji u ISP, IP 213.210.151.2 je nastavena na venkovním rozhraní centrálního routeru. Routování probíhá ze sítě a do sítě ISP pro veřejně sítě. Překlad adres NAT pro neveřejné sítě, například: 10.0.0.0/8 -> 213.210.151.2.

Síť 195.47.47.0/24 je veřejná, přidělená od ISP, slouží pro adresaci zařízení, která mají být „vidět ze světa". Je rozdělena na subnety s maskou /28 (/29) a dané subnety jsou použity pro adresaci některých páteřních routerů a pro adresaci

rozhraní v připojovacích uzlech pro eventuální přidělování zákazníkům. Například: 195.47.47.0/29 je použita pro adresaci centrálního uzlu celé sítě, 195.47.47.64/29 je použita pro adresaci zákaznických jednotek na připojovacím AP v dané lokalitě.

Stávající topologie sítě je orientačně znázorněna na obr 7.

Obr. 7 Rozvržení sítě IPv4



Zdroj: [vlastní]

6.2.2 Routování, RIP

Na všech routerech, kromě koncových routerů u klientů, je spuštěn routovací protokol RIP v.2, který je nakonfigurován tak, aby svým definovaným „sousedům" propagoval routovací tabulku pro svá vybraná rozhraní a své vybrané a připojené subnety. Centrální router navíc propaguje do okolí informaci o „default route", čili svoje statické pravidlo pro směrování „do světa", jinak také svoji výchozí bránu. RIP na všech zařízeních tak dynamicky upravuje routovací pravidla ve své routovací tabulce.

Koncové routery u zákazníků mají svoji výchozí bránu definovanou staticky jako adresu rozhraní APčka, ke kterému jsou připojeny. Například: 10.62.0.1.

6.2.3 NAT

Překlad IP adres NAT je v celé síti zprovozněn ve dvou úrovních. První úroveň NATu se používá v koncových jednotkách zákazníků, kdy je veškerý provoz z adres domácí sítě směrem do světa překládán na adresu jejich vnějšího portu: například 192.168.10.0/24 -> 10.62.74.1.

Druhou úroveň NATu tvoří pravidla na centrálním routeru, kdy provoz z veškerých neveřejných adres směrem ven ze sítě je překládán na veřejnou adresu svého vnějšího portu zhruba takto: 10.0.0.0./8 -> 213.210.151.2, 192.168.0.0/16 -> 213.210.151.2.

6.3 Adresní plán IPv6

Podobně jako v případě adres pro IPv4 bylo zažádáno u ISP o blok adres IPv6 s tím, aby byl co nejnižší prefix (alespoň /48), aby bylo k dispozici větší množství podsítí s prefixem /64 pro přidělování veřejných IPv6 adres zákazníkům.

Tento prefix délky /64 umožní pohodlné nastavení jejich domácích počítačů „autokonfigurací" podle principu EUI-64.

Podařilo se získat veřejný globální prefix 2001:af0:8047::/48 (*Obr. 18*). Tento prefix umožní základní strategii rozdělení na celkem až 65536 podsítí s prefixem /64 schematicky takto:

2001:af0:8047:0000::/64

2001:af0:8047:0001::/64

2001:af0:8047:0002::/64

...

2001:af0:8047:fffe::/64

2001:af0:8047:ffff::/64

Princip přidělování a využití IPv6 podsítí by kvůli srozumitelnosti a snazší správě měl odpovídat principům adresace IPv4. Stejně tak i topologie IPv6 by co nejvíce měla odpovídat topologii IPv4. Na všech rozhraních, která mají přidělenou adresu IPv4 musí mít analogicky přidělenou i adresu IPv6. Zda a jak to ve všech případech bude možné, bude zjištěno při vlastní realizaci a nastavení všech zařízení.

Rozdělením prefixu /48 na subnety s prefixem /64 získáme dvoubajtový prostor (16 bitů, 4hexa hodnoty 0-f) pro adresaci vnitřní sítě a přidělování veřejných prefixů /64 zákazníkům. Bude rozumné zvolit strategii přiměřené agregace podle stávající situace v prostředí IPv4.

V současné době je 7 páteřních spojů do různých lokalit, v každé je uzel AP s několika rozhraními pro připojování zákazníků, kterých je na každém jednotlivém rozhraní připojeno méně než 50. Z pohledu rozvoje sítě se prý neuvažuje o přílišném „zahušťování" klientů na jednotlivých rozhraních, zvyšování poptávky by se řešilo buď rozběhnutím dalšího rozhraní na daném routeru nebo zřízením dalšího AP uzlu. Důvodem je reálná propustnost a agregace na WiFi spojích.

Pokud bychom uvedených 16 bitů (čtvrtý blok mezi dvojtečkami zleva) rozdělili tak, aby první 4 bity označovaly lokalitu, druhé 4 bity označovaly rozhraní v lokalitě a dalších 8 bitů označovalo připojené zákazníky ke konkrétnímu rozhraní v lokalitě, pak by to schematicky mohlo vypadat následovně:

```
2001:af0:8047:1234::1/64
             ||||
             ||++-- koncová stanice v uzlu,  hodnoty 00-ff,  reálně spíše 01-ff, čili max. 255 zákazníků
             |+---- rozhraní,                hodnoty  0- f,  reálně spíše  1- f, čili max.  15 rozhraní
             +----- lokalita,                hodnoty  0- f,  reálně spíše  1- f, čili max.  15 lokalit
```

Tento princip by vypadal reálně asi takto, tedy například router běžného zákazníka s vnější privátní IPv4 adresou 10.62.74.1/16, který je připojen k AP uzlu 10.62.0.1/16 (jeho IPv4 brána) a má vnitřní domácí privátní subnet 192.168.10.0/24 (NAT), by mohl mít vnější IPv6 adresu např. 2001:af0:8047:6200::6274/64 a je připojen k témuž uzlu s IPv6 2001:af0:8047:6200::1/64 (jeho IPv6 brána), by mohl mít vnitřní domácí subnet IPv6 2001:af0:8047:6274::1/64.

Uvedené schéma IPv6 odpovídá strategii přidělování privátních adres v prostředí IPv4 a nikoliv veřejných adres v IPv4. Důvodem je nedostatek veřejných IPv4 adres a proto veřejné adresy principu vhodné agregace neodpovídají.

Navržené schéma je robustní a umožní i rozvoj sítě s dostatečnou rezervou volných IPv6 adres. Při praktickém nasazení se zjistí, zda tato strategie funguje.

Další důležitou otázkou je to, jak moc „plýtvat" veřejnými globálními adresami s prefixem /64 pro páteřní spoje nebo spoje mezi routery (dvoubodové spoje). Je zřejmé, že pokud bude potřeba testovat dosažitelnost routerů (zejména páteřních) i z vnější sítě, bude nutné veřejné adresy použít. V opačném případě by postačilo využití lokálních linkových adres (s prefixem fe80::/10), což ale není moc doporučováno, anebo použití místních lokálních adres (ULA) s prefixem fd00::/8, což je analogie použití privátních adres v IPv4, které se používají už nyní.

Další možností je použití sice globálních veřejných adres, ale s prefixem větším než /64, tedy jakési „naporcování" jednoho subnetu /64 na subnety menší, sloužící jako spojovací. Tato třetí možnost by prakticky mohla vypadat například takto:

Dvojice adres

2001:af0:8047:cc::6:1/112

2001:af0:8047:cc::6:2/112

by mohla adresovat spoj do lokality 6. Tento princip se zdá být s ohledem na místní podmínky nejčistší a pokud nebude problém s přidělováním velkých prefixů, bude použit.

6.4 Routování, RIPng

Analogicky k prostředí IPv4, kde je úspěšně nasazen protokol RIP v.2 bude nakonfigurován tentýž protokol ve verzi pro IPv6. Podle dokumentace všechna zařízení v síti podporují vzájemnou výměnu routovacích záznamů IPv6 v podobě nasazení protokolu RIPng, tak bude možné ho použít.

Vzhledem k tomu, že bude v síti IPv6 mnohem více subnetů, než v případě IPv4, bude nasazení dynamického routování naprosto nezbytným a důležitým prvkem nasazení IPv6. Nárust routovaných subnetů je daný nutností připojování veřejných subnetů jednotlivým koncovým zákaznickým jednotkám až na jejich vnitřní rozhraní, protože v IPv6 neexistuje princip překladu adres NAT, tak jak jej známe z IPv4. V IPv4 mají všichni zákazníci nyní přidělen privátní subnet a používají NAT. Pokud mají přidělenou veřejnou adresu, mají ji připojenu na svém vnějším rozhraní a dovnitř nastaven dst-NAT, forwarding portů, ap., což jsou individuálně nastavované vlastnosti a chování koncových jednotek v současnosti. V každém případě se vždy jedná o jedinou koncovou adresu IPv4 a nikoliv celý subnet, tak jak bude nutné očekávat v případě IPv6.

To znamená, že se stávající množství uvažovaných záznamů v routovacích tabulkách routerů, které nyní zahrnují pouze záznamy subnetů páteřních spojů a subnetů v připojovacích uzlech, patrně značně rozšíří o záznamy celých subnetů přidělovaných zákazníkům.

6.5 Automatická konfigurace, DHCPv6

Princip automatické konfigurace v prostředí IPv6 zůstane rovněž jako v případě IPv4 pouze koncovým zákaznickým jednotkám. Nyní v prostředí IPv4 je v nich nakonfigurován DHCP server, který směrem do vnitřního rozhraní (domácí sítě) přiděluje domácím počítačům dynamicky přidělovanou IPv4 adresu z daného rozsahu privátních adres a poskytuje další nezbytné informace pro správnou konfiguraci počítače v síti (např. IP DNS serverů, atd.).

U ostatních prvků sítě (páteřní spoje, uzly AP) je automatická konfigurace potlačena a veškeré IP adresy jakož i další potřebná nastavení jsou konfigurovány staticky.

Pro přidělení IPv6 adres domácím počítačům a zařízením, která jsou připojena v koncové zákaznické domácí síti, bude použita autokonfigurace pomocí EUI-64. U konfigurace páteřních spojů a uzlů AP budou adresy nastaveny staticky.

6.6 RA, ND

Čili "Router advertisement" a "Neighbor discovery" jsou nově definované principy výměny informací mezi sousedními routery v prostředí IPv6. Z teoretických podkladů je zřejmé, jak by měly fungovat, že například nahrazují použití protokolů ARP, RARP a některých funkčností ICMP protokolu IPv4, a dále mají velký význam zejména v případě autokonfigurace. Autokonfigurace by díky těmto novým protokolům měla být velmi jednoduchá.

Všechna použitá zařízení v síti nějakou formu nastavení těchto parametrů obsahuje. Je možné, že použití DHCPv6 v domácích sítích ani nebude potřeba, že „bezstavová konfigurace (SLAC)" bude plně dostačující.

6.7 DNS

V síti je umístěn linuxový server s OS Centos7, který pro celou síť mimo jiné slouží jako DNS server (BIND named). Je na něm konfigurováno několik domén, pro které zde existují příslušné DNS záznamy pro IPv4 (záznamy A) a jsou sem rovněž od ISP delegovány reverzní překlady adres IPv4.

Podle příslušné dokumentace by měl DNS server standardně podporovat oba protokoly a vlastní podpora IPv6 se umožní pouhou změnou „zónových" souborů tak, že se pouze dopíší adresní záznamy AAAA pro IPv6. Také se patrně budou muset upravit reverzní domény pro IPv6.

Zprovoznění DNS pro IPv6 by mohlo být relativně jednoduché. DNS server pro IPv6 by asi měl být zprovozněn co nejdříve, aby bylo možno již při testování používat čitelné záznamy místo dlouhých IPv6 adres.

Strategii nasazení IPv6 v tomto případě je možno souhrnně popsat takto. Plošné nasazení nativního IPv6 při zachování stávající struktury IPv4 (paralelní funkčnost obou protokolů). Shodná topologie IPv6 s topologií IPv4, pokud to bude možné (kde je adresa IPv4, bude i IPv6). Záměr použití veřejných globálních IPv6 adres s prefixem 2001:af0:8047:aaaa::bbbb:cccc/112 podle principů adresního plánu pro spoje mezi routery. Záměr použití veřejných globálních IPv6 adres s prefixem

2001:af0:8047:xxxx::/64 podle principů adresního plánu pro domácí sítě zákazníků. Statické přidělování adres IPv6 pro páteřní spoje, uzly AP a adresaci zákaznických jednotek. Dynamické přidělování adres IPv6 pro domácí sítě zákaznických jednotek (DHCPv6, SLAC autocfg.). Použití a konfigurace routování IPv6 pomocí RIPng. Konfigurace DNS pro IPv6.

7 Metodika testování

Všechna nastavování a následné testování budou prováděna na počítačích provozovatele sítě, které jsou připojeny uvnitř sítě a odkud se v současnosti celá síť spravuje. Z těchto počítačů se rovněž bude vzdáleně konfigurovat celá síť a všechna zařízení.

Veškeré konfigurace a testy budou probíhat vždy pod dozorem některého z techniků, aby bylo co nejvíce eliminováno riziko narušení nebo výpadku funkčnosti sítě.

Pro vzdálené nastavování všech routerů Mikrotik bude použit jejich program WinBox, pro potřeby vzdáleného připojení k serveru Linux bude použit oblíbený terminálový program PuTTY.

Cílovým stavem by měla být situace, kdy se bude možné z testovacího počítače připojit do internetu protokolem IPv6 a funkčnost protokolu IPv4 přitom nebude nijak narušena, čili budou fungovat oba protokoly současně.

Pro zjednodušení bude probíhat konfigurace prozatím pouze na zařízeních „po trase" a server Linux. Na nich bude odladěna základní funkčnost IPv6. Bude zajištěno spuštění protokolu IPv6, pokud ještě neběží, budou přiděleny IPv6 adresy podle adresního plánu a bude rozběhnut RIPng a DNS pro IPv6.

Pro otestování funkčnosti bude stačit konfigurace pouze na části sítě. V případě funkčnosti, pak není problém provést konfiguraci i ve zbylé části sítě, nasazení tak bude probíhat později.

Vzhledem k povaze konfigurací bude muset základní testování pravděpodobně probíhat průběžně.

Pro základní testování budou určitě použity standardní diagnostické programy obsažené ve všech systémech a těmi jsou zejména ping (ping6), tracert (traceroute, traceroute6), route (route -6).

Po zprovoznění základní trasy IPv6 směrem ven ze sítě, pak bude možné testovat dosažitelnost webových stránek pomocí IPv6, výkon a jeho srovnání s výkonem IPv4.

7.1 Jednotlivé body:

- nebude narušena funkčnost sítě, konfigurace bude probíhat za plného provozu
- konfigurace testovacího počítače, linuxového serveru a jednotlivých routerů
- přidělení IPv6 adres
- rozběhnutí RIPng a DNS pro IPv6 protokol
- testování pomocí ping a traceroute z hlavního routeru, z linuxového serveru a také z testovacího počítače
- testování funkčnosti DNS pomocí traceroute
- testování z PC na webové stránky (zároveň test DNS)
- testování rychlosti a tvoření statistik připojení

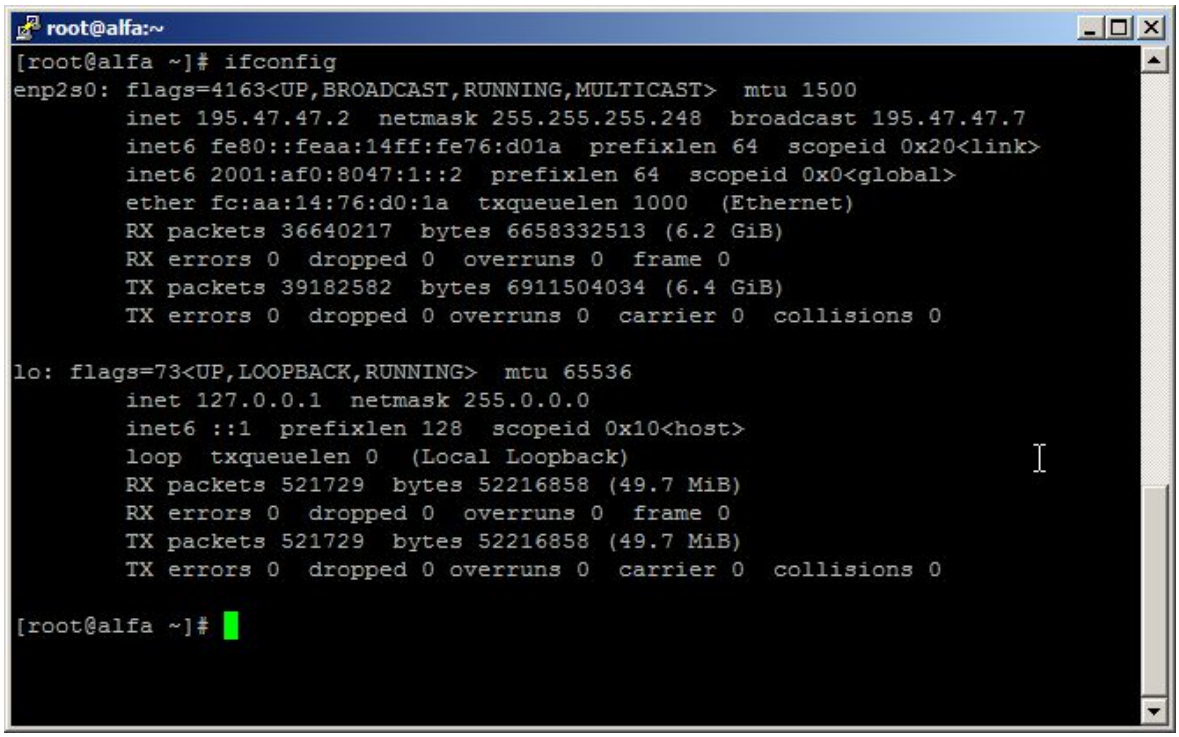
8 Výsledky testů a jejich zhodnocení

Základní spuštění IPv6 na routerech Mikrotik spočívalo v zapnutí balíčku IPv6, který je standardní součástí systému, ale je vypnut. (Byl zde nutný restart routerů, který proběhl v nočních hodinách, kdy je malý provoz v síti).[2]

Po restartu routerů se v ovládacím programu Winbox následně objevilo vždy samostatné menu pro nastavování parametrů IPv6 a dále pak několik nových možností v menu „Routing", například RIPng.

Současně se v seznamu IPv6 adres objevila vygenerovaná linková adresa s prefixem fe80::/10 pro každé z jeho aktivních rozhraní. V linuxu byl IPv6 již standardně spuštěn, příkazem ifconfig byla zjištěna přítomnost IPv6 adres. Na obrázku č. 8 je vidět základní nastavení síťové karty v linuxu.

