VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
DEPARTMENT OF INFORMATICS

IMPLEMENTACE PROTOKOLU IPV6 VE FIREMNÍ SÍTI

IMPLEMENTATION OF IPV6 PROTOCOL IN CORPORATE NETWORK

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — PAVEL PRIESNITZ
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, PhD.
SUPERVISOR

BRNO 2012

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2011/2012
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Priesnitz Pavel

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Implementace protokolu IPv6 ve firemní síti

v anglickém jazyce:

Implementation of IPv6 Protocol in Corporate Network

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

DOSTÁLEK, L, KABELOVÁ, A. Velký průvodce protokoly TCP/IP a systémem DNS. 2. aktualizované vydání. Praha: Computer Press, 2000. 426 s. ISBN 80-7226-323-4.
PETERKA, J. Jiří Peterka: archiv článků a přednášek [online]. [b. m.]: Jiří Peterka, 2011. Dostupné z: http://www.earchiv.cz/
RFC 2460. Internet Protocol, Version 6 (IPv6) Specification. [b. m.]: Network Working Group, 1998. 39 s. Dostupné z: http://www.ietf.org/rfc/rfc2460.txt
RFC 4291. IP Version 6 Addressing Architecture. [b. m.]: Network Working Group, 2006. 25 s. Dostupné z: http://www.ietf.org/rfc/rfc4291.txt
SATRAPA, P. Internetový protokol verze 6. Praha: CZ.NIC, 2008. 357 s. ISBN: 978-80-904248-0-7.

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2011/2012.

L.S.

Ing. Jiří Kříž, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA Děkan fakulty

V Brně, dne 15.04.2012

Abstrakt

Bakalářská práce se zaměřuje na implementaci protokolu IPv6 v prostředí firemní sítě podniku Teplárny Brno, a.s. V první části obsahuje stručnou definici protokolu, rozdíly oproti IPv4 a teoretický popis fungování. Praktická část se zaměřuje na analýzu současného stavu síťové infrastruktury v reálném prostředí a nabízí možné řešení implementace včetně doporučených zařízení.

Abstract

The bachelor's thesis focuses on the IPv6 internet protocol implementation in Teplárny Brno, a.s. network. At the first part it contains a brief definition of the protocol, differences between IPv6 and IPv4 and the teoretical description. Practical part is focused on the analysis of the network infrastructure present state in the real enviroment and offers some possible solution to implementation including recommended devices.

Klíčová slova

síťový protokol, IPv6, IPng, 6to4, dvojí zásobník, DHCPv6, adresace, automatická konfigurace, Teredo, ISATAP

Keywords

network protocol, IPv6, IPng, 6to4, dualstack, DHCPv6, adressation, autoconfiguration, Teredo, ISATAP

Bibliografická citace práce

PRIESNITZ, P. *Implementace protokolu IPv6 ve firemní síti.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2012. 72 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D..

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně.

Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2012 ……

Poděkování

Rád bych poděkoval panu Ing. Viktoru Ondrákovi PhD. za odborné vedení mé bakalářské práce a stejně tak za cenné rady. Dále děkuji panu Ing. Vladislavu Kovářovi ze společnosti Teplárny Brno, a.s. za konzultace a poskytnutí materiálů k analýze stavu firemní sítě.

Obsah

Úvod

Datová komunikace po sítích zaujímá v dnešním životě každého z nás nezastupitelné a jedinečné místo. Nemusí se přitom vždy jednat o momenty, kdy si tuhle nezastupitelnost uvědomujeme, jako je přímá interakce člověka s počítačem. S datovými sítěmi se v běžném životě setkáváme téměř na každém kroku. Bezhotovostní platby v obchodech, aktuální informace o odjezdu spojů na zastávkách MHD, zabezpečení silniční a železniční dopravy, mobilní telefony, rádia, televize, bezpečnost budov a spousty dalších oblastí jsou závislé na síťové komunikaci.

Aby všechny tyto věci fungovaly, je potřeba, aby měly svůj řád a pevně definovaná pravidla. Ta jsou v určitém segmentu sítí označována souhrnným názvem Internet Protocol (zkratka IP).

Stejně jako většina věcí v tomto světa zastarává, zastarávají i komunikační standardy v datových sítích a postupně přichází potřeba nahradit stávající nedostačující řešení něčím novým. Každá taková změna s sebou nese nezanedbatelný výdaj prostředků, a proto se jim lidé snaží vyhnout nebo je co nejvíce oddálit.

Ve své práci bych chtěl popsat možnosti nového protokolu, označovaného jako IPv6 nebo také IPng, který definuje komunikační standardy v datových sítích. Dále se budu věnovat analýze konkrétního síťového prostředí ve společnosti Teplárny Brno, a.s. a nastíním možnosti implementace protokolu IPv6 do stávající síťové infrastruktury tak, aby zůstala zachována funkčnost a nedošlo k žádným omezením v klíčových oblastech komunikace.

1 Vymezení problému a cíle práce

Hlavním cílem mé práce je navrhnout funkční a přijatelný model implementace komunikačního protokolu IPv6 do prostředí stávající firemní sítě Tepláren Brno, a.s. Zde je v současné době hlavním protokolem, využívaným pro datovou komunikaci, IP verze 4, se kterým mají podnikoví IT specialisté zkušenosti.

Protože dnes nový komunikační protokol není moc rozšířený, firmy se jeho přímé implementaci vyhýbají, i když je jasné, že jednou se na něj alespoň ve větší části internetu bude muset přejít. V souvislosti s tím jsem si vytyčil následující dílčí cíle:

V úvodní části chci provést analýzu stávajícího stavu s důrazem na nestandardní prvky počítačové sítě. Dá se předpokládat, že moderní počítačové stanice a serverové systémy nebudou mít s protokolem výrazný problém a jeho implementace bude otázkou nastavení. Naopak můžeme předpokládat velké potíže u specifických technologických zařízení, sloužících pro řízení a kontrolu provozu a rozvodných sítí.

V teoretické části své práce chci protokol představit, definovat jeho odlišnosti od předchůdce IPv4 a v teoretické rovině vyjmenovat přechodové mechanismy. Budu se přitom zaměřovat na ty vlastnosti, které jsou stěžejní pro nasazení a údržbu protokolu v počítačové síti z pohledu správce IT, ale i aspekty, které jsou klíčové pro pochopení principu fungování a způsobu adresování.

Druhá praktická část práce bude věnována návrhu implementace nového protokolu do sítě tak, aby zůstala co nejvíce zachována současná funkcionalita. Zaměřím se přitom na možnosti stávajících technických zařízení. Budu se také věnovat zhodnocení, zda je v současné době přechod na nový protokol výhodný a jestli přináší tolik výhod, že se vyplatí.

2 Analýza současného stavu

V této části své práce uvedu stručnou historii a popis firmy Teplárny Brno, a.s. a dále budu analyzovat skutečnosti, které jsou klíčové pro přechod na protokol IPv6. Zaměřím se na infrastrukturu počítačové sítě, informace o jednotlivých uzlech a jejich schopnost pracovat v rámci protokolu IPv6.

2.1 Informace o společnosti

2.1.1 Souhrnné informace o společnosti

Obchodní firma:	Teplárny Brno, a.s.
Sídlo společnosti:	Okružní 25, 638 00 Brno
Datum vzniku:	1. 5. 1992
Právní forma:	akciová společnost
IČ:	46347534
DIČ:	CZ46347534
Akcie:	listinné, na jméno
Jmenovitá hodnota:	88 565 000,- Kč / 1 akcii
Celková hodnota:	885 650 000,- Kč

Společnosti je zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně pod spisovou značkou B/786 (Teplárny Brno, 2010, s. 4-5).

Obrázek 1: Logo Tepláren Brno, a.s. (Zdroj: Teplárny Brno)

2.1.2 Historie

Brněnské teplárny vznikly v první polovině 20. století, kdy se začala zvyšovat potřeba centrálního zdroje tepla a páry. Na svou dobu se jednalo o velmi ambiciózní projekt, jelikož už od začátku spojoval výrobu tepla s výrobou elektrické energie.

Práce na vybudování prvního provozu začaly 1. dubna 1929 na ulici Špitálka, odkud měly teplárny výhodnou pozici pro zásobování Brněnských textilních podniků. V roce 1930 zásoboval provoz na Špitálce teplem 8 továren ve svém okolí (Teplárny Brno, 2011, Historie společnosti).

Brněnská teplárenská síť se ze Špitálky postupně rozrůstala o špičkové výtopny na Starém Brně, na Červeném mlýně a také o výkonný zdroj v Brně-Maloměřicích. Postupem času se staví administrativní budova na ulici Okružní na Lesné, doplněná o spoustu menších zdrojů a výměníků na území Brna.

V průběhu vývoje před rokem 1992 vystřídala brněnská teplárenská síť velké množství majitelů a zastřešujících organizací, až nakonec přešla pod Fond národního majetku. Ten v roce 1992 zakládá akciovou společnost Teplárny a.s. V roce 1993 přechází Teplárny a.s. na jméno Teplárny Brno a.s., pod kterým společnost vystupuje do dnes.

V roce 2004 převádí majoritní vlastník akcií MVV Energie s.r.o. svůj podíl na společnost Tepelné zásobování Brno, a.s., která je přímo ovládaná statutárním městem Brnem.

1. října 2009 dochází ke sloučení všech brněnských teplárenských podniků pod nástupnickou organizaci Teplárny Brno, a.s., vlastnící výrobní kapacity i přenosovou soustavu (Teplárny Brno, 2011, Přehled historických milníků).

2.1.3 Předmět podnikání a výrobní program

Hlavními činnostmi společnosti Teplárny Brno, a.s. jsou výroba a distribuce tepelné energie, výroba elektřiny a obchod s elektřinou (Teplárny Brno, 2010, s. 4). Tyto činnosti jsou s ohledem na zaměření podniku shodné s předmětem podnikání a odvíjí se od nich také výrobní program, zahrnující hlavně tepelnou a elektrickou energii.