Obr. 8 Nastavení síťové karty v linuxu



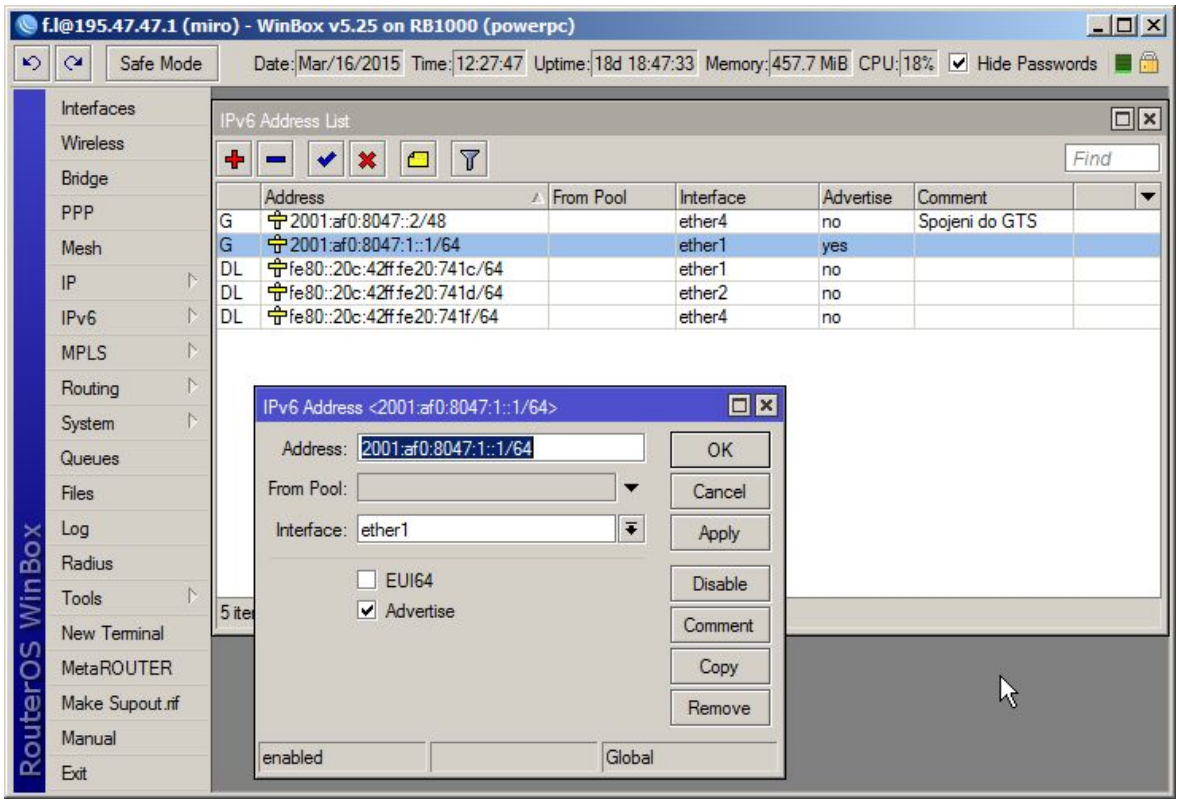
Zdroj: [vlastní]

Základní nastavování statických adres IPv6 na všech routerech Mikrotik po trase bylo poměrně jednoduché, a až na pár drobných příhod, kdy např. nefungoval ping na souseda a následně se zjistil překlep v adrese, vše probíhalo podle očekávání.

Na obrázku č. 9 je vidět příklad nastavení IPv6 adresy pro router Mikrotik v prostředí Winbox. Je zde nastavena adresa pro připojení k ISP, zároveň proběhlo testování, že se lze na adresu poskytovatele připojit (Obr. 19, Obr. 26, Obr. 29). Stejné testování pomocí ping a traceroute bylo provedeno i v linuxu (Obr. 35, Obr. 38).

Pro každou IP adresu tady lze nastavit EUI-64, což je automatická konfigurace s použitím MAC adresy síťové karty a Advertise, což je zprostředkování a propsání adresy do použitelných prefixů. Aby toto políčko mohlo být zaškrtnuté, pak musí být prefix adresy /64, pokud by byl zadán jiný prefix, pak Advertise nefunguje a do seznamu prefixů se musí zapsat ručně (Obr. 28). Dále bylo nutné nastavit ND (Neighbor Discovery), kde lze zaškrtnout propisování MAC adresy, podpora DNS atd. Nastavení je vidět na Obr. 27.

Obr. 9 Nastavení IPv6 adresy na Mikrotiku

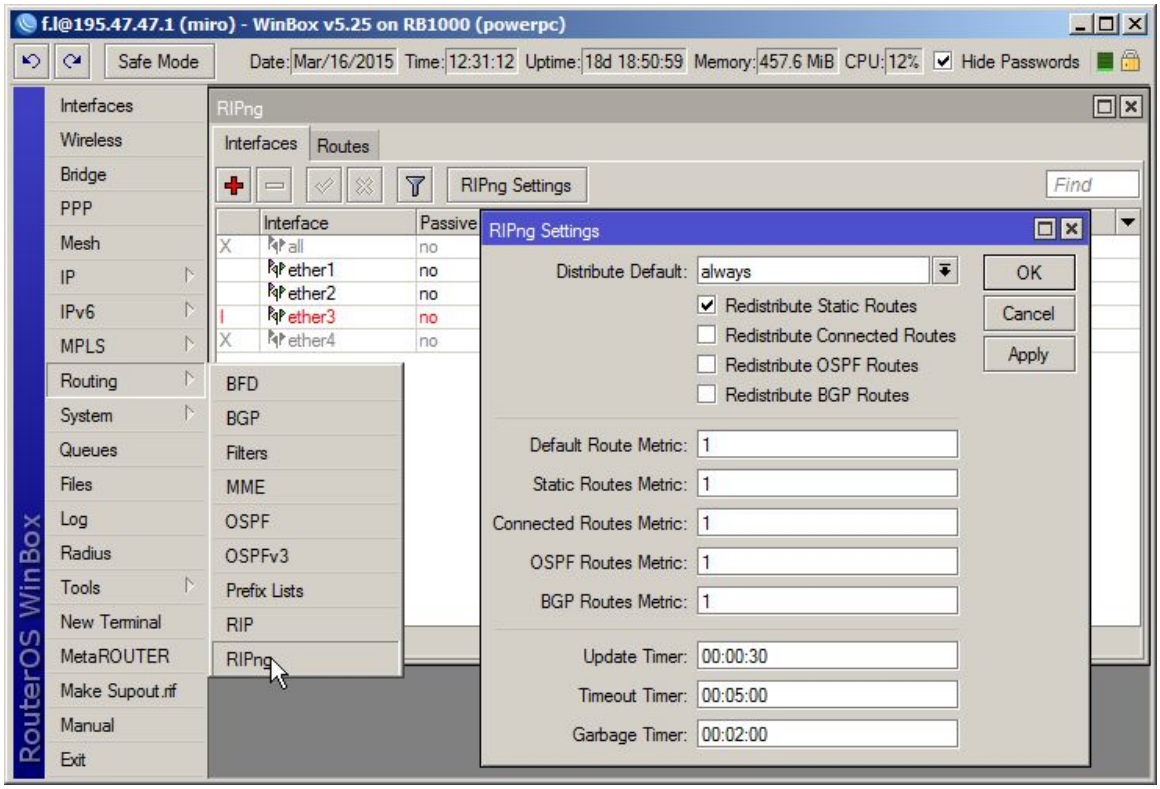


Zdroj: [vlastní]

Velmi brzo se ukázalo, že bude nutné spustit současně i RIPng kvůli testování trasy delší než jen k sousedovi. Proto byl spouštěn a nakonfigurován RIPng na routerech současně s přidělováním adres IPv6. RIPng byl nastaven vždy pro všechna

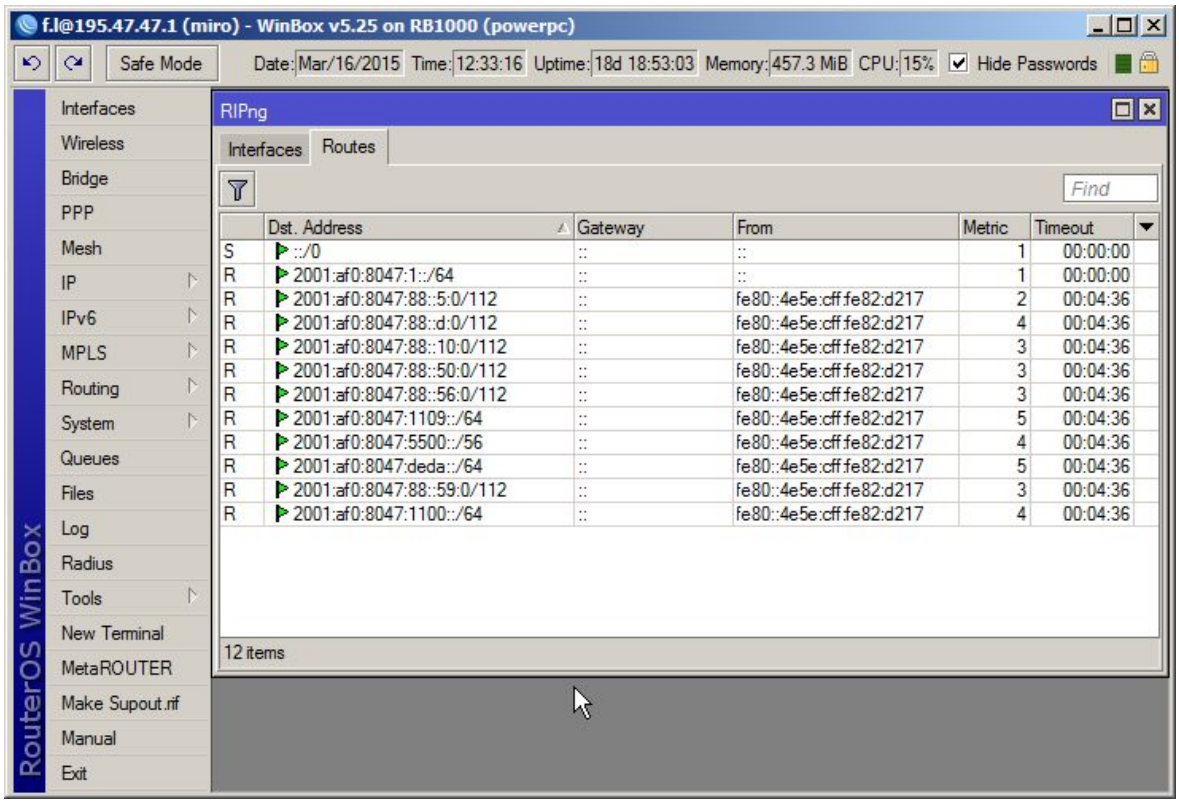
rozhraní daného routeru a stejně jako u IPv4 se ponechalo propagování „connected routes". V routovací tabulce se pak vždy objevily subnety okolních routerů se zapnutým RIPem (Obr. 10).

Obr. 10 Nastavení RIPng na Mikrotiku



Zdroj: [vlastní]

Obr. 11 Routovací tabulka



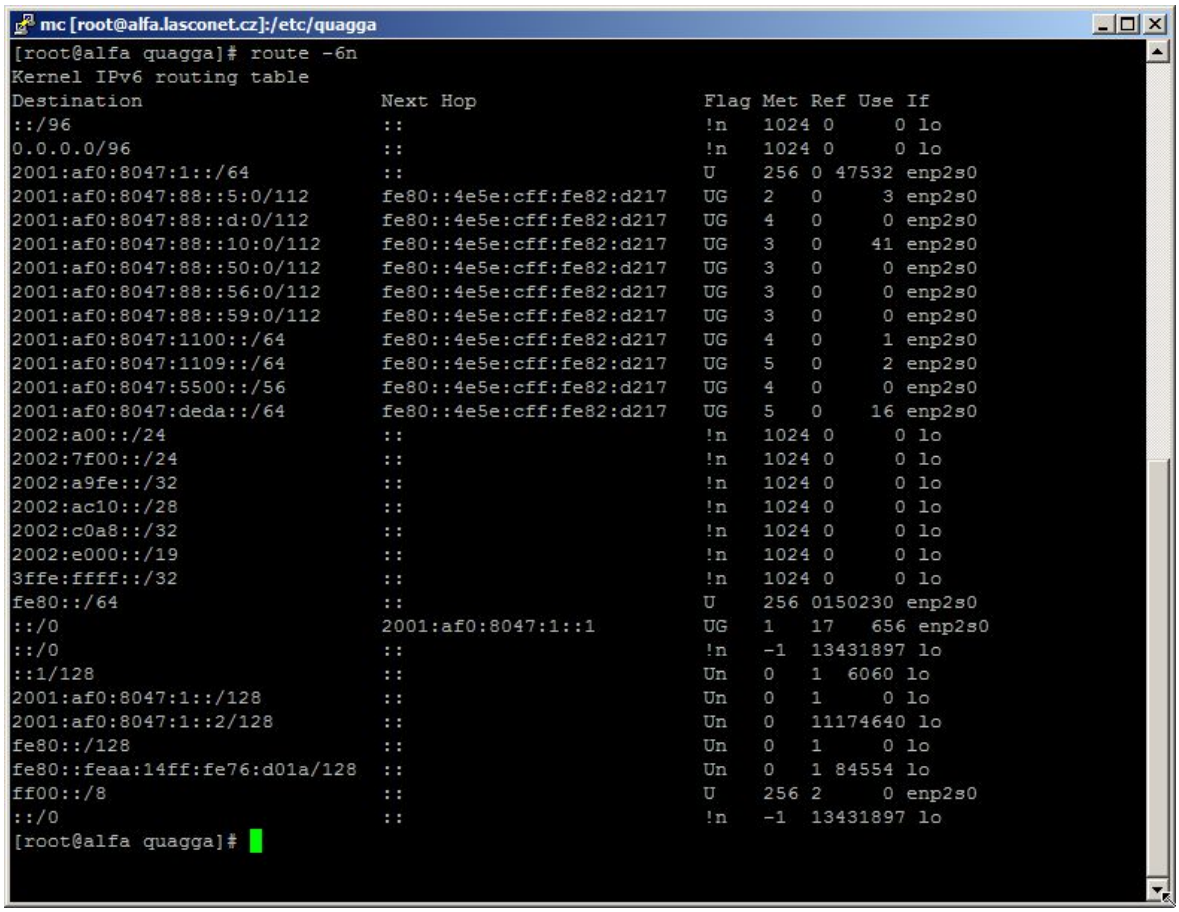
Zdroj: [vlastní]

V linuxu byla situace o něco složitější. Byla nastavena statická IPv6 adresa (Obr. 30) a byl spuštěn RIPng pomocí démonů Quagga (Zebra), který již úspěšně obsluhoval RIP pro IPv4. Výpis routovací tabulky však neobsahoval vše, co by RIPng od svých sousedů měl obdržet. Probíhalo několik různých pokusů s parametry v nastavení Zebry, ripngd, síťových konfigurací, atd. (Obr. 31, Obr. 32).

Po mnoha pokusech stále nic nového, linux nebyl schopen výměny routovacích tabulek se sousedy v síti. Nakonec se zjistilo, že je firewallem zakázán port 521/udp, na kterém RIPng komunikuje s okolím.

Po tom, co příkazy **firewall-cmd --add-port=521/udp –permanent** a **firewall-cmd –reload** byla povolena příslušná komunikace, se RIPng úspěšně rozběhl i na linuxu. Jeho routovací tabulka pak již správně obsahovala záznamy i od svých sousedů (Obr. 12).

Obr. 12 Routovací tabulka v Linuxu



Zdroj: [vlastní]

Poslední částí základní konfigurace bylo spuštění IPv6 na vlastním testovacím počítači. Je zde instalován OS Windows server 2008, který po aktivaci IPv6 na svém rozhraní v režimu autokonfigurace dynamicky přidělil sadu IPv6 adres pro všechna svá rozhraní. V prostředí Windows je standardně automaticky spuštěna možnost tunelování 6to4 pomocí tunelů Teredo nebo ISATAP a to i přesto, že je počítač připojen do prostředí nativního IPv6, což je tento případ. Proto byly tyto tunely vypnuty. Tuto službu poskytl příkaz netsh takto:

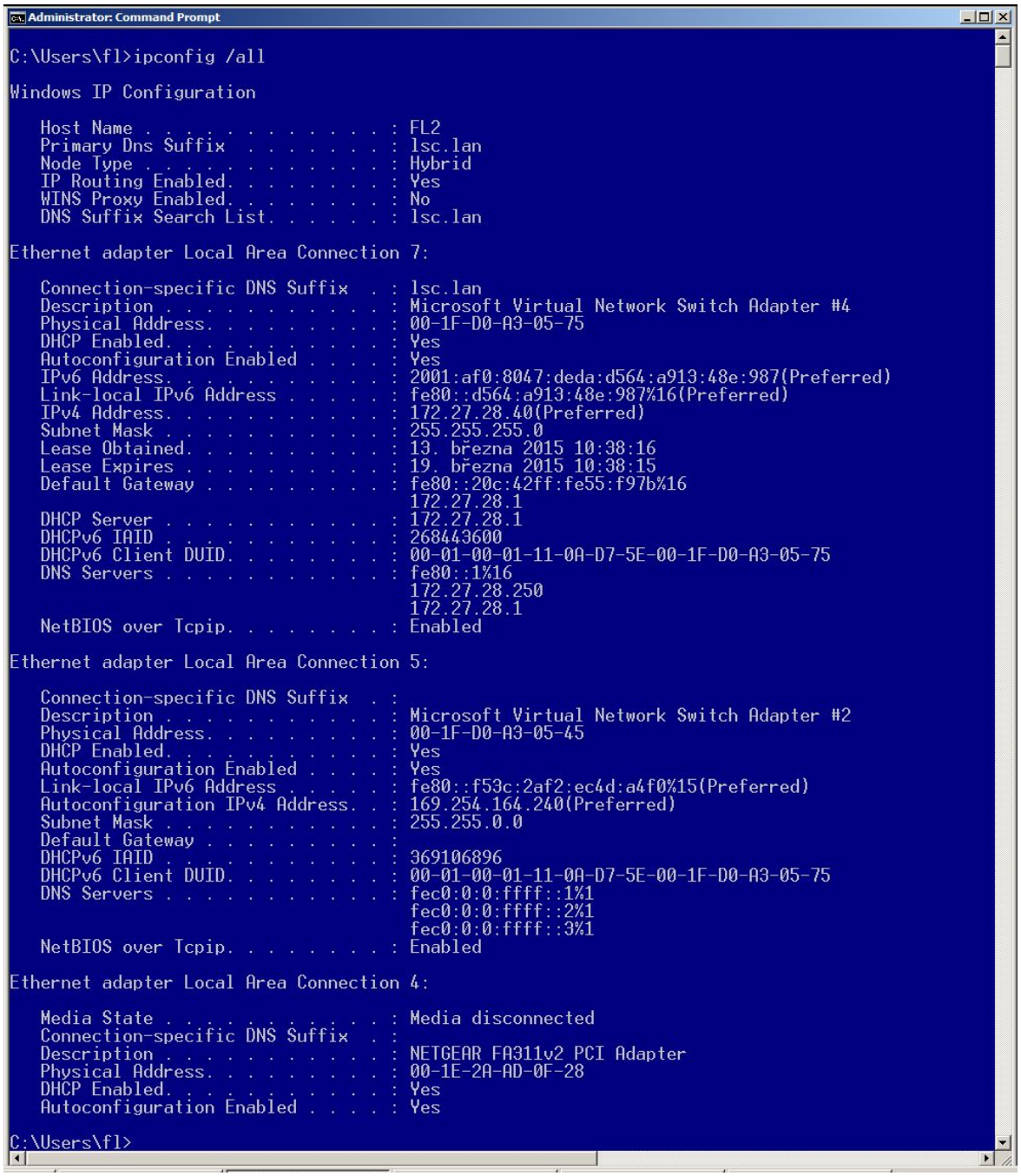
netsh interface 6to4 set state disabled

netsh interface isatap set state disabled

netsh interface teredo set state disabled

Příkazem ipconfig lze zjistit, že oba tunely opravdu zmizely, a zůstala jen standardní rozhraní.

Obr. 13 Nastavení síťové karty ve Win



Zdroj: [vlastní]

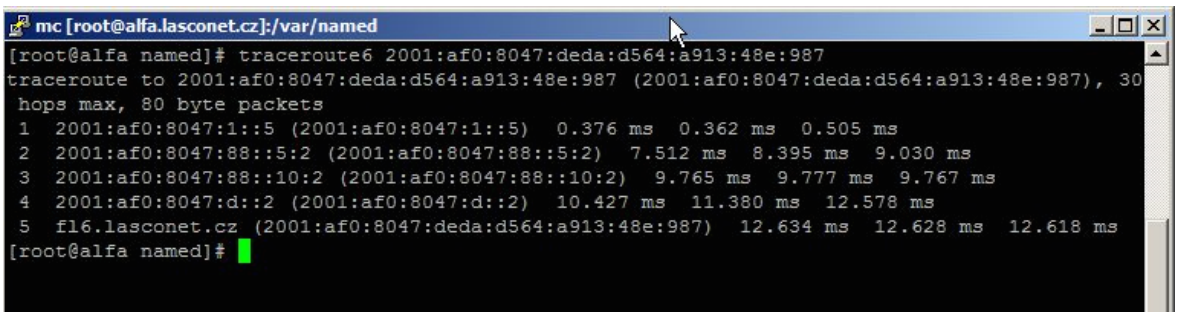
Po konfiguraci těchto základních částí začalo testování pomocí příkazů ping a traceroute z linuxového serveru, z počítače s WIN 2008 a také postupně z jednotlivých routerů po cestě. Program Winbox standardně podporuje ping

a traceroute na konkrétní IP adresu, jak pro IPv4 tak i pro IPv6, ale nepodporuje DNS záznamy pro IPv6. Proto bylo potřeba pro testování použít terminál, který je přímo implementovaný v prostředí Winbox.

Příkazy ping a traceroute pro ověření IPv6 adresy a zároveň ověření funkčnosti DNS serveru se musí zadávat jako **ping [:resolve alfa6.lasconet.cz]** přímo do terminálu, nelze zadat příkaz ping6 jako v linuxu nebo standardní ping ve windows. Testování je vidět na obrázkách (Obr. 20-25).

Na obrázku č. 20 je vidět základní ping z hlavního routeru na alfa6.lasconet.cz, což je linuxový server s jednotlivými službami. Na dalších dvou obrázkách je vidět ping na ipv6.google.com a na fl6.lasconet.cz, což je počítač s WIN 2008, ze kterého se testovalo. Do DNS záznamů byl přidán řádek se záznamem fl6 a IPv6 adresou počítače, aby byla možnost otestovat přístupnost a DNS server. Nastavení DNS záznamů je vidět na obrázku č. 33. Na obrázku č. 34 je také vidět nastavení reverzního DNS, kdy se zadává IPv6 adresa pozpátku, je nutné si dát pozor na nuly v adrese, které se vypustily. Na stejné adresy byl použit příkaz traceroute, toto je vidět na obrázkách č. 24 a 25. Dále bylo provedeno testování z prostředí linux opět pomocí příkazů ping a traceroute. Výsledky testů jsou vidět na obrázkách č. 36, 37, 39. Na obrázku č. 14 je vidět příkaz traceroute na adresu fl6.lasconet.cz, je zde vidět zohledněné reverzní DNS, ukazuje se jak doménové jméno, tak i IP adresa počítače. Toto platí pouze pro doménová jména, která jsou uložená včetně IP adresy v linuxu v souboru (Obr. 33).

Obr. 14 Traceroute na fl6.lasconet.cz s reverzní DNS z Linuxu

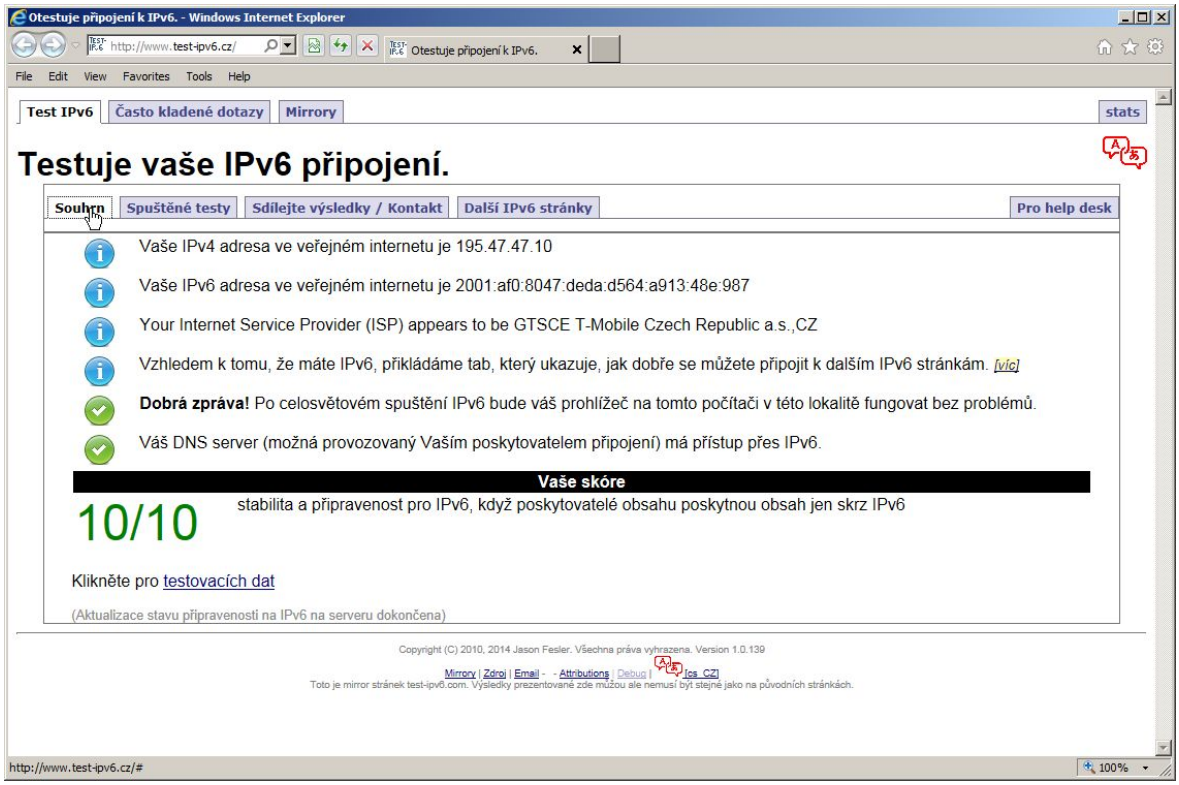


Zdroj: [vlastní]

V neposlední řadě bylo potřeba odzkoušet příkazy ping a traceroute také v prostředí windows na počítači. Toto testování je vidět na obrázkách č. 40 a 41.

Pro úplné otestování průchodnosti a funkčnosti v síti byl spuštěn internetový prohlížeč a proběhl test na stránky www.test-ipv6.cz, která slouží pro kompletní test IPv6 v síti (Obr. 15, Obr. 42). Na stránkách www.ipv6-test.com lze otestovat funkčnost připojení, poskytovatel připojení, rychlost a zároveň i test porovnání IPv4 a IPv6 (Obr. 43 - 46).

Obr. 15 Souhrnný test IPv6



Zdroj: www.test-ipv6.cz [13]

Pro otestování rychlosti jsme použili stránky www.ipv6-test.com. Lze zde nastavit, na jaký testovací server se má připojit a otestovat rychlost. Byl proveden test pro tři různá města a pro každé dvacet měření. Výsledky testů najdete v Tab. 1. Všechny naměřené hodnoty jsou v Mbit/s.

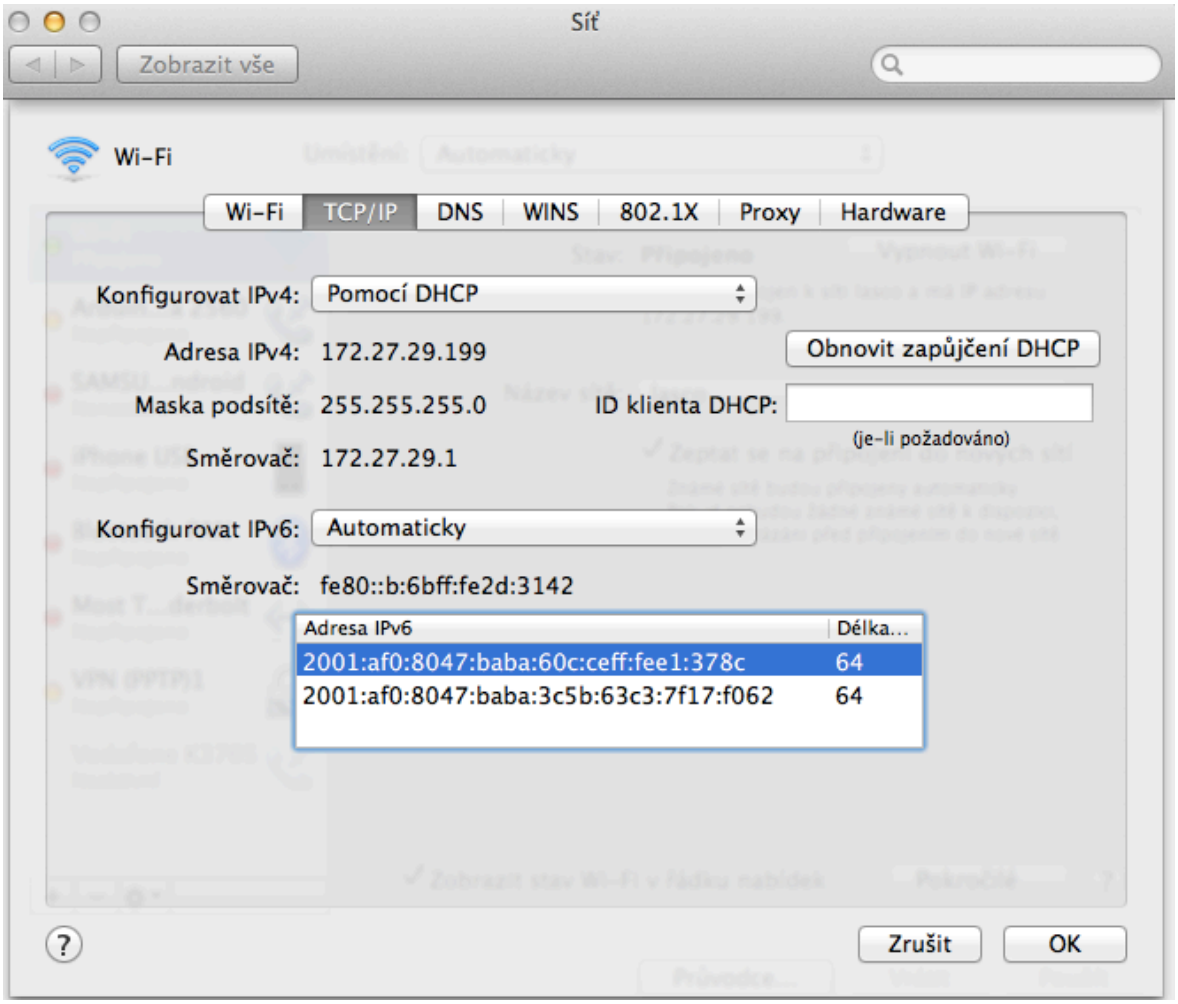
Tab. 1 Testování rychlosti

	UK Portsmouth		FR Roubaix		RU Bukurešť	
	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
1	6,84	5,71	11,1	6,57	7,3	5,32
2	8,32	7,05	9,41	4,75	6,89	6,24
3	4,14	3,76	7,31	4,47	7,1	7,87
4	4,91	5,21	9,63	6,19	8,63	7,66
5	5,79	4,25	7,4	5,77	7,14	6,61
6	6,03	9,09	9,59	8,7	8,31	6,87
7	5,96	5,29	11,5	4,56	8,78	4,84
8	6,49	5,54	12,1	11,2	4,89	5,43
9	6,98	6,55	12,6	4,88	5,74	6,73
10	6,5	6,61	12,7	7,24	5,12	5,73
11	8,56	4,9	6,63	5,66	7,03	9,69
12	6,27	6,77	13,2	7,38	6,24	5,61
13	6,37	9,19	8,19	6,12	5,64	6,28
14	8,06	4,45	8,93	5,07	3,87	4,93
15	4,41	7,76	10,2	5,42	4,56	4,2
16	7,4	5,21	9,39	5,63	5,54	6,75
17	6,2	5,04	9,57	7,44	5,01	6,62
18	7,27	5,59	5,78	6,42	4,85	7,67
19	6,82	5,9	10,5	5,49	7,29	4,82
20	4,56	5,52	8,13	6,79	4,96	4,69
Průměr	6,394	5,9695	9,693	6,2875	6,2445	6,228

Po všech testech z prostředí Linux, Windows i Mikrotik bylo ještě možné otestovat připojení k místní síti prostřednictvím wifi ve firmě na notebooku s operačním systémem Mac OS 10.9. Pro síťové rozhraní, na kterém je firemní wifi síť bylo nutné povolit přidělení IPv6 adres. Po pár pokusech se povedlo získat IPv6 adresu a připojit se na internet. Na *Obr. 16* je vidět nastavení a přidělená adresa na notebooku s operačním systémem Mac OS, takto se povedlo otestovat další operační systém. V podstatě u Mac OS se nemusí nic speciálně nastavovat, jen povolit automatickou konfiguraci IPv6. Obrázek skvěle slouží i pro ilustraci mechanismu EUI-64.

MAC adresa mého notebooku je 04:0c:ce:e1:37:8c a výsledná IPv6 adresa je 2001:af0:8047:baba:60c:ceff:fee1:378c.

Obr. 16 IPv6 adresa na MAC OS



Zdroj: [vlastní]

Opět bylo otestováno připojení pomocí příkazů ping a traceroute na adresu ipv6.google.com z posledního operačního systému. Na obrázkách č. 47 a 48 jsou tyto dva příkazy a výsledky vidět.

8.1 Zhodnocení testů

Vzhledem k tomu, že testování dostupnosti internetu po protokolu IPv6 bylo prováděno průběžně, tak při finálním testování byla zaměřena pozornost spíše na kvalitu připojení IPv6. Proběhlo i srovnání obou protokolů tam, kde to bylo možné. Opakovaně byla měřena rychlost připojení k několika serverům, které podporovaly měření pro oba protokoly. Výsledky jsou přehledně vidět v tabulce č. 1.

Z měření vyplynulo, že reálná rychlost IPv6 v několika případech byla vyšší než u IPv4, ale ve většině případů byla rychlost vyšší u IPv4. Tato skutečnost je překvapením, protože vzhledem k teoretickým předpokladům bylo očekáváno, že provoz po IPv6 bude obecně rychlejší než po IPv4. Čím je to způsobeno, je možné pouze spekulovat. Možná je protokol IPv6 nebo jeho implementace na různých zařízeních po trase ještě nedokonalá. Je možné, že ISP ve svých konfiguracích preferují IPv4 před IPv6 nebo pro IPv4 přidělují větší přenosovou kapacitu než pro IPv6. Rovněž je možné, že ISP používají nějakou formu tunelování, nebo pakety putují k cíli jinými cestami pro IPv4 a jinými pro IPv6. Toto všechno by mohly být důvody degradace reálných přenosových rychlostí po IPv6.

Padla i otázka, zda není problém na straně firemní sítě. Proběhly proto srovnávací rychlostní testy s použitím vestavěného programu BandwidthTest mezi nejbližším routerem a hraničním routerem celé sítě pro oba protokoly. Dosažené rychlosti pro oba protokoly byly srovnatelné, usuzuji, že uvedený problém se nachází spíše za hranicí firemní sítě směrem k cílovým testovaným serverům.

Všechny testy proběhly úspěšně, povedlo se připojit ze všech zařízení na internet na stránky ipv6.google.com, povedlo se příkazem ping a traceroute ze všech systémů ověřit dostupnost těchto stránek. A povedlo se také otestovat DNS server na linuxovém serveru a přidělení IPv6 adres v místní wifi síti.

9 Doporučení

S ohledem na zkušenosti s implementací IPv6 a následné výsledky testování IPv6 v reálných podmínkách se objevilo několik otázek. Jedna z otázek by mohla být, zda je vůbec nutné na IPv6 přecházet když se ukazuje, že zatím není v praxi rychlejší než IPv4? Obecně se zdá, že zatím nikoliv, ale pokud bude do budoucna potřeba vlastnit více veřejných IP adres, pak nebude jiné řešení.

Není nutné s přechodem na IPv6 moc spěchat, důležité je se velmi dobře připravit a důkladně promyslet nasazení v celé síti a připravit současnou infrastrukturu na přechod k IPv6.

Teoreticky se IPv6 jeví jako lepší protokol, nabízí oproti IPv4 nové možnosti, ale zatím není ani výrobci hardwaru tak dobře a masivně podporován jako IPv4. Velmi pravděpodobně se jedná o přechodný stav a v budoucnosti se bude podíl IPv6 zvyšovat.

Velmi důležitým aspektem při přechodu na IPv6 je podpora tohoto protokolu na současných zařízeních a případně nutná výměna. Při výběru síťových prvků s podporou IPv6 je důležitý i odhad toho, jak se výrobci vypořádají s vývojem a podporou IPv6 ve svých výrobcích. V současné době levné výrobky nepodporují IPv6 a přestože někteří výrobci propagují funkčnost tohoto protokolu, ne vždy podpora odpovídá předpokladům.

Proto bych doporučila vybírat pouze kvalitní, i když momentálně dražší výrobky od kvalitních společností jako jsou Cisco, Mikrotik apod. Z vlastní zkušenosti s nasazením a podporou v případě společnosti Mikrotik, mohu tuto firmu jen doporučit, mají kvalitní síťové prvky, které protokol IPv6 plně podporují.