Společnost je držitelem následujících licencí:

- Licence č. 110 100 887 – skupina 11 výroba elektřiny, č.j. P4196/2001/300 ze dne 28. 12. 2001, s termínem zahájení licencované činnosti 28. 11. 2001 a koncem platnosti licence dne 13. 12. 2026 včetně.

- Licence č. 320 100 888 – skupina 32 rozvod tepelné energie, č.j. P4198/2001/300 ze dne 16. 11. 2001, s termínem zahájení licencované činnosti 1. 12. 2001 a koncem platnosti licence 16. 12. 2026 včetně.
- Licence č. 310 101 346 – skupina 31 výroba tepelné energie, č.j. P4197/2001/300 ze dne 5. 11. 2003, s termínem zahájení licencované činnosti 1. 12. 2001 a koncem platnosti licence 16. 12. 2026 včetně.
- Licence č. 140705320 – obchod s elektřinou, č.j. 02119-24/2007-ERU ze dne 21. 6. 2007, s termínem zahájení licencované činnosti 25. 6. 2007 a koncem platnosti licence do 24. 6. 2012 včetně (Teplárny Brno, 2010, s. 4).

Kromě hlavních výrobních činností má společnost navíc živnostenská oprávnění, která slouží především k pokrytí potřeb při vlastním provozu (Teplárny Brno, 2010, s. 4).

2.2 Klíčové provozy a budovy

Při analýze počítačové sítě podniku, která je nutným předpokladem pro návrh implementace nového protokolu IPv6, je důležitá znalost rozsahu sítě a lokalit. V této části se zaměřím nejen na hlavní budovy a provozy v majetku Tepláren Brno, a.s., ale na všechny klíčové lokality na území města Brna, na kterých mají Teplárny Brno soustředěna svá síťová zařízení.

Správa společnosti

Administrativní budova správy společnosti se nachází v městské části Brno-Lesná na ulici Okružní. Třípatrový objekt je obdélníkového tvaru s atriem uprostřed. Uvnitř jsou převážně kanceláře správy společnosti, hospodářských pracovníků a také oddělení IT. Nevyužité části objektu jsou pronajímány dalším firmám.

Protože je budova vhodně umístěna, jednotlivé kanceláře mají v pronájmu také mobilní operátoři, kteří zde mají umístěno technické zázemí pro antény na střeše. Výhodné je umístění budovy také pro datovou síť samotných Tepláren, které používají spojení pomocí mikrovlnných rádio-reléových antén.

Provoz Špitálka

Nejstarší Brněnský teplárenský komplex na ulici Špitálka disponuje velkým množstvím budov. Centrální budova je tvořena provozní částí s velínem. K ní přiléhá komplex kanceláří pro techniky provozu a hospodářské pracovníky.

Další důležitou kancelářskou budovou je úpravna vody. Zde se nachází dvě patra s kancelářskými prostory a velín.

Třetí budovou, využívající datové sítě, v areálu je třípatrový samostatný kancelářský objekt, který využívají techničtí a hospodářští pracovníci s běžným vybavením. Přechod by zde měl proběhnout bez problémů.

Provoz Brno-sever

Zásobování tepelnou energií pro severní část města Brna obstarává provoz Brno-sever na Obřanské ulici. Obdobně jako u provozu Špitálka se zde nacházejí jak kanceláře s běžnými počítači, tak provozní systémy, u kterých můžeme předpokládat menší kompatibilitu s protokolem IPv6.

Provoz Červený mlýn

Provoz Červený mlýn na ulici Sportovní je jedním z nejmodernějších teplárenských provozů. V roce 1999 byl přestavěn ze zastaralého zdroje uhlí na moderní zemní plyn. Kromě výroby tepelné energie je schopen zásobovat elektrickou síť také špičkovým proudem (Teplárny Brno, 2011, Provoz červený mlýn).

V areálu se nacházejí dvě správní budovy, ve kterých je největší koncentrace výpočetní techniky, převážně kancelářských počítačů. Další je pak možno nalézt v dozorně provozu v centrální výrobní budově a v přilehlých dílnách a laboratořích.

Menší provozy

Součástí brněnské teplárenské sítě je množství dalších provozů, které se liší velikostí a výkonem. Kromě dalších výkonově velkých zdrojů, jako jsou provozy Staré Brno, Kamenný Vrch a Bystrc, se jedná o malé kotelny, výměníky a podpůrné provozy, kterých je na území města Brna celkem 62. Jejich seznam je uveden v příloze 1.

Ve větších provozech se nachází malé množství uživatelské výpočetní techniky a stálá obsluha. Malé zdroje a výměníkové stanice jsou dnes již provozovány bez obsluhy a o

měření a regulaci se starají technologické počítačové systémy, řízené na dálku z velínů velkých objektů.

2.3 Počítačová síť

V dnešní době je pochopitelným požadavkem, aby mezi všemi provozy fungovala bezchybná komunikace bez nebezpečí výpadků. Výpadek služeb by mohl být, zvláště v zimních měsících, pro mnoho obyvatel Brna minimálně nepříjemný. Proto je kvalita datových sítí, které se používají pro řízení a vyhodnocování chodu technologických zařízení, velmi důležitá.

2.3.1 Propojení lokalit a páteřní síť

Teplárny Brno jsou, jak bylo naznačeno v kapitole 2.2, velmi komplexním podnikem, který má svoje provozy rozprostřeny na poměrně velkém území. Z toho vyplývá velké množství síťových lokalit, které je potřeba propojit dohromady.

Tabulka 1: Seznam klíčových lokalit Tepláren Brno, a.s.

Lokalita	**Ulice**
Správa akciové společnosti	Okružní
Provoz Špitálka	Špitálka
Provoz Brno-sever	Obřanská
Provoz Červený mlýn	Cimburkova
Provoz Staré Brno	Rybářská
Bystrc	Teyschlova
Kamenný vrch	Svážná

Zdroj: Teplárny Brno

V tabulce 1 je popsán seznam všech klíčových lokalit v síti Tepláren Brno. Spadají sem nevýrobní oblasti s velkým počtem zaměstnanců a také provozy s vysokým instalovaným výkonem.

Menší lokality se dělí na dva typy. Prvním typem jsou malé kotelny nebo výměníkové stanice. Jsou umístěny převážně na sídlištích, kde dodávají tepelnou energii blokům panelových domů.

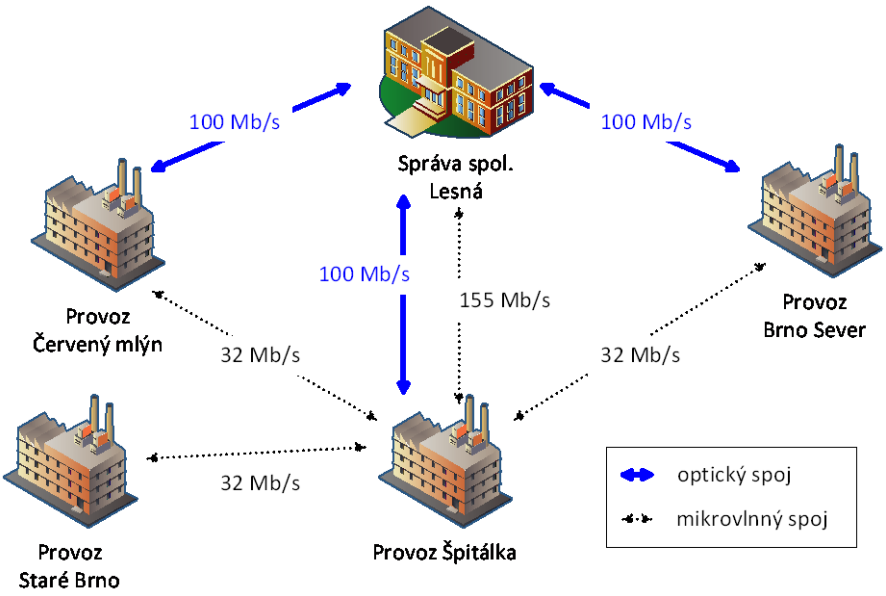
Další typ tvoří podpůrná místa, která se nepodílejí na výrobě elektrické nebo tepelné energie, ale slouží ke komunikaci. Příkladem podpůrného místa s pohledu komunikační sítě je budova Lokotrans v Kohoutovicích, která díky své poloze a výhledu na Brno

poskytuje ideální komunikační uzel pro rádio reléové antény. Kompletní seznam výměníkových stanic a podpůrných míst, připojených do IP sítě, bez rozlišení je uveden v příloze 1. Propojení ostatních neuvedených lokalit popisuji dále v kapitole 2.3.3.

Propojení jednotlivých lokalit a celá komunikační strategie z části vychází z nedávného spojení dvou samostatných sítí – Tepláren Brno a společnosti TEZA. Síť původních Tepláren je dimenzovaná na velkou propustnost a jednotlivé uzly tvoří převážně standardní počítače koncových uživatelů. Původně zajišťovala komunikace mezi relativně málo velkými lokalitami.

Druhou sítí je bývalá síť společnosti TEZA, která propojuje velké množství malých lokalit na území města Brna. Spíše než pro přenos typických uživatelských dat je uzpůsobena pro komunikaci technologických řídících a měřících zařízení.

Jednotlivé lokality, připojené do podnikové datové sítě, jsou v současné době propojeny různým způsobem. Používá se kombinace optických kabelů, bezdrátového mikrovlnného spojení a sítě místních poskytovatelů internetu. Tyto typy spojení můžeme na různých lokalitách najít současně, protože zabezpečují redundantní spojení pro případ výpadku. Na obrázku 2 je ukázka redundantního propojení klíčových lokalit společnosti. Regulace přenosu dat podle vytíženosti jednotlivých spojů je řešena pomocí standardu EIGRP, zabezpečujícího rovnoměrný provoz v síti.



Obrázek 2: Propojení klíčových lokalit (Upraveno dle: Teplárny Brno)

Propojení optickými kabely řeší Teplárny Brno pronájmem od společností Faster CZ spol. s r. o. Využívají je lokality v Bystrci, Komíně, Novém Lískovci, na Vinohradech v Černých Polích a Žabovřeskách. Kromě kotelen a výměníkových stanic ústí toto spojení také v lokalitách správy akciové společnosti na Lesné, provozu Červený Mlýn a Brno-sever. Veškerý provoz po optických trasách společnosti Faster je směrován na provoz Špitálka.

Mnohem větší uplatnění má v komunikaci jednotlivých provozů bezdrátové spojení. Teplárny Brno k tomuto účelu používají převážně licencovaná pásma, aby nedošlo k nežádoucímu rušení signálu. Probíhá-li nějaký přenos v neplaceném pásmu, je v současné době snaha převést jej do placeného.

Tabulka 2: Seznam frekvencí, používaných v bezdrátové síti Tepláren Brno

Kmitočet	Licencované
23GHz	ano
18GMz	ano
11GHz	ano
10GHz	ne
5,5GHz	ne

Zdroj: Teplárny Brno

V tabulce 2 je vidět seznam pásem, používaných Teplárnami při bezdrátovém přenosu dat. K mikrovlnnému propojení slouží soustava rádio-reléových směrových antén, které jsou osazovány ve dvojicích, mířících proti sobě. Všechna v současné době využitá řešení jsou k dispozici v tabulce 3. Uvedená přenosová rychlost není pro dané zařízení maximální, ale jedná se o reálnou komunikační rychlost v tomto konkrétním nasazení.

Tabulka 3: Typy antén, používaných v Teplárnách Brno

Zařízení	Kmitočet	Přen. rychlost
NERA Compact Link 23	23 GHz	32 Mb/s
NERA Evolution METRO 18	18 GHz	155 Mb/s
ALCOMA 18D	18 GHz	
ALCOMA AL 11F	11 GHz	
ALCOMA AL 10D	10 GHz	
Tsunami QuickBridge	5,5 GHz	

Zdroj: Teplárny Brno

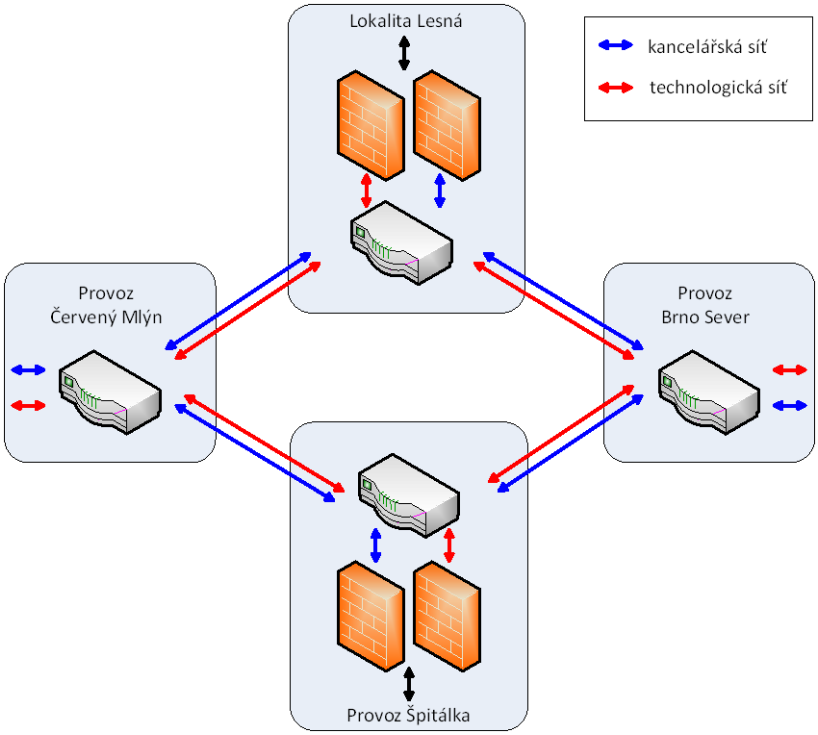
Směrovou anténou je možné vysílat na poměrně velké vzdálenosti. Podmínkou použití takového spojení je však dobrá viditelnost s minimálním počtem překážek. Přípojné anténní body v tomto případě nelze osadit na všechny potřebné lokality.

U lokalit, postrádajících dobrou viditelnost na některý další přípojný bod a bez možnosti připojení pomocí optických kabelů je využíváno sítě operátora Netbox společnosti SmartCom, a.s. Veškerá komunikace je tunelována na provoz Špitálka.

2.3.2 Sítě a podsítě

Na síť Tepláren Brno můžeme pohlížet z několika pohledů. Budeme-li k dělení přistupovat z pohledu účelu, můžeme síť rozdělit na technologickou a kancelářskou. Toto označení budu používat v následujících kapitolách.

Z pohledu místního a provozního ji můžeme zase rozdělit na několik podsítí, které jsou provozovány v jednotlivých lokalitách nebo se v případě provozních sítí prolínají více lokalitami. Tyto sítě jsou pak podmnožinou účelového dělení sítě.



Obrázek 3: Schéma provozu kancelářské a technologické sítě na jedné spojnici (Upraveno dle: Teplárny Brno)

Technologická a kancelářská síť jsou realizovány na stejných fyzických spojnicích s požadavkem na jejich separaci. Na úrovni 2. vrstvy zajišťuje řešení standard IEEE 802.1Q, díky kterému jsou od sebe virtuální sítě odděleny při komunikaci mezi jednotlivými přepínači. Na páteřních směrovačích Cisco je potom implementována technologie VRF-lite, která umožňuje přenos několika virtuálních LAN po jedné

fyzické spojnici. Na obrázku 2 v na straně 17 je vidět, že páteřní spojnice sítě jsou vedeny po více fyzických trasách, z čehož vyplývá potřeba optimálně rozložit provozní zátěž. Vyrovnaný provoz zajišťuje na každé ze sítí (kancelářské i technologické samostatně) protokol EIGRP.

Komunikace technologické a kancelářské sítě probíhá přes vyhrazené firewally. Primární je umístěn v lokalitě správy akciové společnosti na Lesné, záložní v provozu Špitálka. Schéma rozdělení kancelářské a technologické sítě společně s použitými firewally je vidět na obrázku 3.

Nedílnou součástí dvou hlavních sítí jsou i logické podsítě, definované rozsahy IP adres. Jejich zkrácený výčet bez uvedení IP rozsahů je v tabulce 4. V každé lokalitě navíc kromě uvedených fungují také rozsahy pro podpůrné systémy.

Tabulka 4: Logické podsítě podle zaměření a rozsahu IP adres

Lokalita	Kancelářské	Technologické
Správa společnosti	servery + PC + tiskárny	směrovače + teplota + UPS + docházka
	bezdrátová síť zaměstnanci	přepínače
	bezdrátová síť návštěvy	bezpečnost
Provoz Špitálka	servery + PC + tiskárny	stanice operátorů
	bezdrátová síť zaměstnanci	měřící stanice staré
	bezdrátová síť návštěvy	kamery + měřící stanice + docházka
		přepínače
Provoz Brno-Sever	PC + tiskárny	převodníky staré
		převodníky + měřící stanice + UPS + docházka
		přepínače
Provoz Červený Mlýn	PC + tiskárny	převodníky + stanice staré
	bezdrátová síť zaměstnanci	převodníky + stanice nové + docházka
	bezdrátová síť návštěvy	přepínače
Provoz Staré Brno	PC + tiskárny	převodníky
		přepínače
		docházka

Zdroj: Teplárny Brno

Z hlediska rozsahu IP adres, nastíněného v tabulce 4, je vidět rozdělení na stále se opakující podsítě s jasnou strukturou. Kancelářská síť se dělí na pracovní stanice s tiskárnami, bezdrátovou síť pro zaměstnance a bezdrátovou síť pro návštěvy. Dělení technologické sítě ve výrobních lokalitách je jednoduché. První podsíť obsahuje technologická zařízení, měřící stanice, kamery, docházkový systém a veškeré provozní

přístroje, zatímco druhá obsluhuje management přepínačů. Dublování sítí v jednotlivých lokalitách je dáno rozsahy IP adres, které se v daných případech používají. Zatímco nově nasazované technologie využívají IP adresy třídy C, původní technologická zařízení a stanice jsou adresována v sítích třídy A.

V síti je momentálně používán systém ručního přidělování statických IP adres bez použití DHCP serveru.

2.3.3 Uzly

Stejně, jako můžeme síť dělit na technologickou a kancelářskou, tak podle jejich účelu můžeme dělit také uzly na standardní kancelářské a technologické.

Koncovými uzly kancelářské sítě jsou standardní stanice PC s operačními systémy, založenými na platformě Windows. Seznam používaných operačních systémů a podpory IPv6 je v tabulce 4.

Tabulka 5: Operační systémy v kancelářské části sítě Tepláren Brno

OS	**IPv6**
Windows Server 2003	nekompletní
Windows Server 2003 R2	nekompletní
Windows Server 2008	ano
Windows Server 2008 R2	ano
Windows XP Professional SP2	nekompletní
Windows Vista	ano
Windows 7	ano

Upraveno dle: Teplárny Brno; Tulloch, 2006

Podpora protokolu IPv6 u operačních systémů Microsoft se dá rozdělit na produkty, které mají podporu plně implementovanou a poté produkty, u kterých je v tabulce uvedeno „nekompletní“. U těch je potřeba IPv6 nejdřív doinstalovat a ani po instalaci se nejedná o podporu v plném rozsahu. Jedná se spíše o experimentální rozšíření. Chybí například možnost Teredo, DHCPv6 nebo služba vzdálené plochy. U Windows server 2003 nejsou pod IPv6 dostupné všechny funkce Active Directory nebo MS Exchange (Microsoft, 2003).

Kromě základních typů koncových počítačů se v kancelářské síti vyskytují specifická zařízení, která jsou nedílnou součástí firemní IT infrastruktury. Jedná se především o síťové tiskárny, zálohovací zařízení anebo samostatná disková pole, která sice ke své

práci nepotřebují přímo síťové spojení, ale toto se využívá například pro jejich management a sledování stavu. Typy těchto zařízení jsou uvedeny v tabulce 6.