Co se týká operačních systémů, v dnešní době již není problém s nasazením IPv6 jak u Windows, u Linuxu, tak ani u MAC OSX. Z vlastních testů jsem ověřila, že nastavení v jednotlivých systémech není tak složité a z obrázků je vidět, že IPv6 protokol podporují.

Dalším bodem k zamyšlení je konkrétní varianta přechodu na IPv6. Díky tomu, že firemní síť je poskytovatele internetu, byla jediná možná volba přechodu paralelní chod obou protokolů tak, aby nedošlo k výpadku služeb pro koncové zákazníky.

Myslím, že tato varianta je nejlepší i pro nasazení v jiných podmínkách. Vzhledem k tomu, že spoustu stránek a serverů zdaleka nepodporuje protokol IPv6 a bude ještě nějakou dobu trvat, než firmy na tento protokol přejdou, je tato varianta nejšikovnější. Není problém si nastavit protokol IPv6 v síti a tam, kam se dá dostat přes tento protokol, tak to bude fungovat a tam, kde ještě není podpora, tak bude stále fungovat IPv4. Ještě je možnost tunelování, ale to bych doporučovala spíše tam, kde je z nějakého důvodu nainstalovaný operační systém, který ještě nepodporuje protokol IPv6 nebo také například síťové tiskárny, kamery a podobná zařízení, která nemusí mít tuto podporu.

V případě rozhodnutí pro přechod je také důležité promyslet, zda adresování bude probíhat dynamicky nebo staticky. Lze použít obě varianty, stejně tak, jako u IPv4. Pro koncové stanice bych ponechala automaticky konfigurované IPv6 adresy, které jsou vygenerované pomocí EUI- 64 z MAC adresy. Je lepší využít tento mechanismus než DHCPv6, který není zdaleka tak kvalitní jako v případě IPv4. Pro ilustraci mechanismu EUI-64 a automaticky generované adresy krásně slouží obrázek vygenerované IPv6 adresy v systému MAC OS (Obr. 16).

Pro páteřní spoje je lepší využít statické adresy, umožňuje to mnohem lepší přehlednost a zároveň možnost dát konkrétní adresy tak, aby v tom byl určitý systém. Je dobré věnovat více času na promyšlení adresního plánu, aby nebyla nutnost to několikrát měnit a komplikovat si tak práci.

Pro shrnutí protokol IPv6 doporučuji, ale je nutné si velmi dobře promyslet všechny aspekty návrhu pro přechod. V případě, že bude potřeba vyměnit více prvků v síti, je nutné počítat s většími náklady. Prozatím není tak velká podpora IPv6 a tak bych doporučovala spíše postupný plynulý přechod.

10 Závěr a ekonomické zhodnocení

Cílem této práce bylo navrhnout a realizovat přechod na protokol IPv6 u komerčního poskytovatele připojení. Bylo nutné zjistit všechny potřebné informace, provést analýzu současného stavu sítě a navrhnout model přechodu tak, aby co nejvíce vyhovoval možnostem firmy. V průběhu roku firma zažádala o rozsah IPv6 adres od nadřízeného poskytovatele a bylo nutné navrhnout adresní prostor s ohledem na budoucí rozvoj sítě.

Všechny potřebné informace jsem shromáždila, provedla jsem analýzu a následně jsem začala promýšlet, jak přejít na nový protokol co nejsnadněji a za minimálních nákladů navíc.

Vzhledem k tomu, že celá struktura firemní sítě je postavena na platformě Mikrotik a všechna tato zařízení podporují IPv6, nebylo potřeba žádná zařízení měnit a tím nevznikly žádné další náklady. Routery od firmy Mikrotik byly ve firmě již od začátku poskytování služeb nasazovány až ke koncovým zákazníkům do domácností. Již od počátků tedy byla možnost rozšíření pro protokol IPv6. V případě nasazení tohoto protokolu a výměny některých zařízení by se náklady mohly vyšplhat až na několik desítek tisíc a s touto investicí musí firma před přechodem počítat.

Vzhledem k tomu, že firma LASCO je poskytovatel internetového připojení a konfigurace probíhaly za plného provozu, bylo potřeba vymyslet formu přechodu tak, aby nebyly omezené služby zákazníkům a provoz sítě. Nejvhodnější forma přechodu tedy byla paralelní chod obou protokolů současně.

Současný stav sítě mi tedy umožnit konfigurovat jednotlivé routery a testovací počítač ve firmě již od základu. Byl nasazen nový linuxový server, na kterém bylo potřeba nastavit DNS záznamy a další služby poskytované zákazníkům jako jsou SMTP, POP3, IMAP a HTTP server. Po konfiguraci serveru jsem prováděla nastavení adres na jednotlivých routerech a na testovacím počítači. Povedlo se nakonfigurovat všechna zařízení na trase mezi počítačem a internetem tak, abych mohla otestovat průchodnost a funkčnost tohoto protokolu.

Provedla jsem testy průchodnosti z testovacího počítače na hlavní firemní router, na všechny routery po trase, na síť nadřazeného poskytovatele a na linuxový server. Tyto testy proběhly také z linuxového serveru a z hlavního routeru. Takto jsem otestovala průchodnost všemi směry. Dále jsem testovala DNS server včetně reverzních záznamů.

Ke konci testování jsem ještě zkoušela připojení v rámci firemní wifi sítě z notebooku s operačním systéme MAC OS. Testování tedy proběhlo na všech platformách. V závěru jsem otestovala rychlost připojení přes oba protokoly a provedla jsem srovnání.

Testování proběhlo na části firemní sítě, kde jsou nyní nastavené IPv6 adresy a struktura je připravena tak, aby se v budoucnu mohly rozšířit i na další zařízení až ke koncovým zákazníkům.

Na základě teoretických znalostí a informací jsem si mohla ověřit platnost a funkčnost protokolu IPv6 v reálné firmě za reálných podmínek provozu. Teoretický předpoklad se potvrdil a já jsem si tak ověřila, že vyhledané informace jsou platné.

Seznam literatury

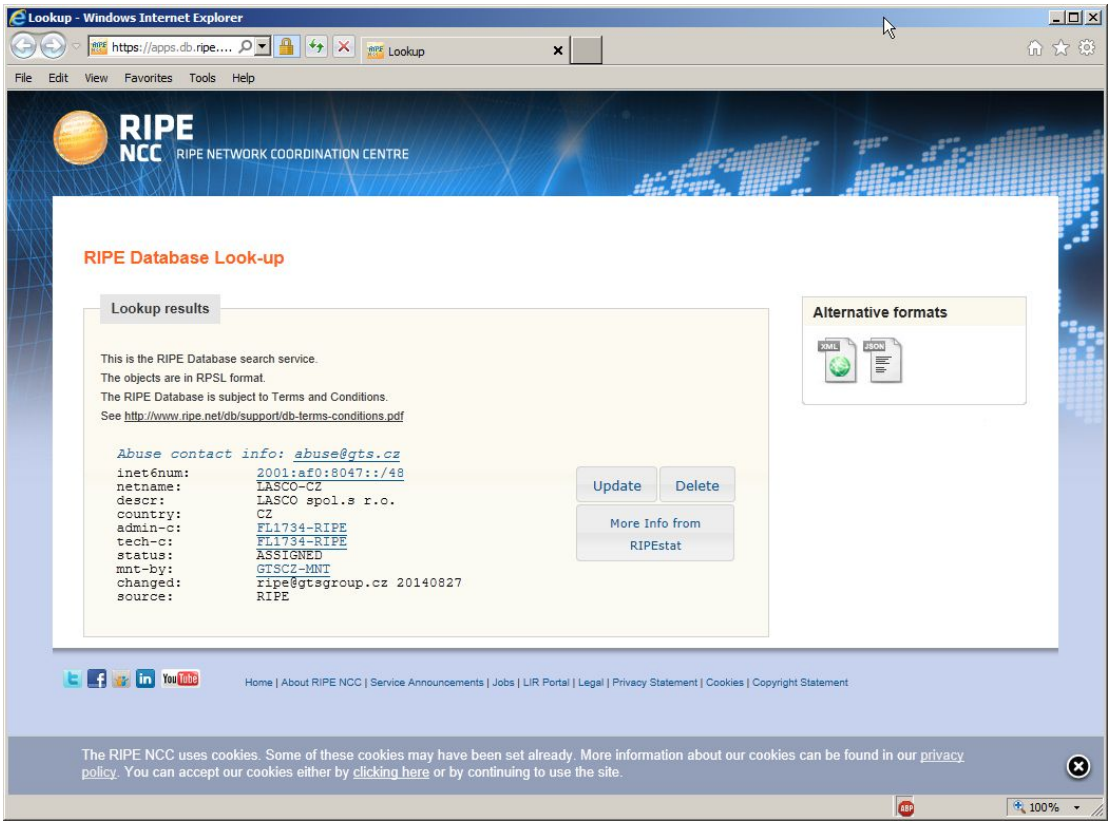
1. APRIAS, R.; KUČA, M. *Cisco PIX Firewall* [online]. Dostupný z WWW: <http://www.cs.vsb.cz/grygarek/TPS/projekty/0405Z/PIX/pix.html>.
2. *Manual:TOC*[online]. 2014 [cit. 2014-11-04]. Dostupný z WWW: <http://wiki.mikrotik.com/wiki/Manual:TOC>.
3. *Víte jak pracuje router?* [online]. 2010 [cit. 2010-6-23]. Dostupný z WWW: <http://www.samuraj-cz.com/clanek/vite-jak-pracuje-router/>.
4. DEERING, S.; HINDEN, R. Internet Protocol, Version 6 (IPv6). The Internet Engineering Task Force [online]. 1995, RFC 1883, [cit. 2011-09-19]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc1883.txt>.
5. DEERING, S.; HINDEN, R. Internet Protocol, Version 6 (IPv6). The Internet Engineering Task Force [online]. 1998, RFC 2460, [cit. 2011-09-19]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc2460.txt>.
6. PODERMAŃSKI, T. Lupa.cz [online]. 2011 [cit. 2011-09-19]. IPv6 Mýty a skutečnost. Dostupné z WWW: <http://www.lupa.cz/autori/tpoder/>.
7. [obrázek]. Dostupné z WWW: <http://www.access.feld.cvut.cz>.
8. [obrázek]. Dostupné z WWW: <http://www.access.feld.cvut.cz>.
9. [obrázek]. Dostupné z WWW: <http://www.ipv6.cz>.
10. [obrázek]. Dostupné z WWW: <http://www.ipv6.test.com>.
11. [obrázek]. Dostupné z WWW: <http://www.ipv6-test.com>.
12. [obrázek]. Dostupné z WWW: <http://www.wikimedia.org>.
13. [obrázek]. Dostupné z WWW: <http://www.test-ipv6.cz>.
14. SATRAPA, P. IPv6 : Internetový protokol IPv6. 3. dopl. vyd. Praha : CZ.NIC,z.s.p.o., 2011. ISBN 978-80-904248-4-5.