Tabulka 6: Další zařízení kancelářské sítě

Zařízení	Výrobce	Typ	IPv6
pásková knihovna	IBM	TS3100	ano
pásková knihovna	IBM	TS3200	ano
UPS	APC	Symmetra	ne*
UPS	APC	Smart 2200VA	ne*
tiskárna	HP	M1536dnf	ano
tiskárna	HP	LJ 1300	ne
tiskárna	HP	LJ 4200	ne
tiskárna	HP	DJ 5550	ne
tiskárna	Kyocera	FS-3900DN	ne
tiskárna	Kyocera	FS-C5100N	ano
tiskárna	Kyocera	FS 9530DN	ne
tiskárna	Kyocera	FS-9520DN	ne
tiskárna	Kyocera	FS-C5015N	ne
tiskárna	Kyocera	KM-2540	ne
tiskárna	Kyocera	KM-1650	ne
tiskárna	Kyocera	KM-C2525E	ne
tiskárna	Kyocera	FS-3900DN	ne
tiskárna	Kyocera	KM-C850D	ne
tiskárna	Kyocera	FS-1350	ne
tiskárna	Kyocera	TaskAlfa 250	ne
tiskárna	Kyocera	TaskAlfa 181	ne

Upraveno dle: Teplárny Brno; Haeusser, 2008; APC, 2012; Kyocera, 2012

Z tabulky 6 vyplývá, která zařízení jsou připravena pro protokol IPv6. Výjimkou jsou záložní zdroj APC, které jsou modulární a podporu IPv6 protokolu lze docílit přidáním modulu s IPv6 síťovou kartou. UPS v síti lze následně hromadně spravovat pomocí software APC PowerChute, který ale v současné verzi (3.0.1) neumožňuje dálkovou správu zařízení, komunikujících na IPv6 (APC, 2012; Schneider Electric, 2012).

Magnetopáskové knihovny IBM TS3100 a 3200 jsou na protokol IPv6 připraveny a podporují také standard dvojího zásobníku (Haeusser, 2008, s. 515).

Jednotlivé uzly technologické sítě jsou reprezentovány specifickými typy zařízení. Jedná se o uzly, jejichž úkolem je konvertovat signál z technologických sériových linek, jako je např. RS-485, nebo specializovaných technických sítí typu LonWorks a BACNet na IP Ethernet. Teplárny Brno k tomuto účelu používají řešení MetaSys od firmy Johnson Controls. Centrálními uzly technické sítě jsou jednotky NCU, osazované Ethernetovými převodníky řady NCM350.

Jednotky NCU s převodníky NCM350 jsou osazeny ve většině malých technických provozů, vyjmenovaných v příloze 1. Sběr dat z ostatních provozů probíhá prostřednictvím standardů RS-485, vedených metalickými linkami nebo prostřednictvím radiomodemů. Linky z určitého okolí jsou v každé oblasti svedeny do centrálního bodu, osazeného NCU.

Jednotky řady NCM350 momentálně podporou protokolu IPv6 nedisponují. V současné době také již firma Johnson Controls k technologiím postaveným na NCM350 neposkytuje žádnou technickou podporu formou upgrade, jelikož jsou zastaralé. Dá se tedy předpokládat, že v případě kompletního přechodu bude třeba toto řešení nahradit jiným (Šesták).

Tabulka 7: Zařízení technologické části sítě

Zařízení	**Výrobce**	**Typ**	**IPv6**
RS 485 -> Ethernet	Papouch		ne
NCU	Johnson Controls	NCM350	ne
docházka	Latronix	Xport	ne
teploměr	Papouch		ne
UPS	APC	1500	ne
UPS	APC	Smart 2200VA	ne*

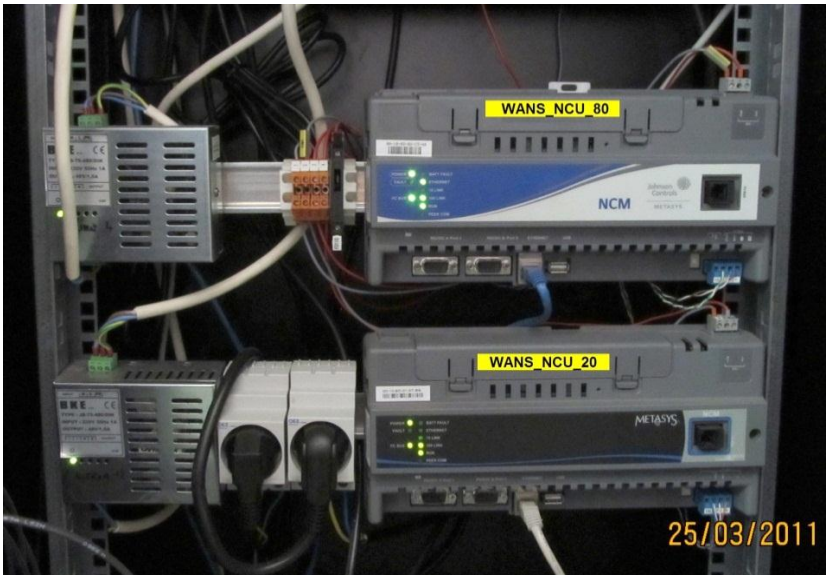
Upraveno dle: Teplárny Brno; Šesták; Lantronix, 2011; Papouch, 2012; APC, 2012

V tabulce 7 je zobrazen přehled zařízení technologické části sítě. Většina technologických funkcionalit, které nejsou zahrnuty do segmentu Metasys, je řešena právě převodníky z RS-485 nebo RS-232 na Ethernet. Do technologické oblasti jsem přidal také zařízení, která se přímo nepodílejí na výrobě a technologickém zajištění provozu, ale přesto jsou potřebná pro řízení a sledování.

Kromě toho je v tabulce 7 uveden ještě segment, který s technologií nesouvisí, ale spadá sem svou povahou mnohem více, než do kancelářské sítě. Jedná se o systém kontroly docházky, který je založený na on-line ověření čipové karty. Dodavatelem řešení je společnost Z-ware, která ve svých zařízeních používá ethernetové převodníky Lantronix X-port.

Jak je vidět, klíčové síťové prvky technologické sítě nejsou na přechod z velké části připraveny. Je-li možnost nějakého upgradu, například firmwaru, jedná se spíše o možnost teoretickou, která v současné době funguje v určitém experimentálním režimu.

Pro většinu dodavatelů je ale rentabilnější dodávat nová zařízení, než pracovat na úpravě stávajících.



Obrázek 4: Ukázka osazení převodníků NCM (Zdroj: Teplárny Brno)

2.3.4 Aktivní prvky

V síti Tepláren Brno se v současné době využívá několik typů aktivních prvků od různých výrobců. Nejpoužívanější značkou aktivních prvků jsou směrovače (routery) a přepínače (switche) firmy Cisco. Následující tabulka uvádí jednotlivé zástupce použitých aktivních prvků v kancelářské i technologické části sítě.

Tabulka 8: Aktivní prvky a jejich podpora protokolu IPv6

Výrobce	Typ	Podpora IPv6	Zařízení
Cisco	3620	ano	směrovač
Cisco	1605	ne	směrovač
Cisco	887VA	ano	směrovač
Taunet	Mikrotik	ano	směrovač
Cisco	Catalyst 3750	ano	L3 přepínač
Cisco	WS-C2960-48TC-L	MLD, management	přepínač
Cisco	WS-C2960-24TC-L	MLD, management	přepínač
Cisco	WS-C2960G-24TC-L	MLD, management	přepínač
Cisco	WS-C2960-8TC-L	MLD, management	přepínač
Edimax	ES-5224RM+	ne (! management IPv4)	přepínač
Edimax	ES-3124RL	ne	přepínač
3com	4200G	ne	přepínač

Zdroj: Teplárny Brno, Cisco Systems, 2012a; Edimax Technology, 2012; Mikrotik, 2011

Z tabulky 8 vidíme, že většina v současnosti použitých zařízení přechod na IPv6 podporuje. V případě dolní části tabulky, ve které jsou uvedeny přepínače, není podpora IPv6 nutně vyžadována, protože tyto pracují na linkové vrstvě, zatímco IP protokol na vrstvě síťové (Peterka, 1997). Problém může nastat u těch přepínačů, které nabízejí port management a zároveň nepodporují IPv6. Typickým příkladem je Edimax ES-522RM+. Jako protipól tomuto zařízení můžeme postavit Cisco WS-C2960-24TC-L, které podporuje nejenom management na IPv6, ale i MLD[1] (Cisco Systems, 2012a).

Cisco887VA, uvedený v tabulce 8, slouží ke směrování provozu do ADSL sítě a pro komunikaci s elektrickým operátorem ČEPS.

V případě směrovače, postaveného na technologii Mikrotik, je podpora protokolu IPv6 závislá především na implementovaném systému Mikrotik RouterOS. Ten je postavený na Linuxovém jádře a od verze 3 už protokol IPv6 podporuje (Mikrotik, 2011).

2.3.5 Bezpečnost

Kancelářská část sítě je zabezpečena protokolem IEEE 802.1X, který umožňuje, aby byl přístup počítače do sítě autorizován. Řešení vyžaduje spravovatelné přepínače a online systém pro správu pověření, který by uzly na základě autentizace autorizoval k přístupu do sítě. Zařízení se autentizují vůči RADIUS serveru (v tomto případě Cisco ACS server), který v případě úspěchu autorizuje příslušný port. V opačném případě je port autorizován pouze do omezené VLAN. Zde je umožněn přístup k internetu a omezená komunikace s vnitřní sítí.

Jako centrální bezpečností firewall jsou nasazeny dvě dvojice zařízení Cisco ASA 5510 Security Plus. Jejich rozložení a umístění je patrné z obrázku 3 v kapitole 2.3.2. Každá dvojice pracuje v redundantním zapojení, což umožňuje zachování síťového toku v případě výpadku jednoho zařízení. Právě tato zařízení od sebe také oddělují technologickou a kancelářskou síť, přičemž každá z nich je přivedena na jiný port firewallu. Tímto způsobem je možné sledovat a omezovat datový provoz mezi dvěma vnitřními sítěmi.

[1] Multicast Listener Discovery – umožňuje menší zatížení sítě v případě IPv6 multicastu prostřednictvím směrování paketu pouze na relevantní uzly v síti

3 Teoretická východiska

3.1 Stručná historie internetu

Historie internetu tak, jak ho známe dnes, se začala psát na konci šedesátých let minulého století v USA. Ministerstvo obrany zadalo firmě RAND Corporation nelehký úkol, vymyslet síť, která bude provozuschopná i v případě velkého poškození. RAND tehdy přišla s netradičním nápadem, decentralizovat řízení sítě a vytvořit systém rovnocenných uzlů, které si mezi sebou budou posílat malé fragmenty dat. Jakou cestou se data dostanou od odesílatele k příjemci, není důležité. Hlavní je, aby zpráva dorazila v celku.

Koncept byl velmi rychle uveden do praxe a v roce 1969 vznikla síť ARPANET, která měla původně sloužit pro předávání tajných vojenských zpráv. Pouze u vojenské aplikace nezůstalo. ARPANET začaly využívat univerzity pro vědeckou činnost a velmi brzy se síť stala oblíbenou díky jednoduchému zasílání elektronických zpráv.

Zlom ve vývoji internetu přišel v roce 1982, kdy byl definován standard ICP/IP, umožňující propojit téměř neomezené množství heterogenních sítí. Od této doby již nic nebránilo masovému rozšíření internetu (Krčmář, 2008, s. 20).

Internet získával stále větší popularitu a rozšiřoval se. Na začátku 90. let bylo jasné, že IPv4 adresy brzy začnou docházet a bylo třeba tento problém začít řešit. Úkolu se zhostilo IETF[1], které se kromě zvětšeného adresního prostoru rozhodlo navrhnout zásadní změny ve fungování.

V roce 1995 byla vydána sada RFC[2], která definuje vlastnosti a chování nového protokolu IPv6. Bylo tedy možné s předstihem začít implementovat tento nový protokol do praxe (Satrapa, 2008, s. 17).

Protokol ale v praxi uplatnění nenašel. Spousta firem měla nakoupený HW, podporující IPv4, a přechod na nový komunikační standard by pro ně byl kvůli nutnosti vyměnit

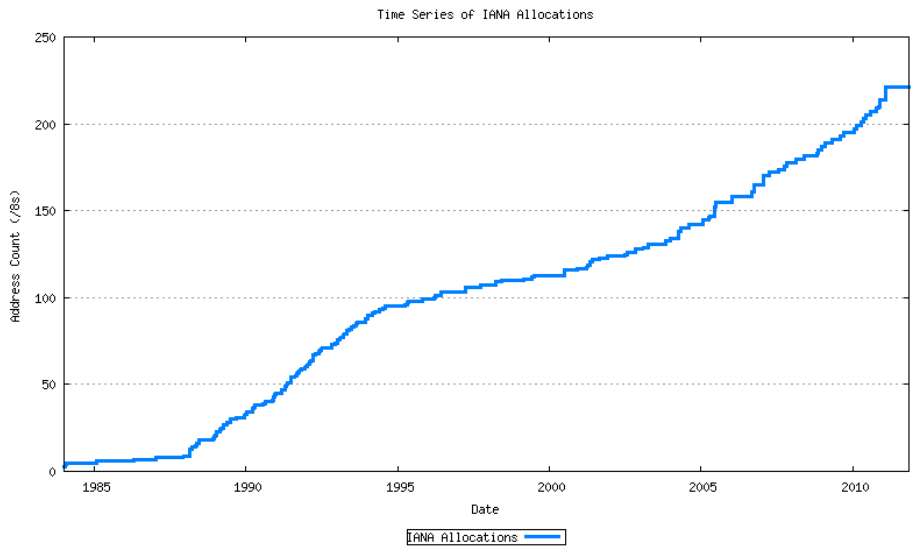
[1] Internet Eningeneering Task Force – „Pracovní skupina techniky internetu“, mající na starosti vývoj internetových standardů

[2] Request for Comments – označení standardů, popisujících internetové protokoly

všechna zařízení příliš drahý. Místo nasazování IPv6 dochází k úpravám IPv4 tak, aby se co nejvíce oddálil moment, kdy budou všechny adresy vyčerpány. Tento stav trvá dodnes, i když je už dlouhou dobu jasné, že pokud si budeme chtít zachovat možnosti internetu tak jak ho známe, jinou možnost než přechod na IPv6 nemáme.

3.2 Nedostatek IPv4 adres

Protokol IP verze 4 používá k jednoznačnému určení rozhraní adresy, skládající se ze 4 bajtů. Má-li jedno zařízení více rozhraní, každé má svou unikátní adresu. Z toho vyplývá, že do sítě můžeme teoreticky připojit nejvýše 2^{32} rozhraní. Ne všechny adresy ale můžeme použít. Některé z nich jsou rezervované pro speciální účely, zahrnující mimo jiné fungování protokolu (např. 255.255.255.255 = broadcast, 127.0.0.0 = loopback, atd.) (RFC 5735, s. 3-5).



Obrázek 5: Kumulativní graf počtu IANAou přidělených IPv4 adres v blocích po 2^{24} (Zdroj: Huston, 2011)

Rozdělíme-li adresní prostor na podsítě podle třídy A[1], dostaneme 256 podsítí, každou s možností adresovat 2^{24}-2 dalších rozhraní (Dostálek; Kabelová, 2000, s. 156). Geoff Huston (2011) spočítal, že podle RFC 5735 je 35,078 těchto podsítí rezervováno pro speciální účely a dalších 220,922 je k dispozici pro přidělování IP adres. Počet zařízení, které tak můžeme adresovat, se tímto zmenšuje na cca 3 706 456 113, což je číslo na

[1] teoretické rozdělení IP adresy na část, označující síť a část, označující rozhraní v síti. Třída A používá první bajt adresy jako identifikátor sítě a další 3 bajty jako identifikátor rozhraní.

první pohled velké. Vezmeme-li ale v úvahu dnešní využití informačních technologií, počty zařízení, připojených k internetu, a virtuální servery, zjistíme, že opak je pravdou.

Na obrázku 5 je graf, znázorňující časovou osu a kumulativní záznam přidělování IPv4 adres společností IANA. Od 3. února 2010 je hodnota přidělených adres konstantní a nezvyšuje se, protože právě k tomuto datu došlo k jejich vyčerpání. Jednotliví oblastní registrátoři RIR mají ještě k dispozici určité volné adresní prostory, ale ty se také velmi rychle tenčí. Je tak otázkou pár let, kdy bude adresní prostor zcela vyčerpán (Huston, 2011).

3.3 Adresy IPv6

V této kapitole popíšu některé vlastnosti protokolu IPv6. Zaměřím se hlavně na odlišnosti od IPv4 s tím, že shodné vlastnosti uvedu okrajově pouze pro upřesnění anebo se jim zcela vyhnu.

3.3.1 Formát adres

Jak již bylo řečeno v kapitole 3.2, hlavním hnacím motorem pro přechod na IPv6 je nedostatek adres ve stávající verzi IPv4. Tato oblast doznala zásadní změny.

Velikost IP adresy byla u verze 6 stanovena na čtyřnásobek verze 4. Nově tak máme k dispozici 16bajtovou adresu, celkem 128 bitů. Počet teoreticky přidělitelných adres se vyšplhal na 2^{128} (RFC 2460, s. 2).

Při velikosti adresy 16 bajtů je ale velmi nepohodlné používat starý způsob identifikace v dekadické soustavě. Je tedy nutné přistoupit k novému způsobu zápisu.

3.3.2 Způsob zápisu adres a prefixu

U protokolu IPv6 se využívá zápisu pomocí osmi skupin po čtyřech číslicích šestnáctkové soustavy, vyjadřujících hodnoty 16 bitů dlouhých částí adresy. Navzájem jsou od sebe odděleny dvojtečkou (Satrapa, 2008, s. 52). Na velikosti písmen při zápisu adresy nezáleží (RFC 5952, s. 6).

Příkladem IPv6 adresy může být hodnota

fedc:ba98:7654:3210:fedc:ba98:7654:3210.

Nový způsob zápisu IPv6 adresy se může zdát nepřehledný a takřka nezapamatovatelný. V porovnání s adresou IPv4, popsanou v kapitole 3.2, se při manuálním zadání vystavujeme většímu riziku chyby. Proto existují mechanismy, které dovolují adresu při dodržení standardů vizuálně zkrátit.

Velmi častou číslicí v adrese je nula, kterou můžeme vynechat, pokud je počátečním znakem čtveřice. Hodnotu „0012“ můžeme zapsat jenom jako „12“ a hodnotu „0000“ jako „0“. Nelze ji ovšem ignorovat, pokud se nachází uvnitř nebo na konci řetězce. Například „1200“ nelze zkrátit vůbec a řetězec „0120“ můžeme zapsat jako „120“. Podmínkou je, že v každém poli musí zůstat alespoň jedna číslice (kromě výjimky, uvedené níže) (RFC 5952, s. 4).

Adresa

1080:0000:0000:0000:0008:0800:200C:417A

bude po zkrácení o nadbytečné nuly vypadat následovně:

1080:0:0:0:8:800:200C:417A.

Další forma zkrácení je realizována možností vynechat pole, kde se opakují pouze nuly. Pole s nulovou hodnotou se nahradí znakem „::“. Platí ale, že tuto možnost lez využít pouze jednou v celé adrese (RFC 5952, s. 5). Dříve uvedená adresa by se podle tohoto schématu dala zapsat jako

1080::8:800:200C:417A.

Extrémem může být nedefinovaná adresa

0000:0000:0000:0000:0000:0000:0000:0000

kterou můžeme nahradit zkratkou

:: (RFC 5952, s. 5).