Seznam obrázků

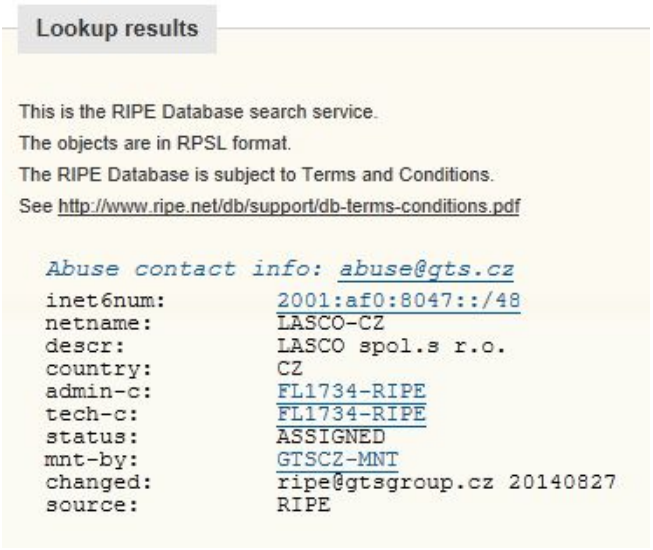
Seznam tabulek

Příloha

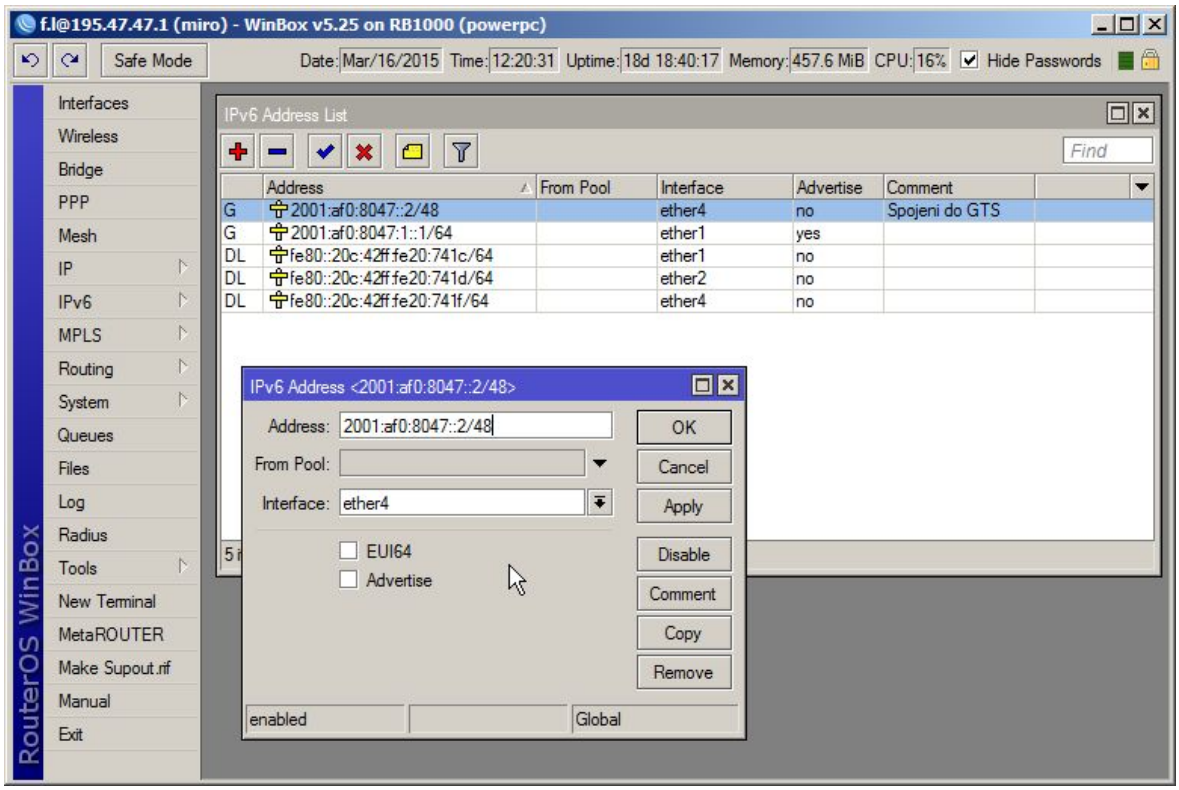
Obr. 17 Výpis přiděleného prefixu- RIPE



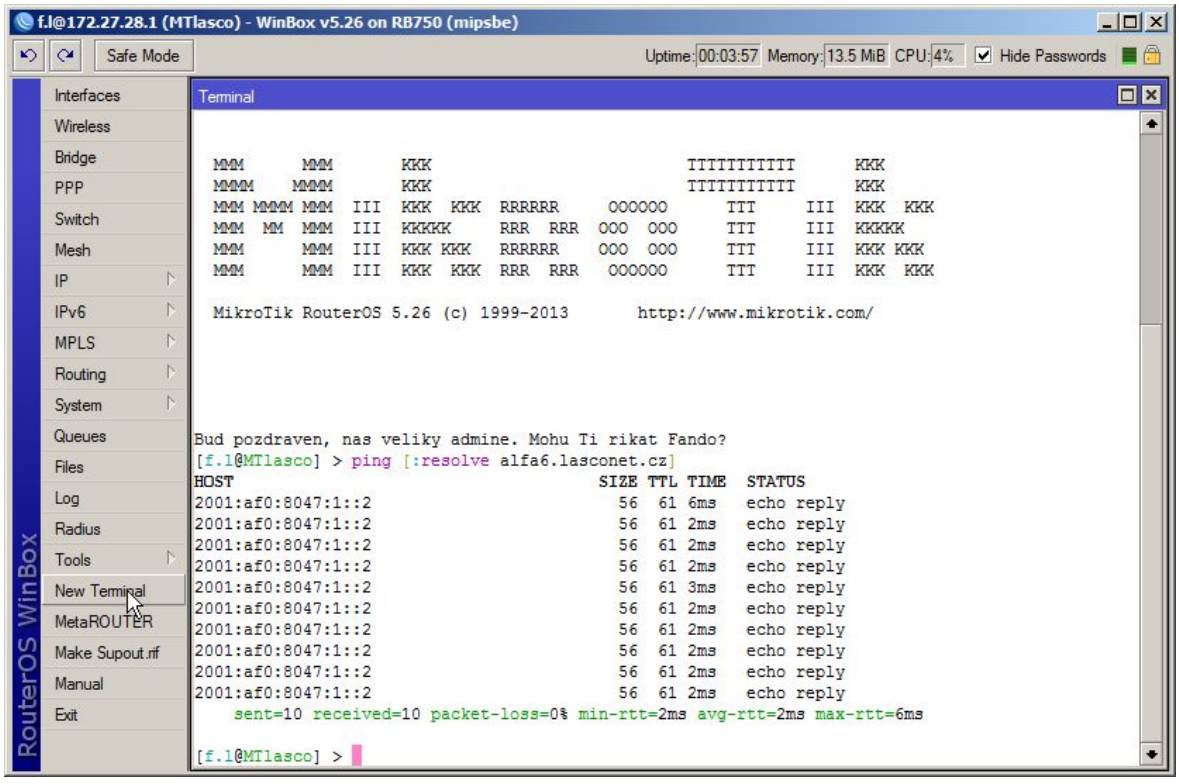
Obr. 18 IPv6 prefix pro LASCO



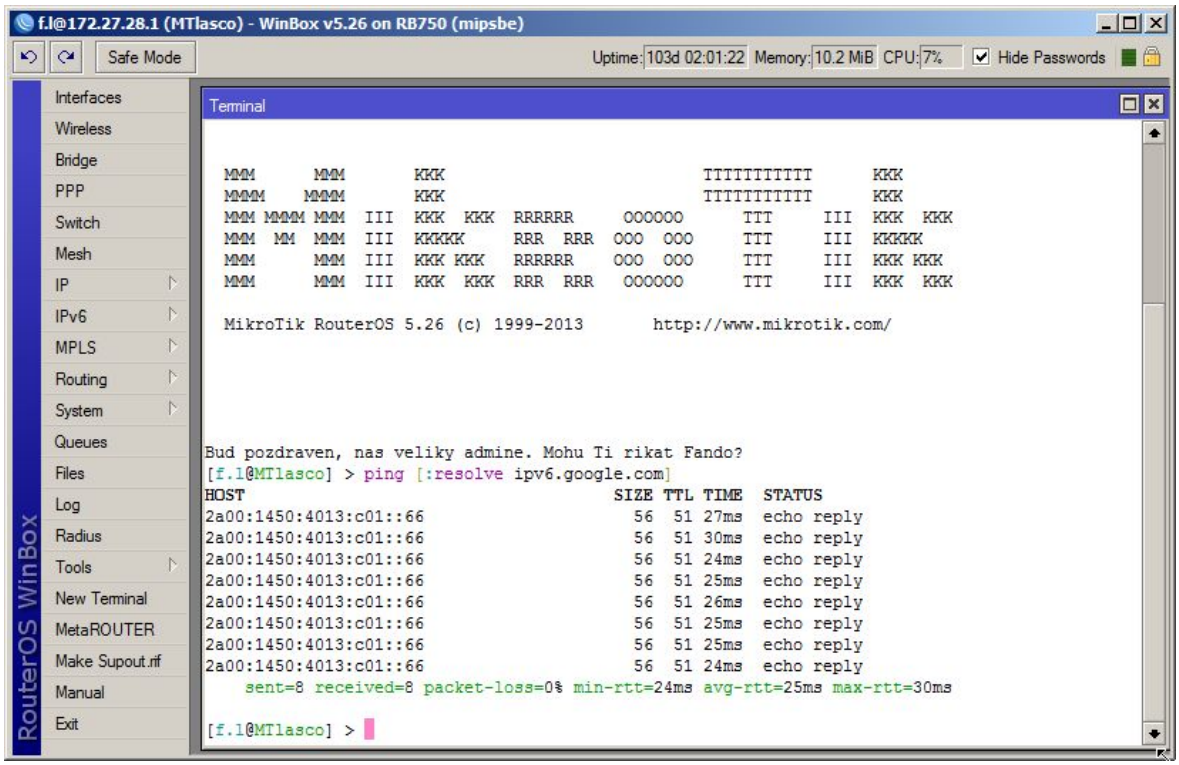
Obr. 19 IPv6 adresa k ISP



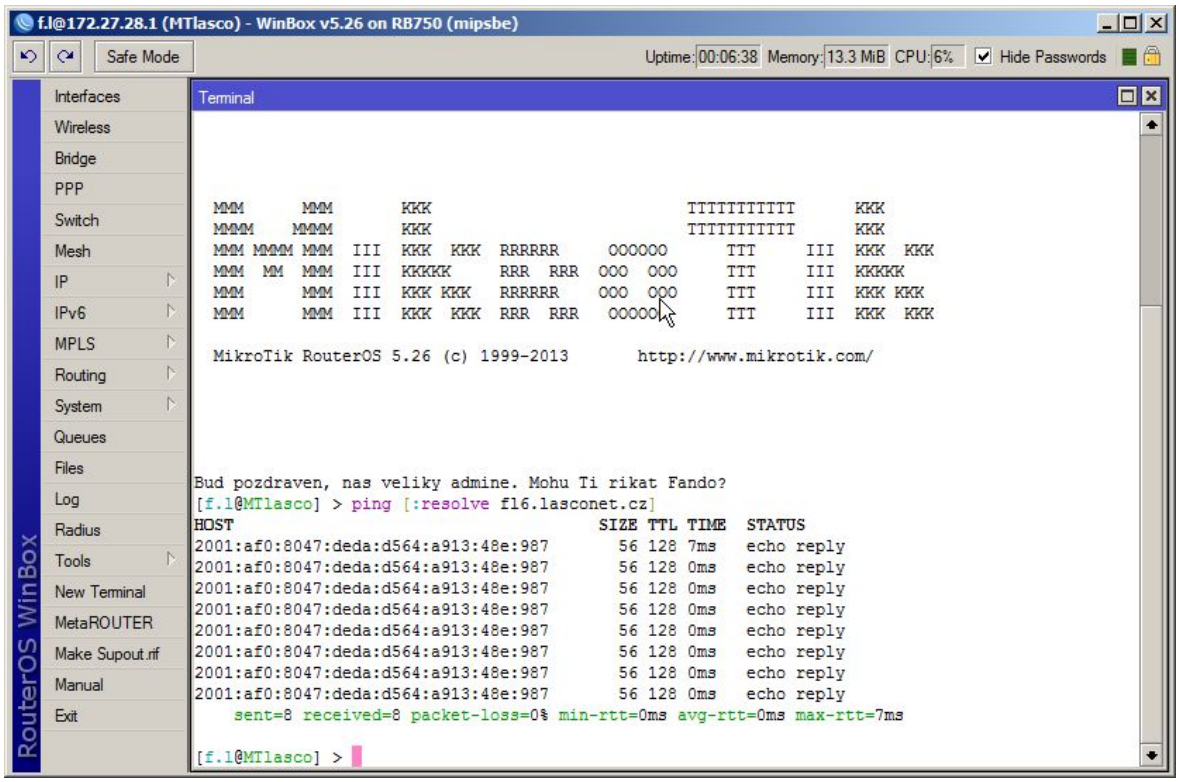
Obr. 20 Ping na alfa6.lasconet.cz



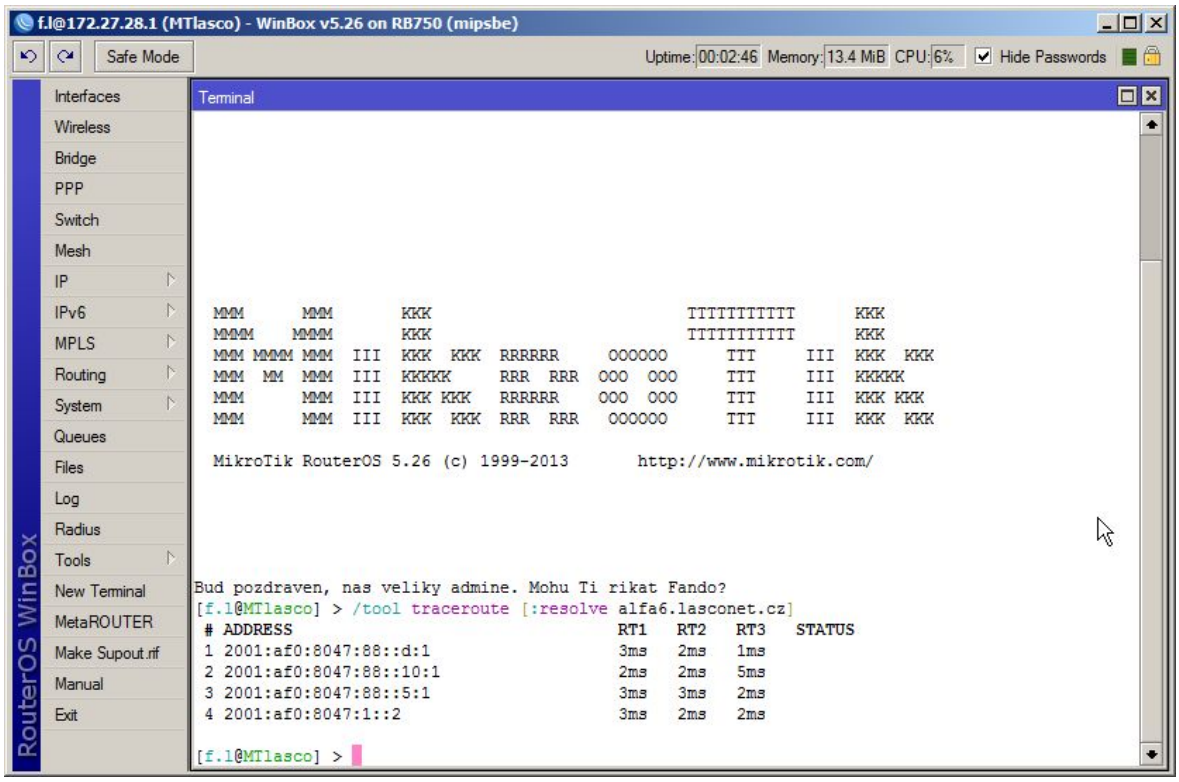
Obr. 21 Ping ipv6.google.com



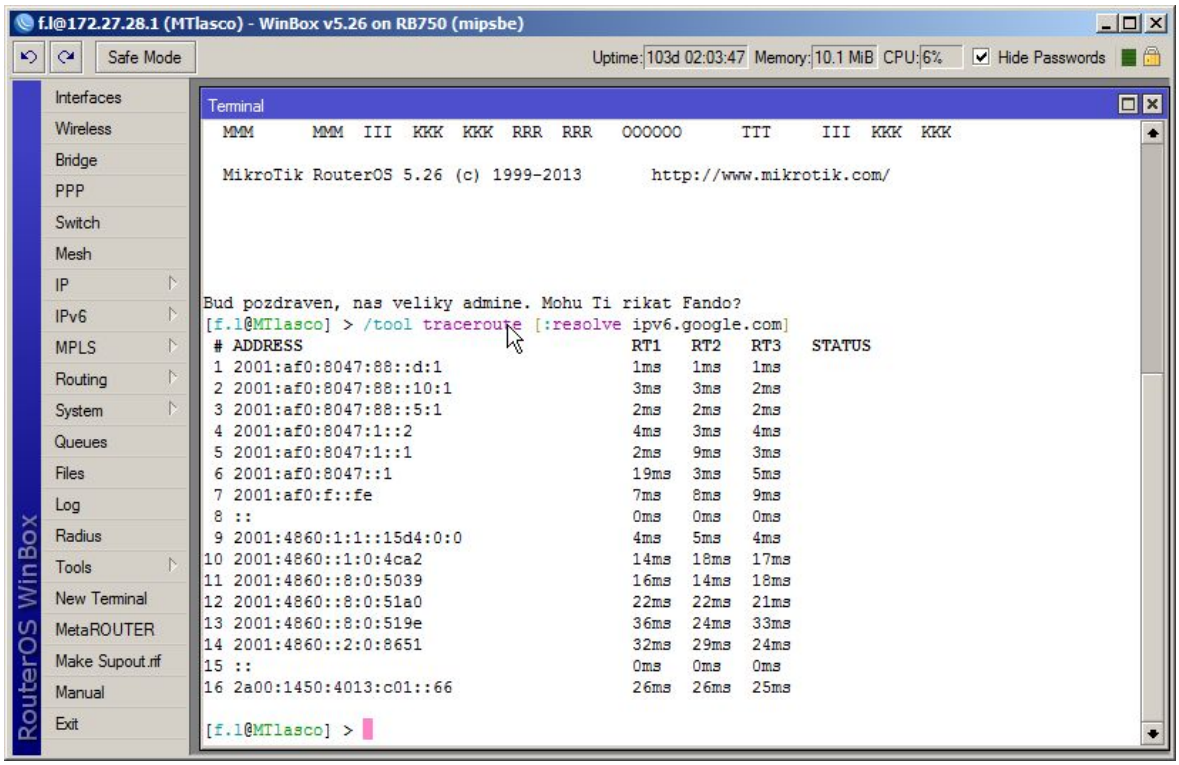
Obr. 22 Ping na fl6.lasconet.cz



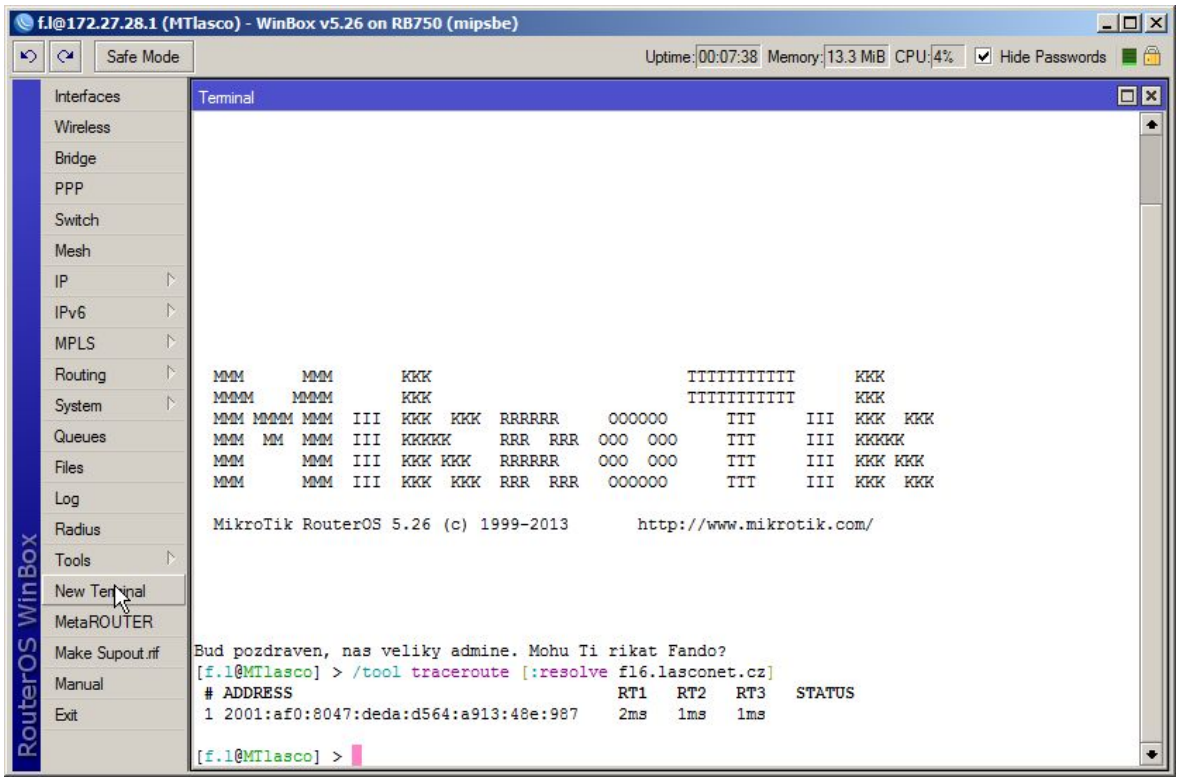