Jak je vidět, adresní prostor je velký a aby bylo možné se v něm lépe orientovat, je vhodné jej rozdělit na sítě a podsítě. Na rozdíl od protokolu IPv4, který má možnost nastavit rozdělení na podsítě buďto pomocí vyjádření prefixu nebo masky, má IPv6 k dispozici pouze identifikací pomocí prefixů. Prefix je počáteční část adresy, která je

shodná pro všechny adresy v síti nebo podsíti. Jeho délka může být různá a záleží na tom, s jakou podrobností chceme adresy rozlišovat (Satrapa, 2008, s. 53).

Délka prefixu se zapisuje ve formátu odvozeného ze zápisu CIDR v případě IPv4 jako

IPv6-adresa/délka-prefixu

kde IPv6 adresa je zapsána ve standardním formátu a délka prefixu, zapsaná v decimálním tvaru, určuje, kolik bitů z počáteční části adresy je považováno za prefix (RFC 4291, s. 5).

3.3.3 Typy adres

Protokol IPv6 dává, stejně jako jeho předchůdce, možnost posílat data pouze pro jedno rozhraní nebo pro skupinu. Tyto adresy dělíme podle typu a chování na následující:

Unicast (individuální) slouží k identifikaci jediného rozhraní. Paket odeslaný na unicast adresu je doručen pouze zamýšlenému příjemci.

Anycast (výběrová) je novinkou protokolu IPv6. Používá se pro identifikaci skupiny rozhraní (typicky různých uzlů). Paket poslaný na anycastovou adresu je doručen pouze tomu rozhraní, které je identifikováno jako nejbližší.

Multicast (skupinová) se chová obdobně jako anycast. Rozdílem je, že paket zaslaný na multicast adresu je doručen každému rozhraní ve skupině.

Broadcastové adresy nejsou v protokolu IPv6 podporovány a jsou nahrazeny multicastovými (RFC 4291, s. 2-3).

Jeden z hlavních rozdílů protokolu IPv6 oproti svému předchůdci spočívá v počtu přidělených IP adres pro jedno rozhraní. Verze 6 může, a dokonce je to vyžadováno, přiřadit jednomu rozhraní více adres pro různé účely (viz též kapitolu 3.3.8) (RFC 4291, s. 17). Některé typy adres mají rezervovanou svou hodnotu nebo prefix sítě.

Tabulka 9: Základní rozvržení adres

prefix	Význam
::/128	nedefinovaná adresa[1]
::1/128	smyčka (loopback)
fc00::/7	unikátní individuální lokální
fe80::/10	individuální lokální linkové
ff00::/8	skupinové adresy (multicast)
ostatní	individuální globální

Zdroj: Satrapa, 2008, s. 54

Jak je vidět z tabulky 9, většinu adres zabírají globální individuální adresy. Z jejich prostoru se zatím používá pouze prefix 2000::/3 a zbytek zůstává nepřiřazen (Satrapa, 2008, s. 54).

Přechodové mechanismy, kterým se budu podrobněji věnovat v kapitole 3.5, potřebují občas přetransformovat adresy IPv4 do IPv6. K tomu slouží tzv. IPv4 mapované adresy. Jejich prvních 80 bitů je nulových, následuje 16 jedničkových a v posledních 32 bitech je zapsána vlastní IPv4 adresa (Satrapa, 2008, s. 53). Například IPv4 adresu

147.229.2.90

můžeme mapovat na IPv6 ve tvaru

::ffff:93e5:025a.

Kromě IPv4 mapovaných adres jsme se v minulosti mohli setkat ještě s adresami IPv4 kompatibilními. Ty se od mapovaných liší prostředními 16 bity, které nabývají místo jedniček hodnoty nulové. V současné době jsou ale zavržené a smí se používat pouze IPv4 mapované adresy (RFC 4291, s. 10).

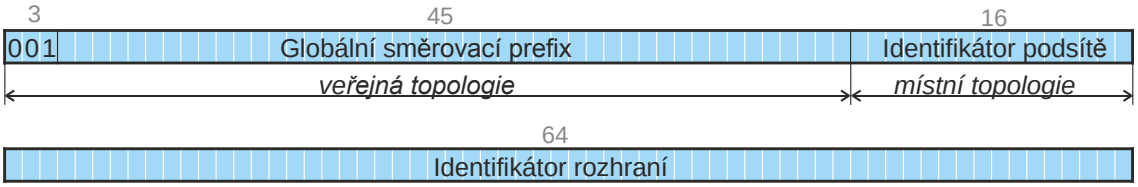
3.3.4 Globální individuální adresy

Globální individuální adresy jsou nejdůležitější částí tabulky 9 a jedná se o ekvivalent dnešních veřejných adres IPv4. Přidělování adres funguje obdobně jako v CIDR u IPv4. Poskytovatel připojení k internetu obdrží určitý prefix, jehož části v podobě dalších prefixů se stejným začátkem pak přiděluje svým zákazníkům. Cílem této hierarchie je

[1] nedefinovaná adresa říká, že dotyčnému zařízení dosud nebyla přidělena IPv6 adresa (RFC 4291, s. 9)

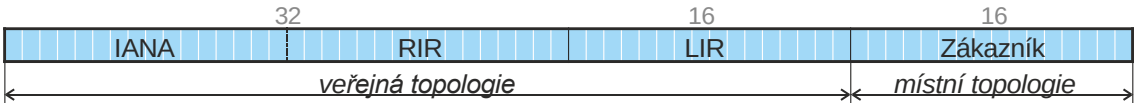
snaha o minimalizaci směrovacích tabulek a o to, aby šlo při pohledu zvenčí popsat celou podsíť jediným záznamem v tabulce (Satrapa, 2008, s. 55).

V současné době se IPv6 adresa dělí na tři části: globální směrovací prefix, identifikátor podsítě a identifikátor rozhraní. Jejich délka není podle RFC 4291 (s. 9) definována, ale Satrapa (2008, s. 56) uvádí, že podle současných pravidel pro přidělování je pro globální směrovací prefix vyhrazeno 48 bitů, adresa podsítě má 16 bitů a identifikátor rozhraní v podsíti zabírá posledních 64 bitů. Rozdělení znázorňuje obrázek 6.



Obrázek 6: Struktura globální individuální adresy (Upraveno dle: Satrapa, 2008, 56)

Globální směrovací prefix (global routing prefix) identifikuje koncovou síť a je z pohledu zákazníka přidělován lokálním internetovým registrátorem (LIR), což je zpravidla poskytovatel internetu. Ve skutečnosti je rozdělen na několik částí podle organizací, které danou část přidělují (Satrapa, 2008, s. 87).



Obrázek 7: Struktura globálního prefixu podle toho, kdo přiděluje jednotlivé části (Upraveno dle: Satrapa, 2008, s. 89)

Jak je vidět z obrázku 7, čím vyšší bit, tím více se zpřesňuje informace o poloze rozhraní. RIR značí zkratku regionálního internetového registrátora[1].

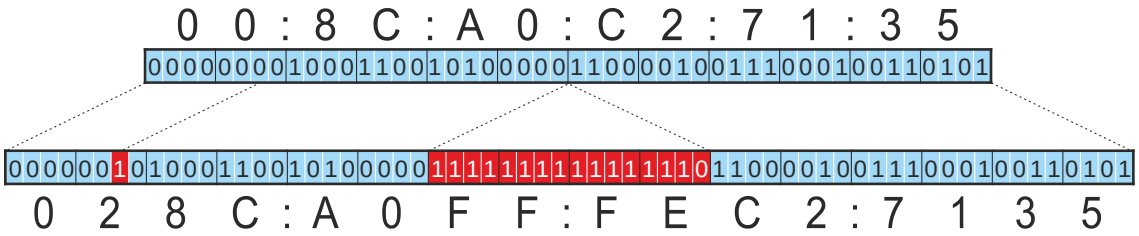
Identifikátor podsítě slouží pro identifikaci podsítě například v rámci firmy. V jedné síti je možnosti mít 2^{16} podsítí, což je dostatečné množství. Díky tomu není nezbytné šetřit při rozdělování podsítí „každý bit“ (Satrapa, 2008, s. 56-57).

[1] v současné době je 5 regionálních registrátorů, jejichž seznam je k dispozici na http://www.iana.org/numbers

Identifikátor rozhraní je se svými 64 bity nejdelší částí celé adresy. Protože jednoznačně určuje rozhraní, v rámci podsítě musí být jedinečný, aby nedošlo ke kolizi (RFC 4291, s.7).

V současné době slouží podle RFC 4291 (s. 8) jako identifikátor rozhraní modifikovaný EUI-64. To je identifikační kód s délkou 64 bitů, který lze vygenerovat pro různá zařízení. Rozhraní, identifikovatelná prostřednictvím ethernetové (MAC) adresy, získají EUI-64 tak, že je mezi 3. a 4. bajt vložena hodnota $FFFF_{16}$ nebo $FFFE_{16}$ (IEEE, 1997). Pro modifikované EUI-64 platí, že je vždy vkládána hodnota $FFFE_{16}$ a zároveň je nastavená hodnota druhého nejméně významného bitu nejvýznamnějšího bajtu[1] na 1 v případě globálního identifikátoru a na 0 v případě lokálního[2] (RFC 4291, s. 8; Satrapa, 2008, s. 58).

Na obrázku 8 je znázorněn převod z MAC adresy 00:8c:a0:c2:71:35 na identifikátor rozhraní.



Obrázek 8: Převod z ethernetové adresy na EUI-64 (Upraveno dle: Satrapa, 2008, s. 58)

Nebezpečným aspektem použití EUI-64 jako identifikátoru rozhraní je ztráta anonymity. Každé rozhraní podle tohoto schématu bude mít svůj identifikátor rozhraní na úrovni globální individuální adresy neměnné. Takové zařízení pak může být velmi jednoduše sledováno a monitorováno a to i za předpokladu, že změní svoji polohu (Satrapa 2008, s. 58).

Na tento problém reaguje norma RFC 4941, která místo EUI-64 navrhuje náhodné generování identifikátorů, které se budou v intervalech hodin až dní měnit. Nevýhoda tohoto řešení je to, že rozhraní s takovým identifikátorem není jednoduché kontaktovat zvenčí.

---

[1] používá se big-endian – nejvýznamnější bity (a bajty) jsou první zleva

[2] tato možnost se používá například u místních sériových linek (Satrapa, 2008, s. 58)

Průnikovým řešením předchozích dvou možností je, že počítač bude mít adresu s identifikátorem získaným na základě EUI-64 zavedenou v DNS. Aktivně bude ale navazovat spojení pod adresou, ve které bude využívat náhodně generovaný identifikátor (Satrapa, 2008, s. 59).

3.3.5 Lokální adresy

Lokální adresy jsou dalším velmi důležitým identifikátorem rozhraní. Na rozdíl od globálních slouží k identifikaci pouze v lokální síti, popřípadě na jednom místě[1] (Satrapa, 2008, s. 59).

Nejvýznamnější jsou **lokální linkové adresy** (anglicky link local), jejichž adresa začíná prefixem fe80::/10 (viz tabulku 9). Zbývající část adresy je vyplněna nulovými bity a do pravé části je vložen šedesáti-čtyřbitový identifikátor rozhraní, generovaný podle EUI-64 (RFC 4862, s. 11-12; Satrapa, 2008, s. 60).

Počátek adresy je v tomto případě chápán jako adresa sítě a podsítě. Nedá se ale použít ke směrování, což je logické vzhledem k tomu, že je ve všech sítích stejný. Jakákoliv takováto adresa tudíž neprojde směrovačem (Satrapa, 2008, s. 60).

Velkou výhodou lokální linkové adresy je její jednoduché vytvoření, ke kterému nejsou kromě EUI-64 potřebné žádné další informace. Počítač je tudíž schopen si adresu vytvořit sám, díky čemuž je lokální linková adresa k dispozici vždy. Následně si pomocí nástrojů automatické konfigurace (více se jí budu věnovat v kapitole 3.4.4) ověří, že je v lokální síti skutečně jedinečná. Existenci lokálních linkových adres používá například automatická konfigurace pomocí DHCP (Satrapa, 2008, s. 60-61).

Dostaneme-li se do situace, kdy potřebujeme zabezpečit komunikaci mezi více oddělenými sítěmi, například pobočkami společnosti v různých městech, lokální linkové adresy nemůžeme použít, jelikož pomocí nich není možné identifikovat cílovou síť a podsíť. Respektive můžeme, za předpokladu, že vytvoříme tunelové spojení. IPV6 ale nabízí elegantnější řešení, kterým jsou **unikátní lokální adresy**, popsané v RFC 4193. Jejich prefix je fc00::/7, který je následován jednobitovým příznakem L, nabývajícím v případě lokálně generované adresy hodnoty 1. Varianta, kdy L nabývá 0, není zatím

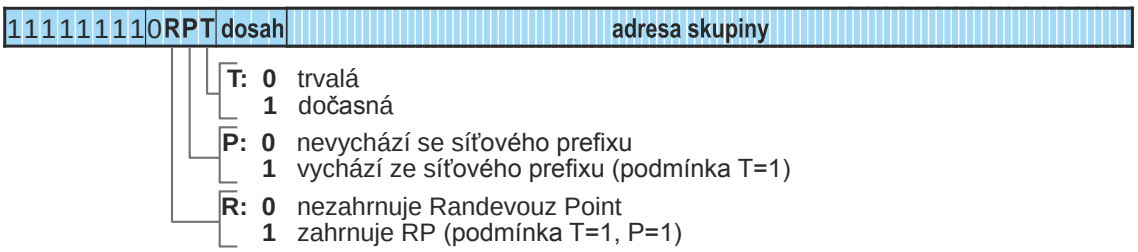
[1] pojmem místo je myšleno více navzájem propojených sítí, například provozoven jedné firmy

v normách definována. (RFC 4293, s. 3). Satrapa (2008, s. 61) se domnívá, že v pozadí této možnosti čeká myšlenka centrální autority, která by v případě adres s L = 0 ručila za celosvětovou jednoznačnost unikátních lokálních adres. Jestli bude něco takového v budoucnu navrženo, to dnes ještě nevíme.

Kombinaci prefixu a hodnoty L při současných pravidlech můžeme nahradit hodnotou prefixu fd00:/8. Za ní se nachází 40ceti bitový globální identifikátor, který dle RFC 4193 (s. 5) musí být vždy generován pseudonáhodně. Následuje 16 bitů dlouhý identifikátor podsítě, přičemž se předpokládá, že stejný identifikátor nese také globální individuální adresa (viz kapitola 3.3.4), je-li přidělená poskytovatelem internetu. Řetězec opět uzavírá identifikátor rozhraní z modifikovaného EUI-64 (RFC 4193, s. 3-7).

3.3.6 Skupinové (multicast) adresy

Skupinové adresy slouží především k distribuci multimediálního obsahu v reálném čase. Oproti protokolu IPv4 zde v základním principu fungování nedochází k žádné velké revoluci (Satrapa, 2008, s. 62). V průběhu vývoje došlo k více možnostem, jak vytvořit skupinové adresy. Základní kostra je zobrazená na obrázku 9.



Obrázek 9: Struktura skupinové adresy (Upraveno dle Satrapa, 2008, s. 63)

Prvních osm bitů je neměnných a signalizují, že se jedná o skupinovou adresu. Následující čtyři bity jsou určené pro příznaky. První bit čtveřice je zatím rezervován a jeho účel ještě nebyl stanoven. Musí tak vždy nabývat hodnotu 0.

Příznak **T** (transient) říká, zda je adresa přidělena trvale (T = 0) nebo dočasně (T = 1). Trvalé adresy přiděluje IANA, kdyžto dočasné si aplikace generují samy. V praxi se více setkáváme s dočasně vytvořenými adresami (Satrapa, 2008, s. 62 – 63).

Pokud je skupinová adresa generována dočasně, je třeba ošetřit, aby nedošlo k přidělení dvou shodných adres. Tento problém řeší RFC 3306, které zavádí skupinové adresy,

vycházející z individuálních. Rozlišení je provedeno na základě příznaku **P**, majícího pro skupinovou adresu obsahující prefix sítě hodnotu P = 1 a pro adresy, nezaložené na síťovém prefixu hodnotu P = 0 (Satrapa, 2008, s. 65 – 66; RFC 3306, s. 3).

Podoba skupinové adresy, založené na adrese individuální, je na obrázku 10. Samotná adresa skupiny začíná rezervovaným bajtem se samými nulami. Následuje délka použitého prefixu, která je nejčastěji 48 nebo 64. V dalších bitech je uložen prefix odpovídající části sítě, z nichž skupinová adresa pochází. Jejich délka je rovna informaci o délce prefixu v předchozí položce, nejvýše však 64 bitů. Poslední, minimálně 32bitová část, část obsahuje identifikátor skupiny (Satrapa, 2008, s. 65).

Obrázek 10: Skupinová adresa založená na individuální (Upraveno dle: Satrapa, 2008, s. 67)

Na obrázku 10 dále vidíme, že je-li příznak P nastaven na hodnotu P = 1, pak musí mít příznak T automaticky také hodnotu T = 1 (RFC 3306, s. 3).

Příznak **R** na obrázku 9 značí tzv. randevouz point. Jeho účel přesně definuje RFC 3956[1]. Pro rozsah této práce ho budeme chápat jako informaci o tom, že adresa vede na takzvané shromaždiště, tedy místo, kde jsou informace o jednotlivých unikátních adresách, na které má být obsah doručen. Výhoda tohoto systému je, že kdokoliv si ze skupinové adresy odvodí adresu shromaždiště a ví, kde se do ní přihlásit (Satrapa, 2008, s. 63, 67-68).

Poslední částí na obrázku 9 zůstává čtyřbitová položka **dosah**, která vymezuje topologickou oblast sítě, ve které je adresa jednoznačná. Může nabývat celkem 16 hodnot, které jsou uvedeny v tabulce 10.

[1] Embedding the Randevouz Point (RP) Address in an IPv6 Multicast Address

Tabulka 10: Dosahy skupinových adres

dosah	význam	upřesnění
0	rezervováno	
1	lokální pro rozhraní	nepřekročí jediné rozhraní, používá se pro skupinové vysílání pro lokální smyčku (loopback)
2	lokální pro linku	dosah je omezen na jednu fyzickou síť (např. ethernet nebo sériovou linku se dvěma účastníky)
3	rezervováno	
4	lokální pro správu	nejmenší dosah, který musí být konfigurován správcem (nelze je automaticky odvodit z topologie), většinou se jedná o podsíť
5	lokální pro místo	část síťové topologie, která se nachází v jednom geografickém místě a patří jedné organizaci
6, 7	volné	
8	lokální pro organizaci	pokrývá několik míst stejné organizace, například několik poboček v různých městech
9 - D	volné	
E	globální	celosvětový dosah
F	rezervováno	

Upraveno dle: Satrapa, 2008, s. 64 a s. 75

V hierarchii, popsané v tabulce 10, nemusí vždy platit, že větší dosah pokrývá o hodně větší část sítě, než dosah menší. V mnoha případech se může jednat o totožné dosahy. Například linka bude v mnoha případech totožná se správní oblastí (Satrapa, 2008, s. 76).

3.3.7 Výběrové (anycast) adresy

Výběrové adresy uzlu jsou novým typem adresování v IPv6. Poskytují možnost zařadit pod jednu výběrovou adresu více uzlů, rozmístěných v různých oddělených oblastech. Pošle-li na tuto adresu klient dotaz, je tento automaticky směřován na jeden z dostupných uzlů (zpravidla ten nejbližší). Tímto způsobem lze řešit například zdvojování počítačů nebo vyhledání nejbližšího zdroje, nabízejícího určitou službu (Satrapa, 2008, s. 69; RFC 4786, s. 4).

Používání výběrových adres přináší spoustu výhod. S jejich použitím lze dosáhnout rychlejší odezvy a automatického rozkládání zátěže. Dotazy z určité části sítě bude vyřizovat „lokální“ server. Výhodou je také zmenšení počtu adres, na kterých je služba poskytována (každý uzel nemusí být dostupný pouze pod svou vlastní adresou). Typickým příkladem mohou být firemní nameservery.