Obr. 23 Traceroute alfa6.lasconet.cz



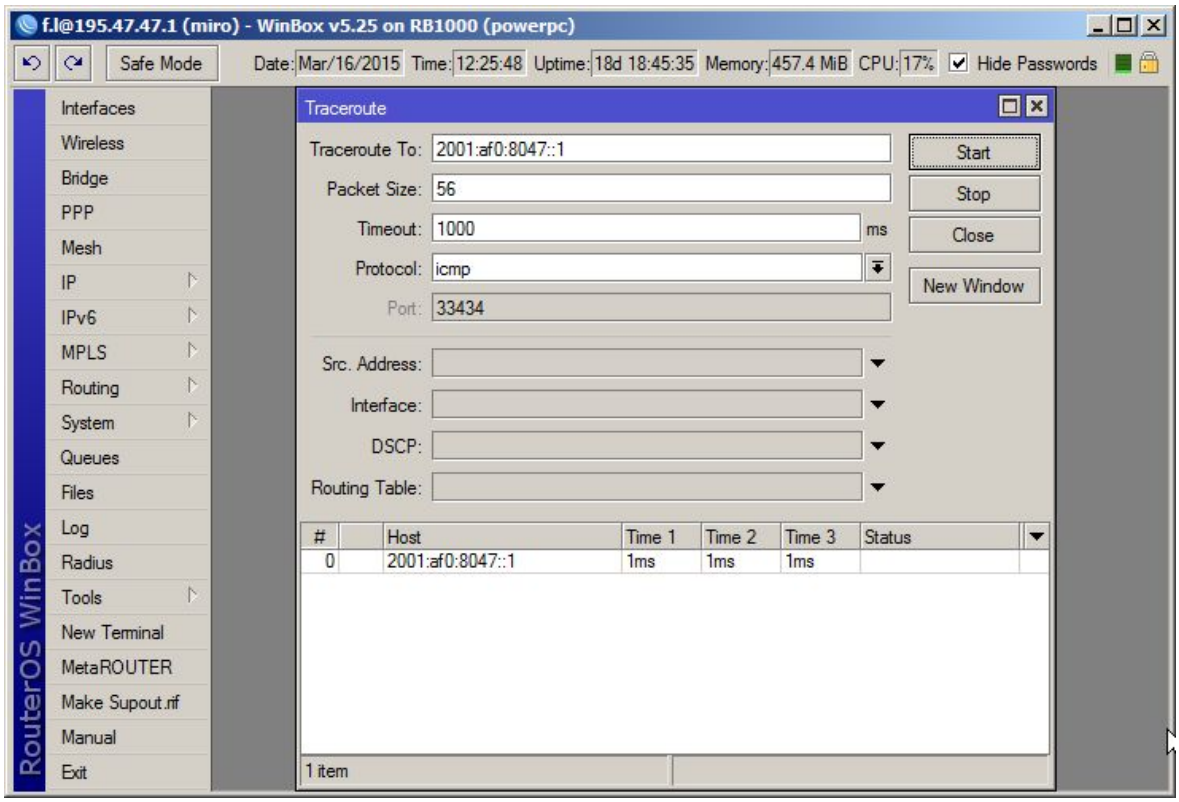
Obr. 24 Traceroute ipv6.google.com



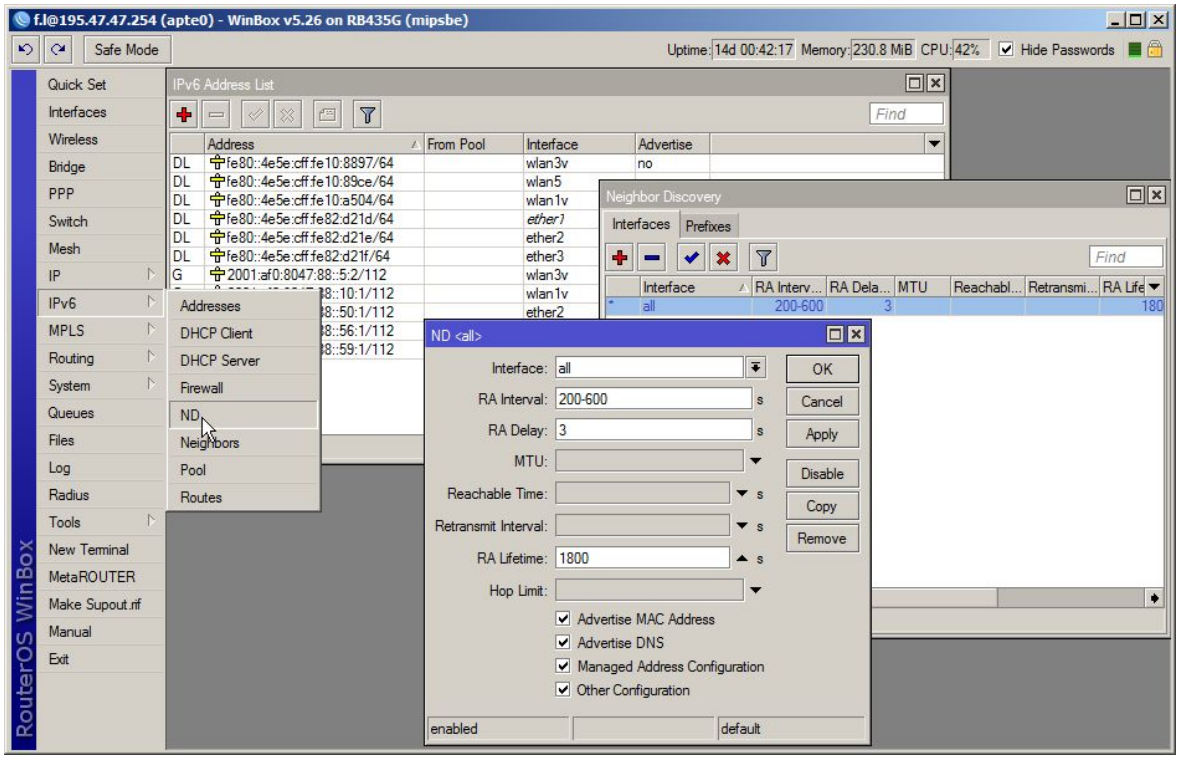
Obr. 25 Traceroute fl6.lasconet.cz



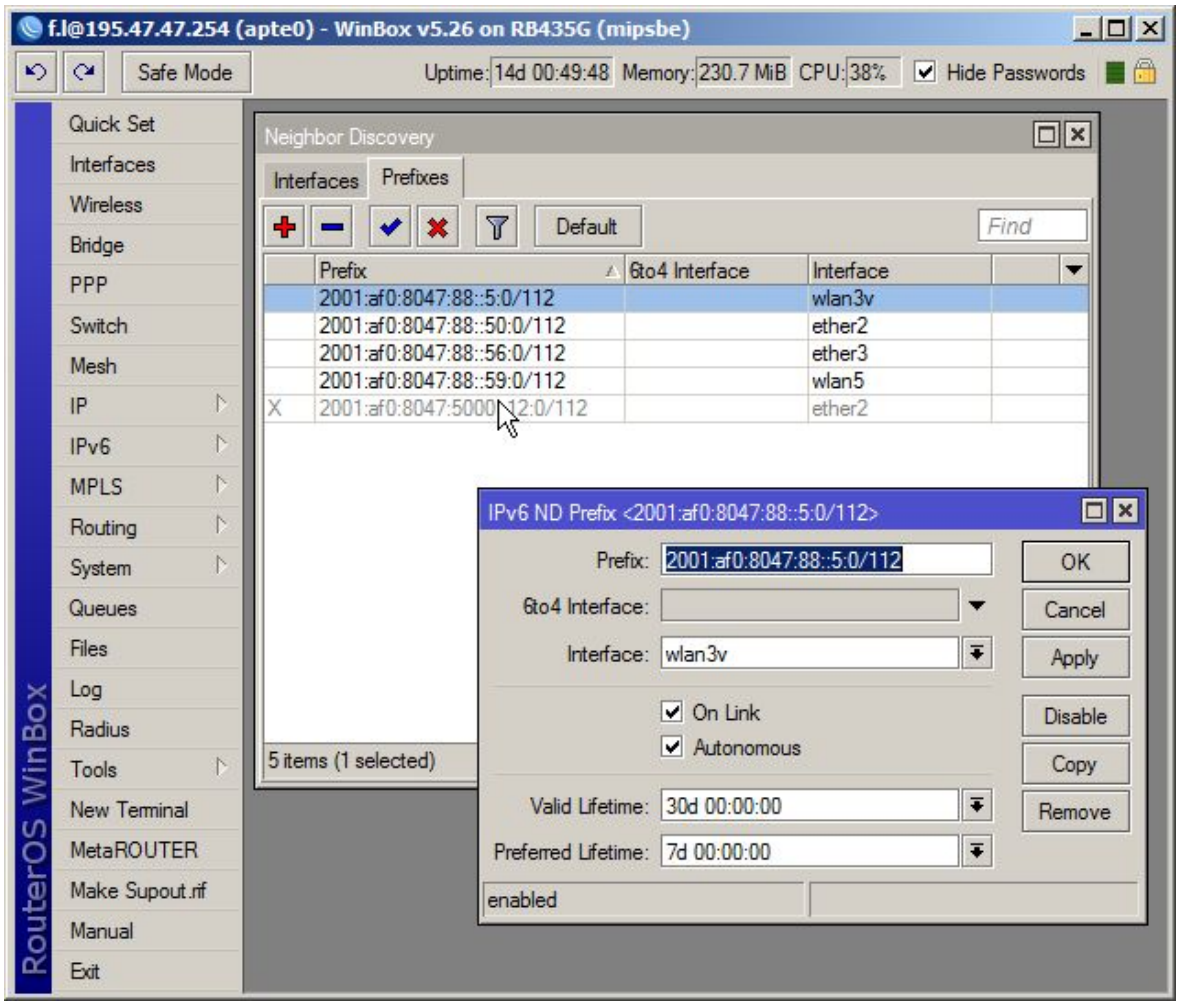
Obr. 26 Traceroute k ISP z hlavního routeru



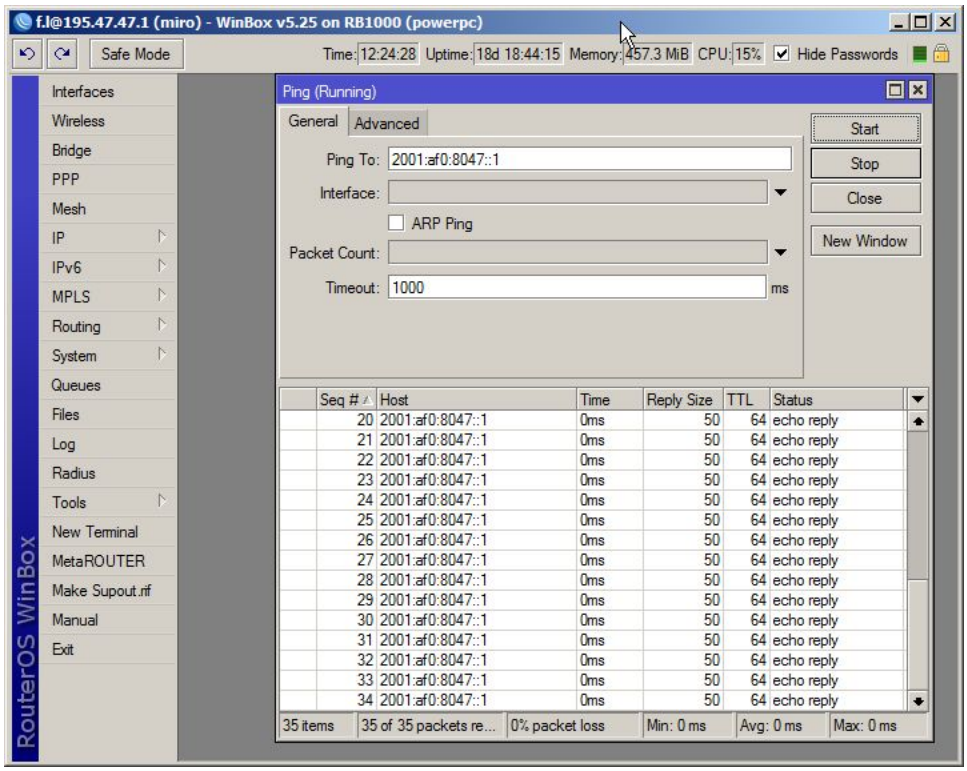
Obr. 27 Nastavení ND



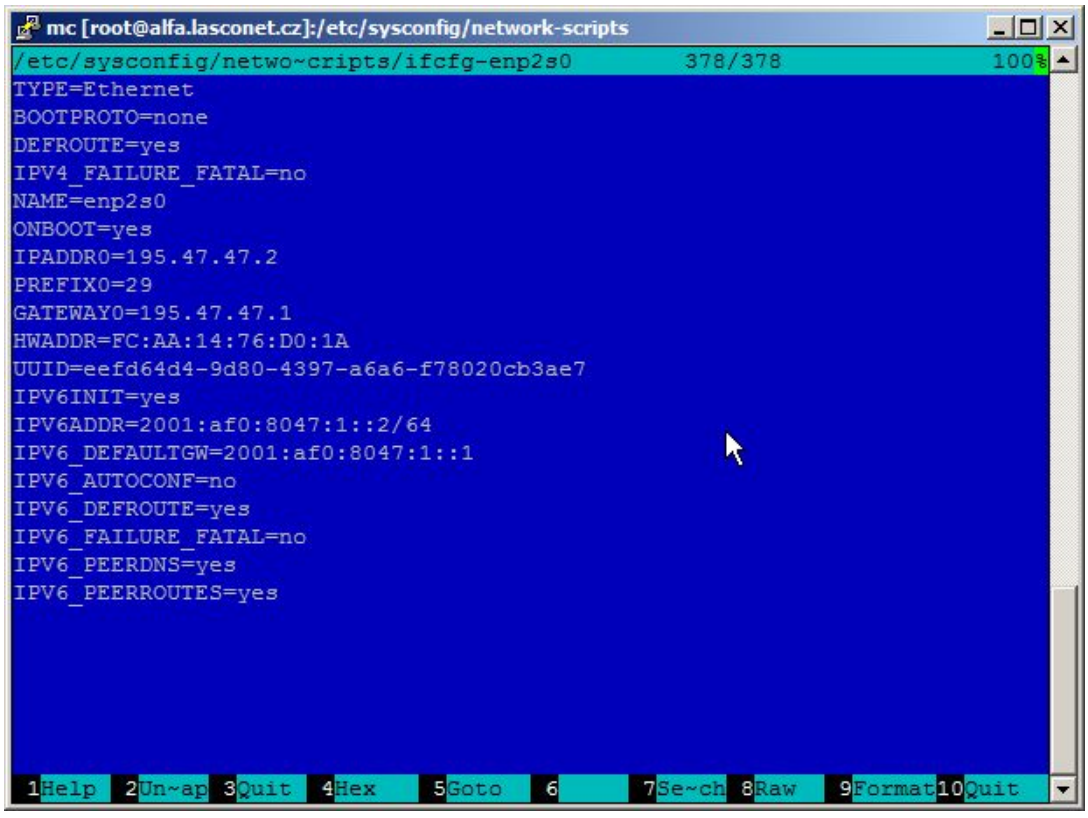
Obr. 28 Nastavení ND s prefixy ručně



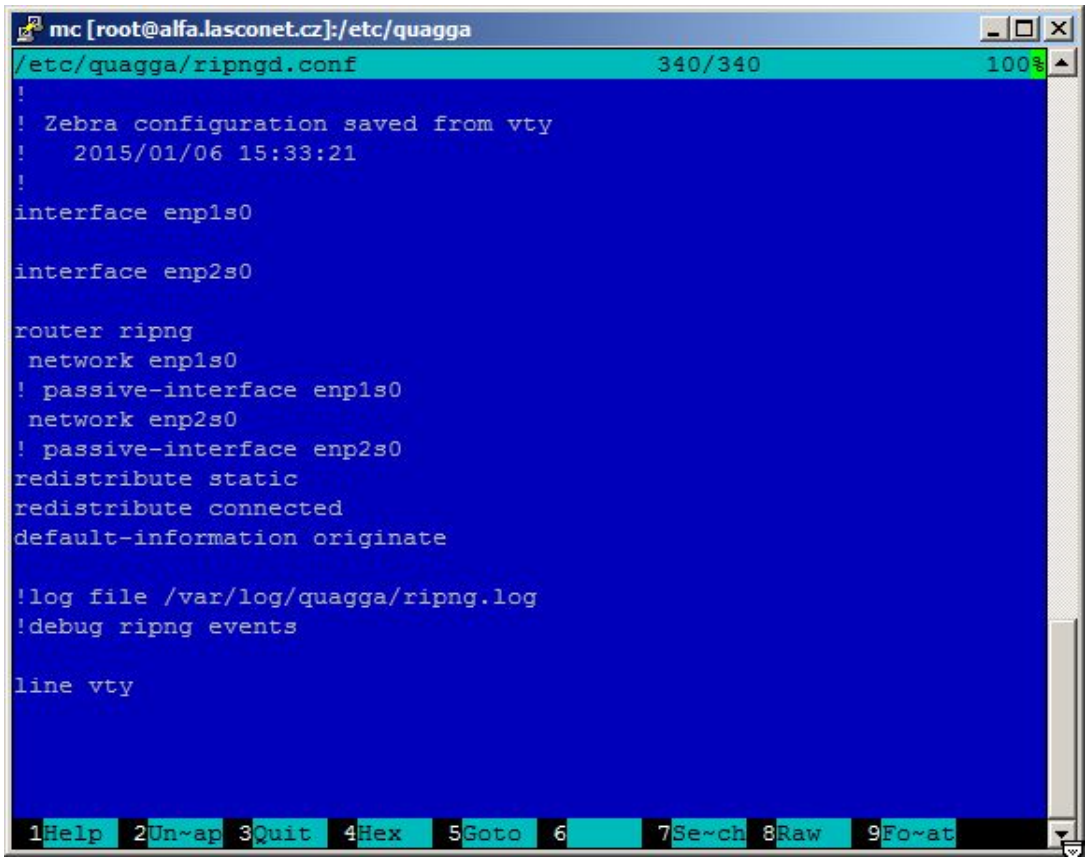
Obr. 29 Ping k ISP



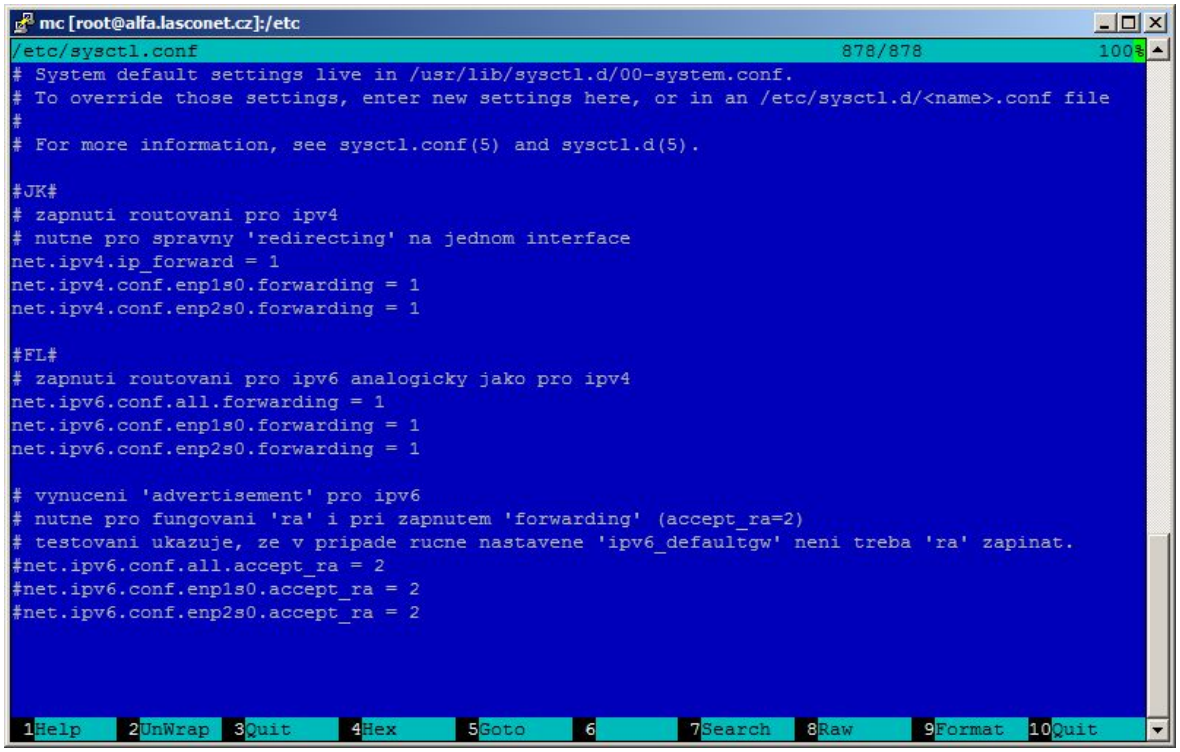
Obr. 30 Ruční nastavení IPv6 adresy v Linuxu



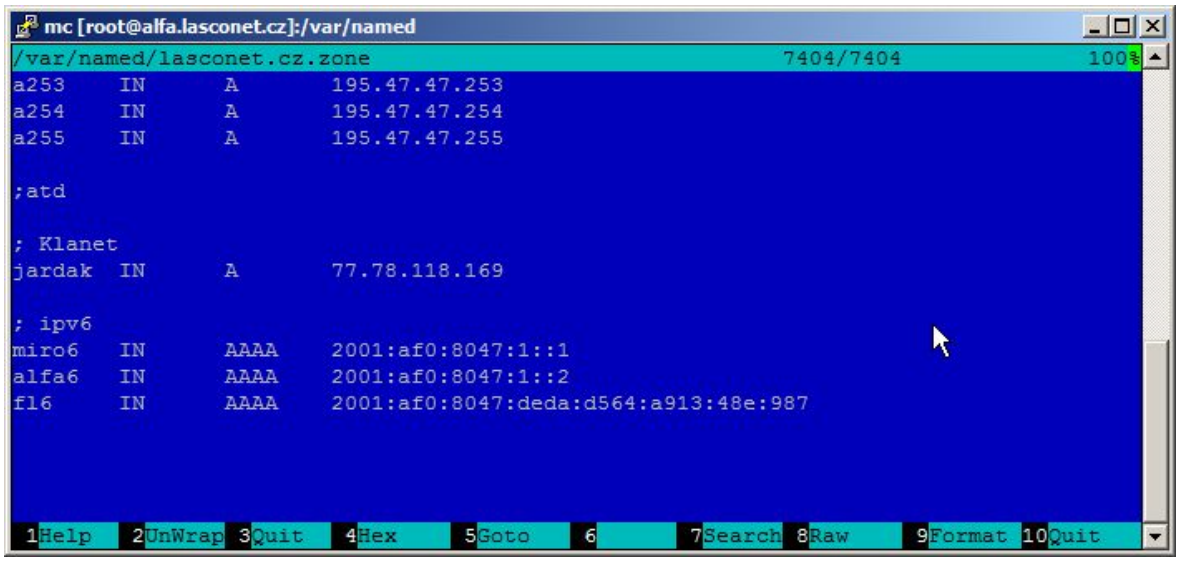
Obr. 31 Konfigurace RIPng v Linuxu



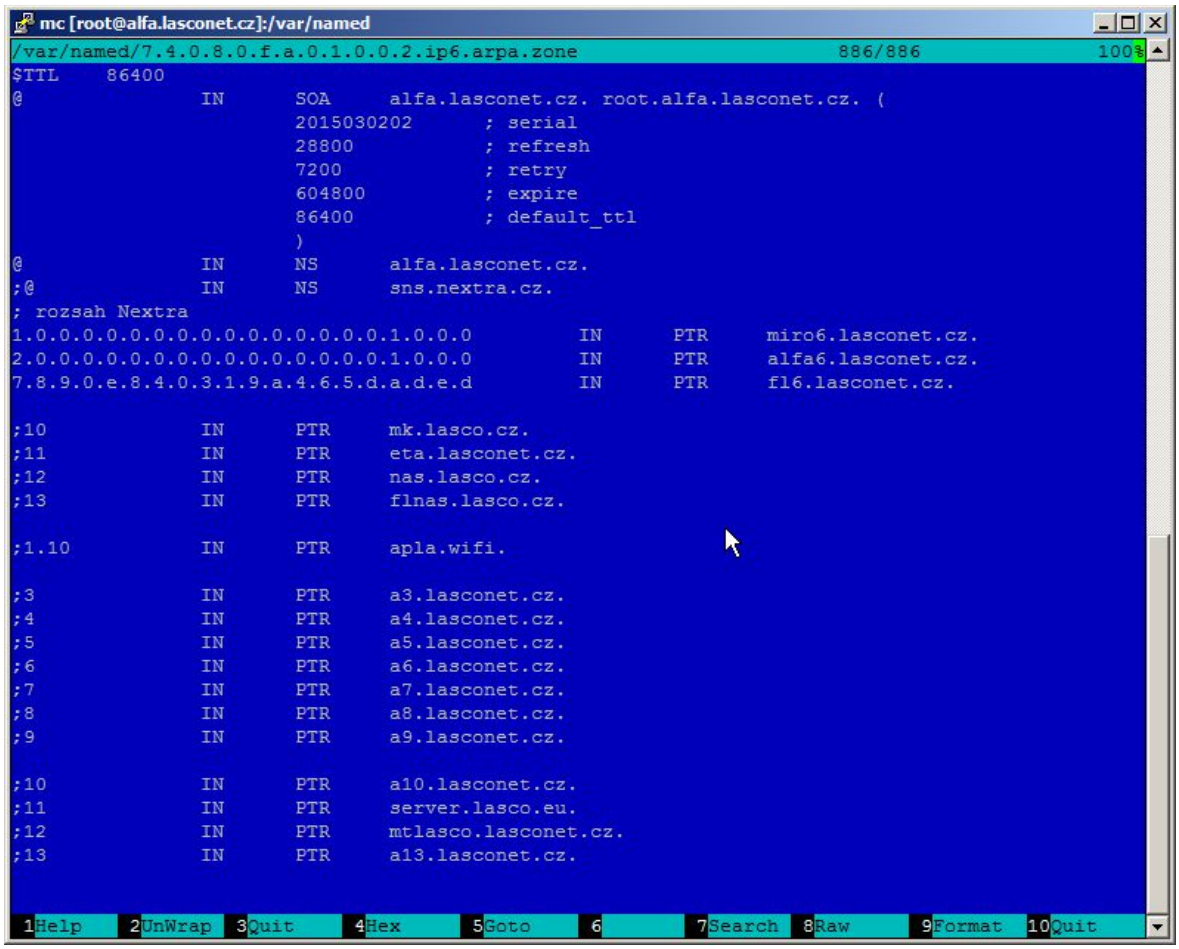
Obr. 32 Konfigurace forwardingu v Linuxu



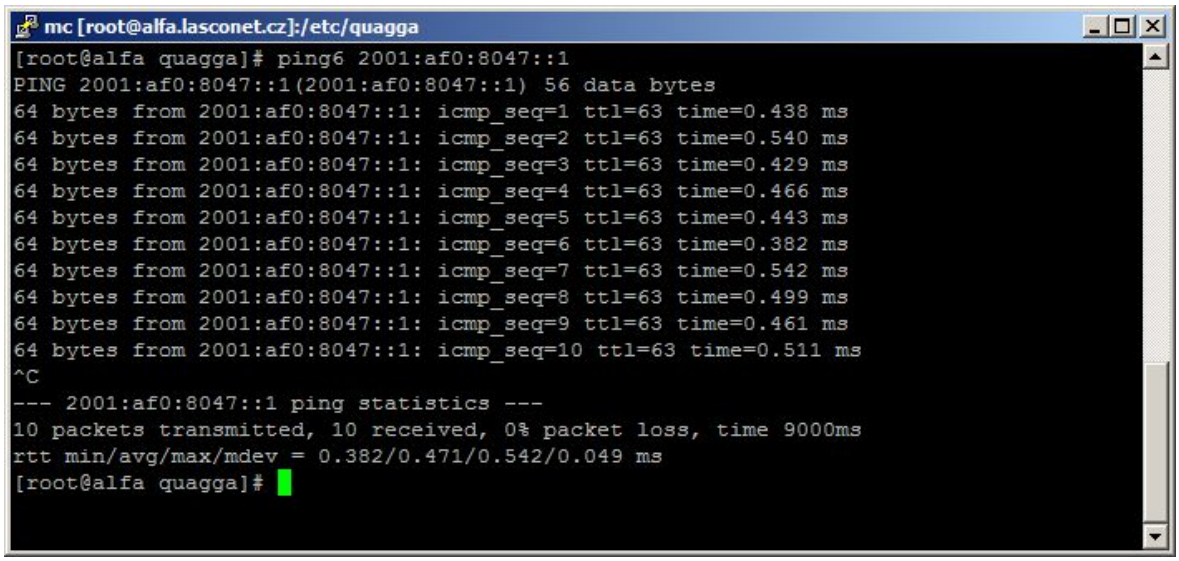
Obr. 33 Konfigurace DNS záznamů v Linuxu



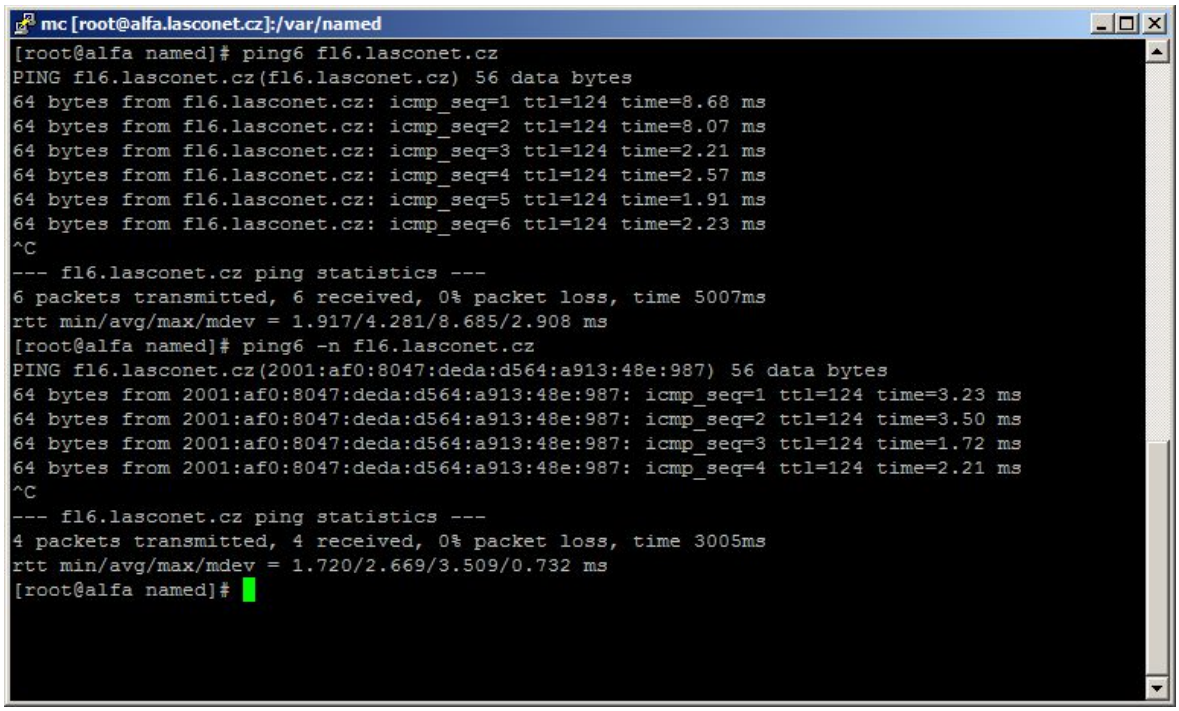
Obr. 34 Reverzní DNS v Linuxu



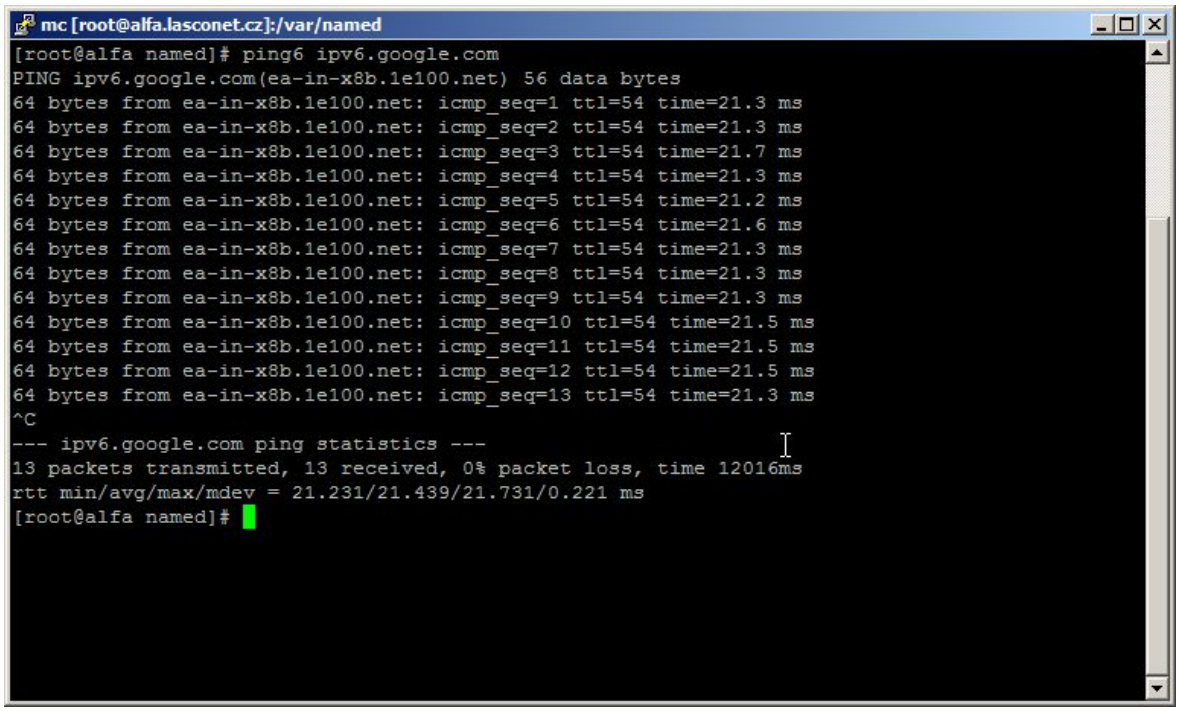
Obr. 35 Ping k ISP z Linuxu



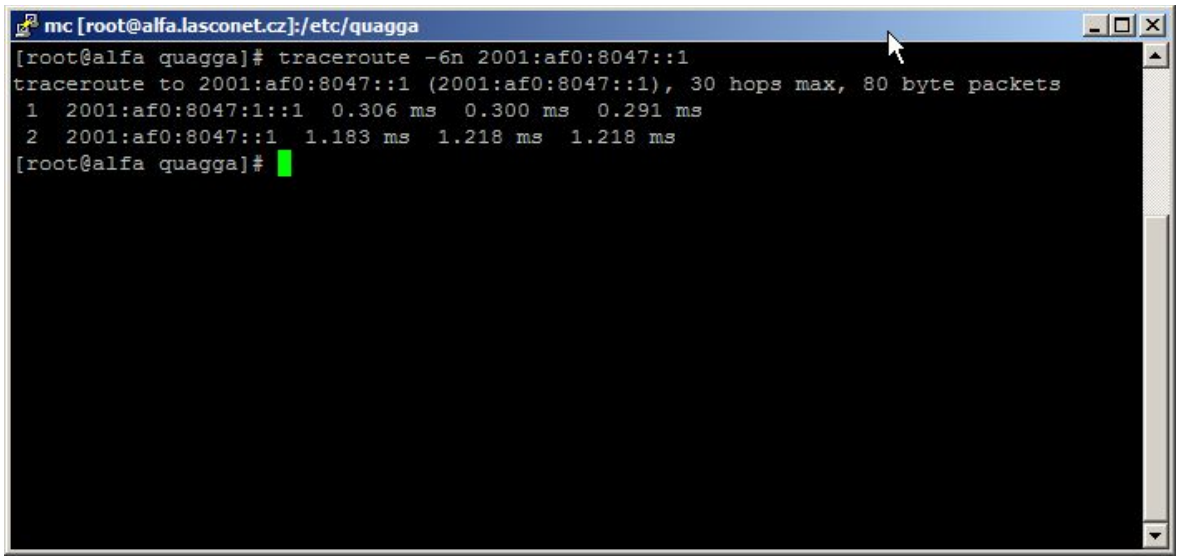
Obr. 36 Ping fl6.lasconet.cz se zohledněným DNS



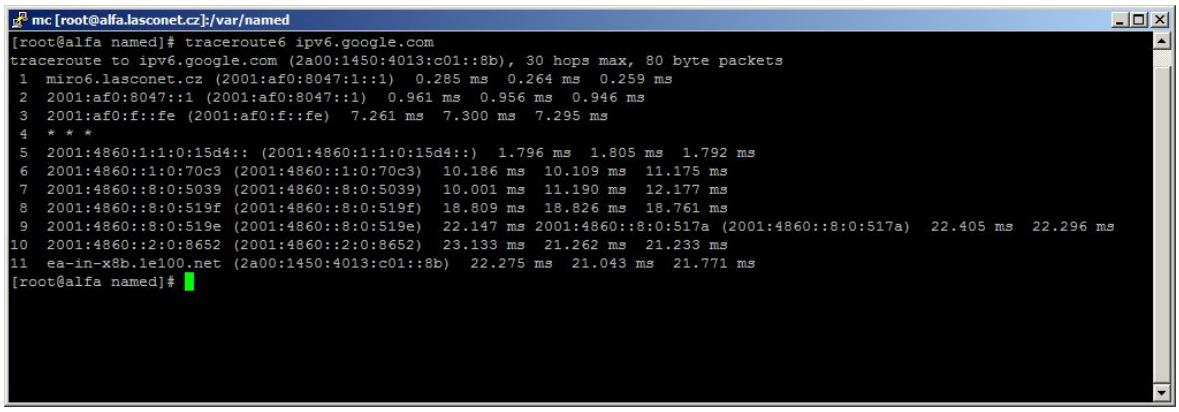
Obr. 37 Ping ipv6.google.com z Linuxu



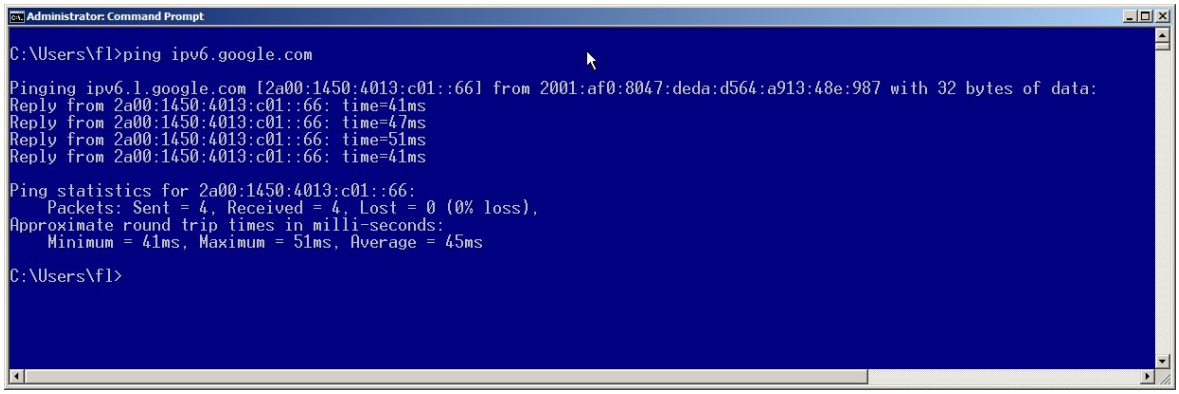
Obr. 38 Traceroute k ISP z Linuxu



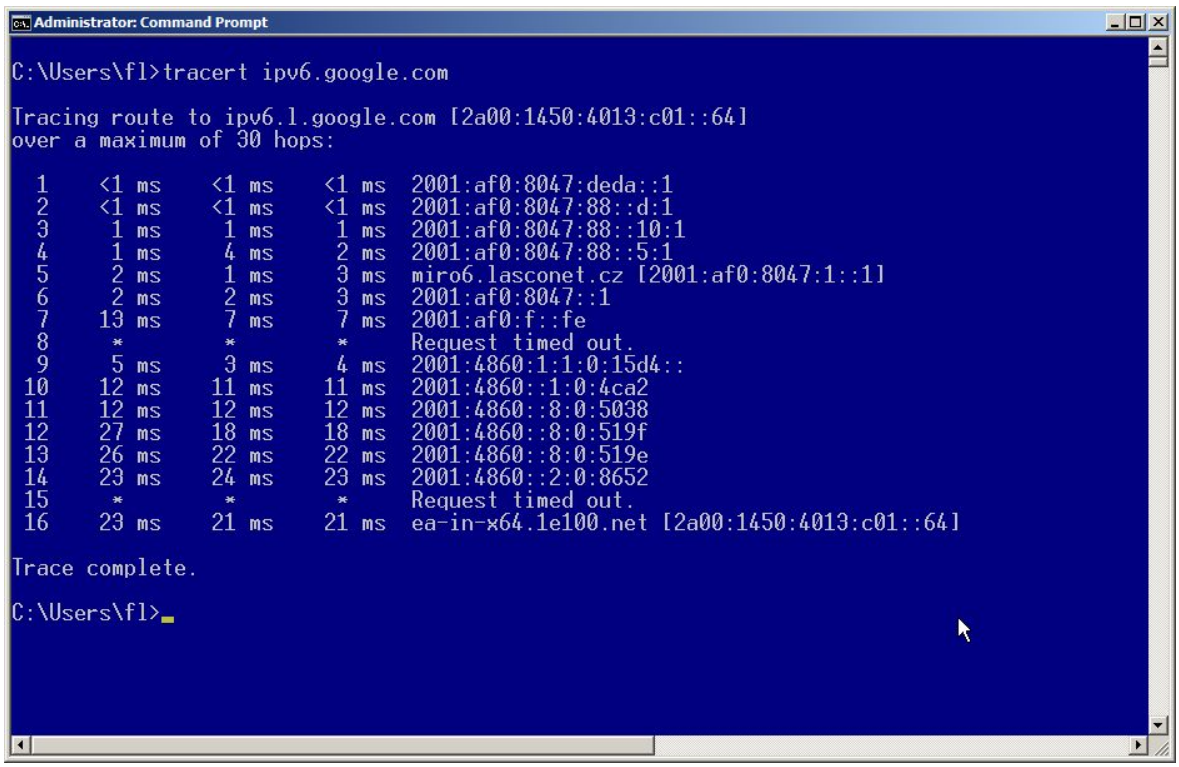
Obr. 39 Traceroute ipv6.google.com z Linuxu



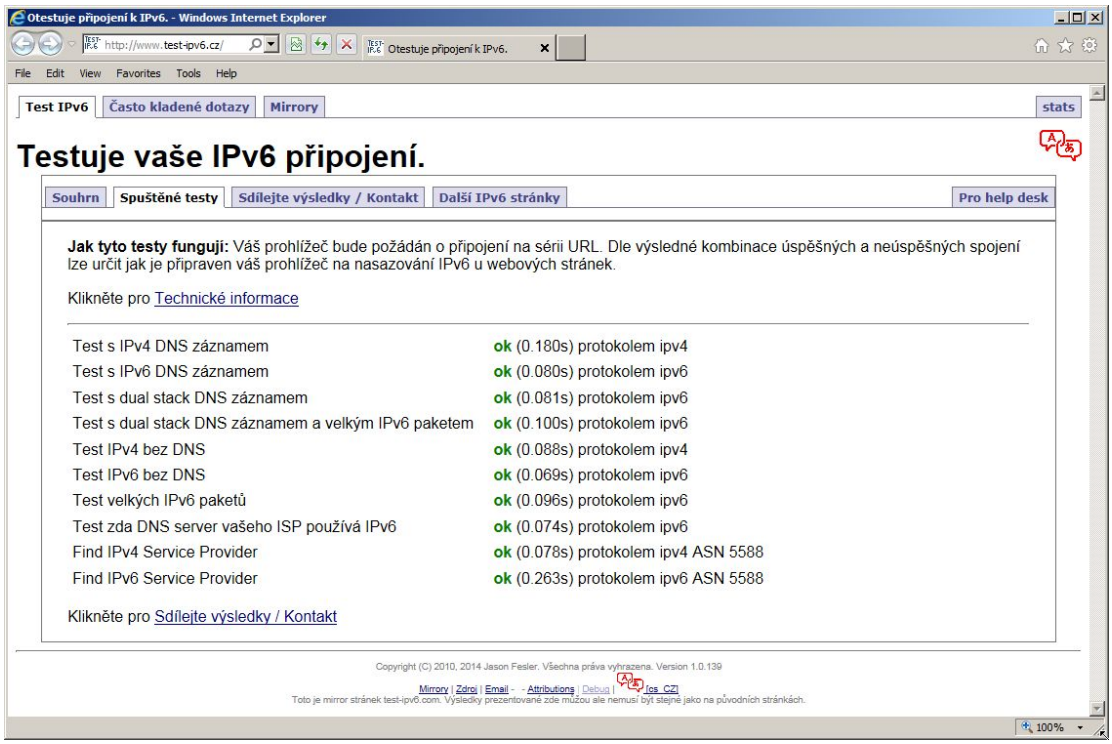
Obr. 40 Ping ipv6.google.com z Win



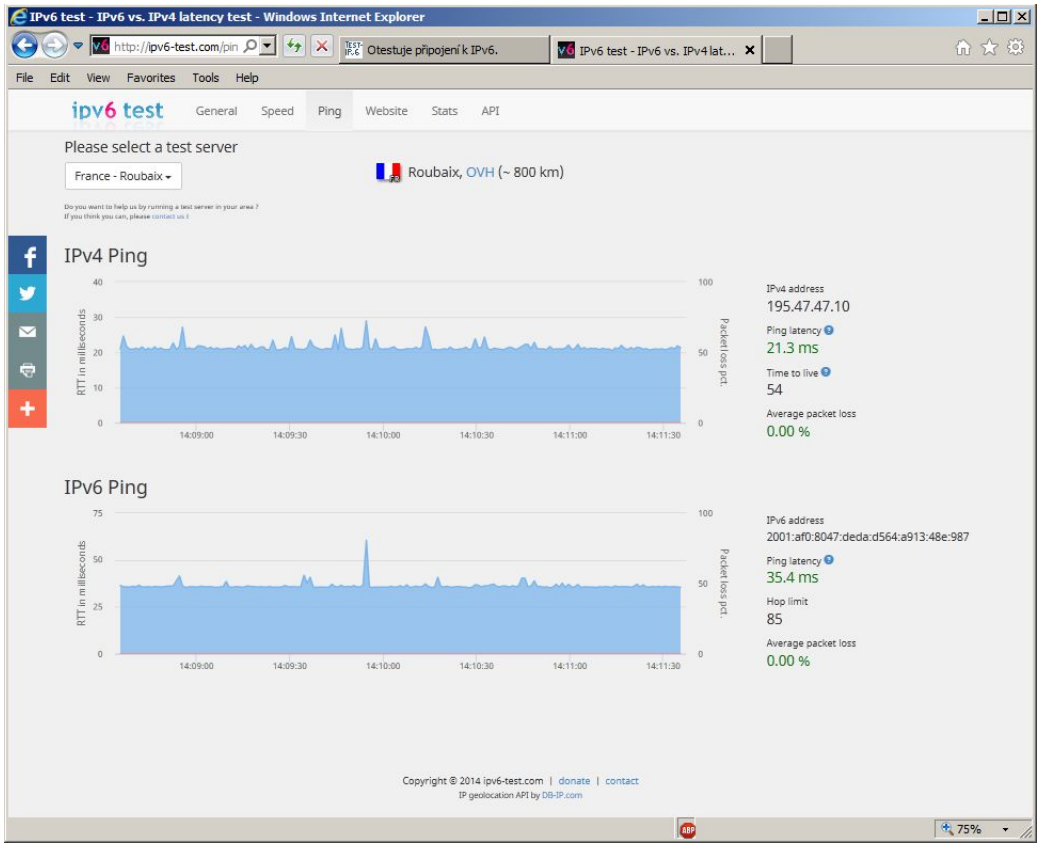
Obr. 41 Tracert ipv6.google.com z Win



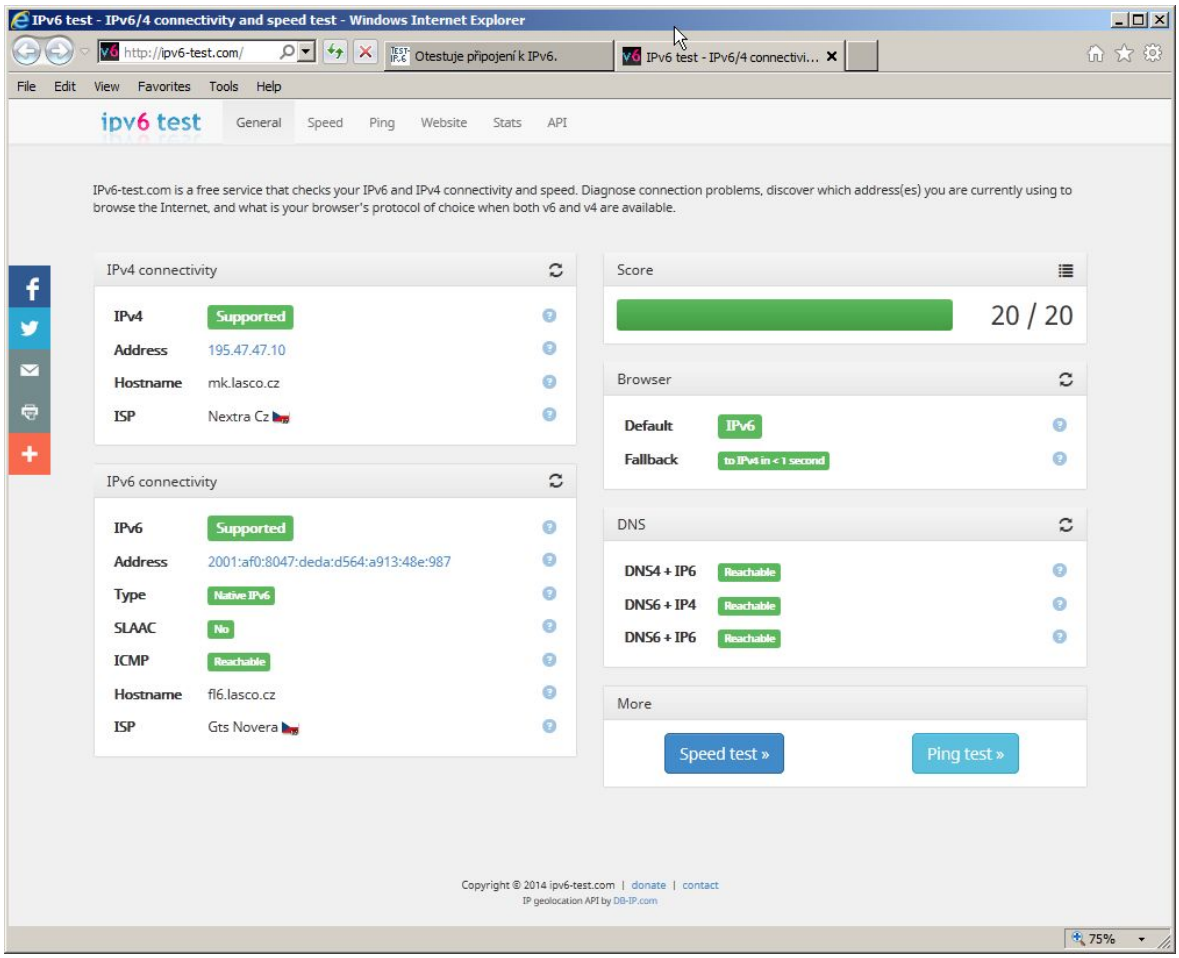
Obr. 42 Spuštěné testy IPv6



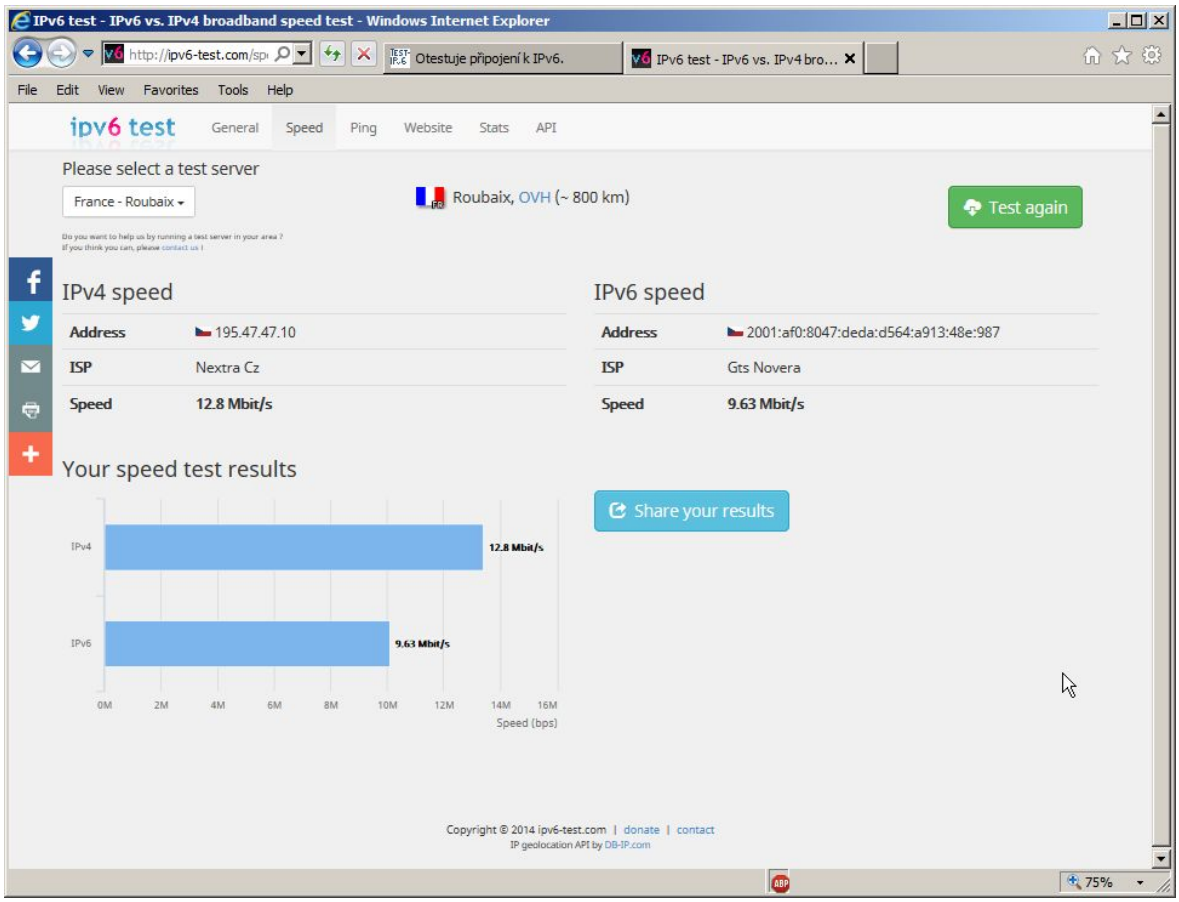
Obr. 43 Test pingu



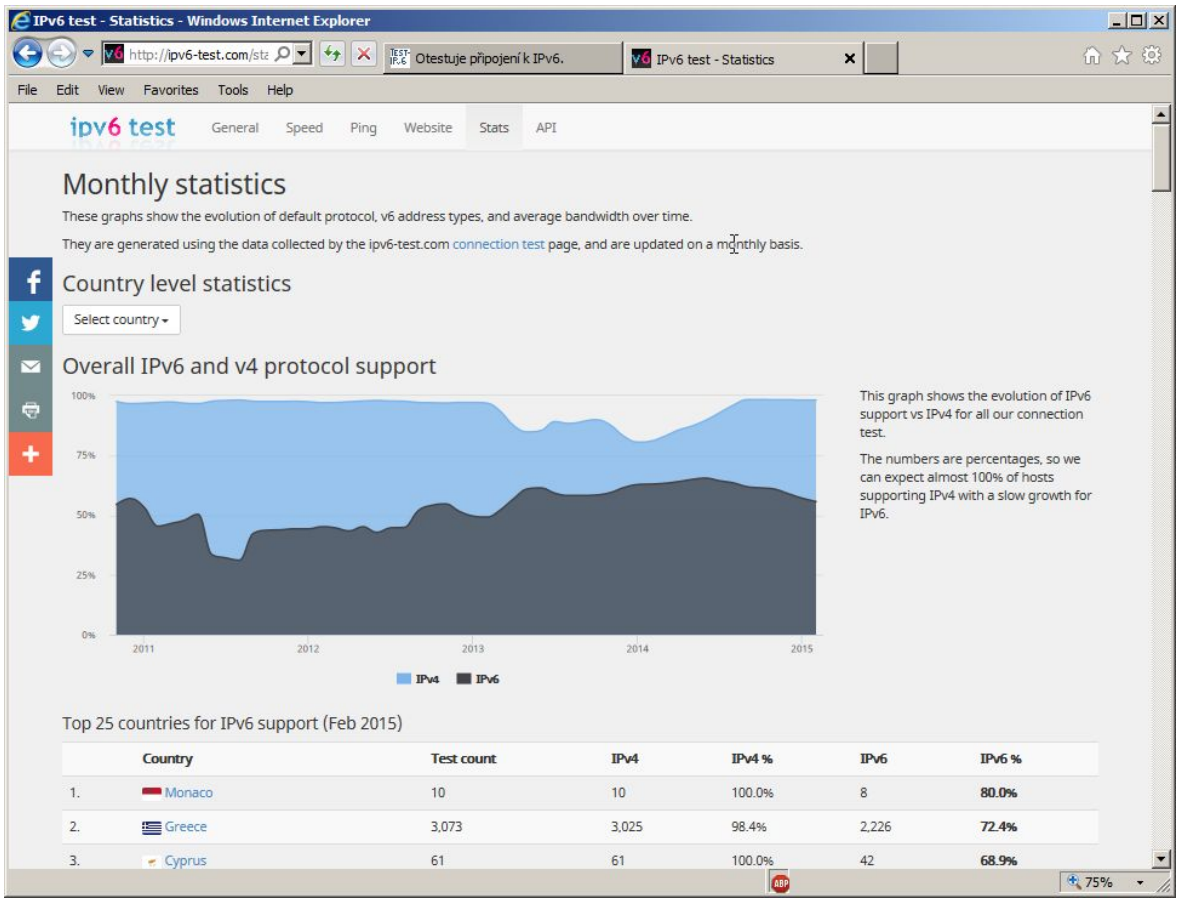
Obr. 44 Souhrnné výsledky



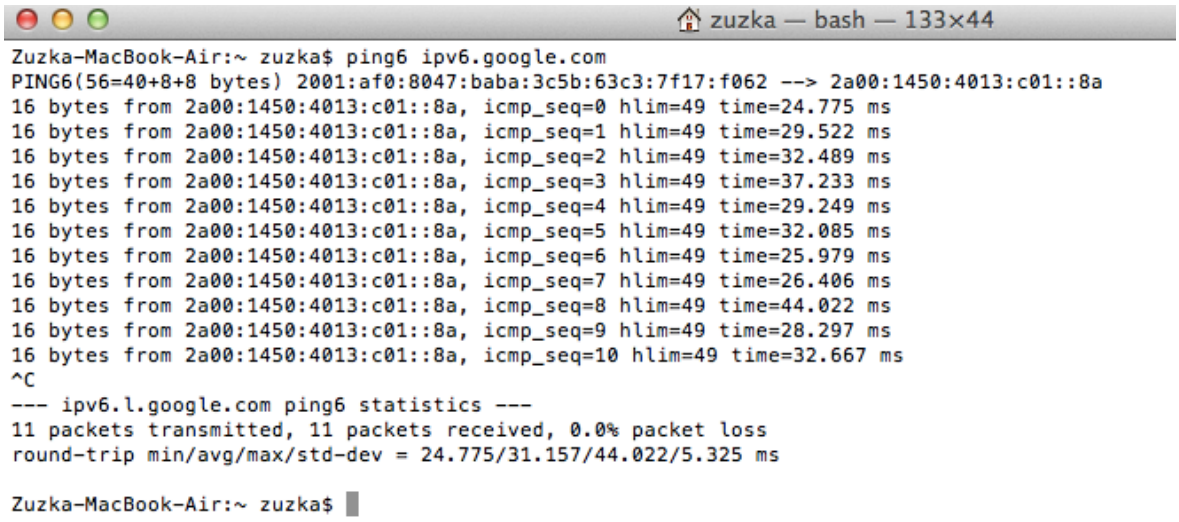
Obr. 45 Testování rychlosti



Obr. 46 Statistika testování



Obr. 47 Ping6 ipv6.google.com z MAC



Obr. 48 Traceroute6 ipv6.google.com z MAC