V neposlední řadě nabízí implementace výběrové adresy také obranu proti DoS a zvýšení obrany proti DDoS útokům – útočníci se dostanou pouze služby ve svých příslušných oblastech. Navíc lze velmi jednoduše identifikovat oblast, ze které útok přichází. (Satrapa, 2008, s. 70; RFC 4786, s. 5 - 6).

Výběrové adresy nemají rezervovanou žádnou svou část adresního prostoru, ale jsou úplně stejné jako adresy individuální. Je tak nemožné je od sebe odlišit pouze na základě podoby adresy. Přidělení výběrové adresy pro určité rozhraní je pak otázkou příslušné konfigurace samotného rozhraní a směrovačů.

Další vlastností výběrových adres je to, že rozhraní, spojená s těmito adresami, se mohou v průběhu času měnit. Počítač, který se chce zapojit do výběrové skupiny, ohlásí tuto skutečnost nejbližšímu směrovači, který zajistí její distribuci ostatním. Výhoda je automatizace, nevýhoda tohoto procesu je, že pokud použijeme výběrové adresy na síti s nízkým prefixem (např. páteřní síti), může dojít k přehlcení směrovacích tabulek anebo nemusí požadavek vyhovět pravidlům pro zařazení do těchto tabulek (Satrapa, 2008, s. 70 - 72). Jako optimální se naopak používání výběrových adres jeví u relativně malých sítí, například podnikových nebo těch, které jsou v rámci jedné firmy roztroušeny mezi několika místy.

Rizikem, spojeným s použitím výběrových adres je také nebezpečí změny v průběhu přenosu. Posílá-li jeden uzel druhému více dat, hrozí nebezpečí, že v čase přenosu dojde ke změně směrovacích tabulek. Jednu část zprávy obdrží první adresát a druhou nějaký jiný. Typickým příkladem může být přenos souborů. Řešení spočívá v rozložení přenosu do dvou fází. V první, inicializační, fázi proběhne spojení klienta na server přes výběrovou adresu. Server sdělí klientovi svoji unikátní adresu a druhá, stěžejní, část komunikace již probíhá přes ni (RFC 4786, s. 6 – 7).

Nebezpečím změny v průběhu přenosu naopak netrpí například služba DNS přes UDP, která využívá k žádosti a odpovědi vždy po jednom paketu. Pro takové služby je použití výběrových adres velmi vhodné (RFC 4786, s. 7).

3.3.8 Povinné adresy uzlu

V kapitole 3.3.3 jsem nastínil, že jeden uzel musí reagovat na více adres. Podle RFC 4291 (s. 17) to jsou pro koncový uzel tyto adresy:

- lokální linková pro každé rozhraní (viz. kap. 3.3.5)
- všechny další individuální (unicast) a výběrové (anycast) adresy, které mu byly přidělené manuálně nebo automaticky
- lokální smyčka (loopback)
- skupinové (multicast) adresy všech uzlů definované v oddílu 2.7.1 RFC 4291[1]
- skupinová adresa pro vyzývaný uzel pro všechny přidělené individuální a výběrové adresy
- skupinové adresy, ve kterých je členem

Směrovač musí povinně rozpoznávat všechny adresy jako koncový uzel a navíc ještě následující adresy, které ho identifikují (RFC 4291, s. 17; Satrapa, 2008, s. 73-74):

- výběrová adresa pro směrovač v podsíti, pro všechna rozhraní, pro která vystupuje jakou směrovač
- všechny další výběrové adresy, pro které byl směrovač konfigurován
- všechny další skupinové adresy, definované v oddílu 2.7.1 RFC 4291

3.4 Některé vlastnosti IPv6

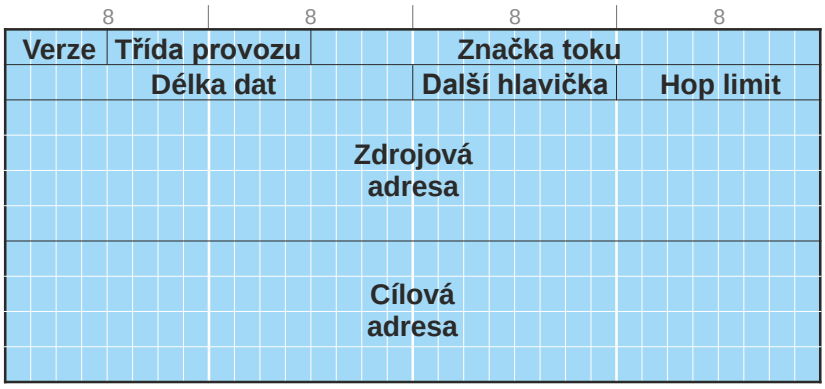
3.4.1 Formát paketu

Vlastnosti a formát paketu doznaly oproti dřívější verzi protokolu několika zásadních změn. Jsou na první pohled patrné z obrázku 11, kde je znázorněná hlavička paketu protokolu IPv6.

Nejviditelnější je redukce počtu položek, které se v hlavičce vyskytují. Zmizely nepovinné a rozšiřující volby. Hlavička má nově konstantní velikost a všechny dodatečné informace se vkládají do rozšiřujících hlaviček, které v paketu mohou, ale nemusí, být přítomny.

Díky tomu, že je dopředu jasně definovaná velikost hlavičky, není potřeba při každém průchodu na směrovači vypočítávat kontrolní součet (Satrapa, 2008, s. 33).

[1] A Node's Required Adresses



Obrázek 11: Základní hlavička paketu (Upraveno dle RFC 2460, 1998. s. 4; Satrapa, 2008, s. 33)

Verze je položka, zpravidla zahajující IP paket. Obsahuje verzi komunikačního protokolu, zde číslo 6 (Satrapa, 2008, s. 34).

Třída provozu slouží k zařazení paketu do určité třídy důležitosti. Na základě toho je pak s paketem zacházeno. Třída provozu momentálně není plně využívána, protože protokol IPv6 nedokáže garantovat kvalitu přenosu. Částečně se toto pole dá využít k prioritizaci provozu, kdy budou konkrétní pakety odbaveny přednostně. Ve specifikaci IPv6 není tato položka dále upřesněna. Základní hodnotou je nula (RFC 2460, s. 25-26; Satrapa, 2008, s. 34).

Značka toku označuje sekvenci paketů se stejnými vlastnostmi. Primárním cílem toku je identifikovat jednotlivé pakety patřící k sobě (do jednoho toku) a zajistit, aby s nimi bylo po cestě podobně nakládáno. Pokud je značka toku 0, pak paket není součástí žádného toku. Podpora toku ještě není dořešena a momentálně se nachází spíše v experimentální fázi (Satrapa, 2008, s. 48-49; RFC 3697, s. 2).

Délka dat nese informaci o velikosti paketu v bajtech. Nezapočítává se do něj velikost hlavičky. Vzhledem k tomu, že hodnota je dvoubajtová, může být základní velikost paketu bez hlavičky maximálně 2^{16} bajtů. IPv6 protokol ale nabízí možnosti, jak toto obejít (Satrapa, 2008, s. 34).

Další hlavička umožňuje standardní hlavičku rozšířit o libovolný počet doplňkových hlaviček. Pokud se hned za hlavičkou nacházejí vlastní data, označuje pole další hlavička typ těchto dat (Satrapa, 2008, s. 36). Například protokol TCP bude mít v poli

Další hlavička hodnotu 6. ICMP zpráva, které se věnuji v kapitole 3.4.2, nese hodnotu 58[1] (IANA, 2011).

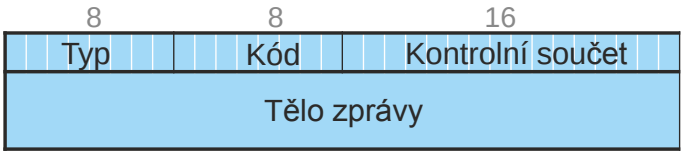
Hop limit nahrazuje dřívější definici životnosti paketu pomocí TTL[2]. Odesilatel nastaví takovou hodnotu, která určuje maximální počet „skoků“ paketu mezi síťovými uzly. Při průchodu každým uzlem se toto číslo sníží o jedničku a pokud paket nedorazí do cíle dříve, než bude jeho hop limit roven nule, zahodí se a odesílateli se pošle ICMP zpráva. Toto opatření má za cíl zabránit zacyklení nedoručitelných paketů v síti (Satrapa, 2008, s. 34).

Zdrojová a **cílová adresa** zabírají kvůli své velikosti největší část hlavičky paketu. O datové velikosti adres píši podrobněji v kapitole 3.3.1.

3.4.2 ICMP

ICMP je servisní protokol, sloužící uzlům k hlášení chyb, ke kterým došlo při zpracovávání paketů. Slouží také pro výměnu informací a diagnostiku sítě, jako je například příkaz PING. Protože je ICMPv6 zároveň nedílnou součástí protokolu IPv6, každé zařízení, které tímto protokolem komunikuje, musí mít ICMPv6 automaticky implementováno (RFC 4443, s. 3).

Pokud se podíváme na standardní IPv6 paket, odhalíme ICMP zprávu podle toho, že pole Další hlavička nese hodnotu 58 (RFC 4443, s. 2). Standardní formát ICMPv6 zprávy zobrazuje obrázek 12.



Obrázek 12: Základní formát ICMPv6 zprávy (Upraveno dle RFC 4443, s. 3)

Položka **typ** určuje druh zprávy a na její hodnotě záleží další obsah zprávy. Kromě standardních typů zprávy rozlišuje protokol ještě podtyp, jehož číslo nese pole **kód**.

[1] všechny aktuální hodnoty pro rozšiřující hlavičky a typy nesených dat jsou k dispozici online na http://www.iana.com/assignments/protocol-numbers/protocol-numbers.xml

[2] anglická zkratka Time to Live

Kontrolní součet se používá, jako již standardně, pro kontrolu, zda nebyl paket po cestě poškozen.

Standardní zprávy protokolu ICMPv6 jsou rozděleny do dvou skupin, jež od sebe dělí hodnota prvního bitu v poli typ. Je-li tato hodnota 0 (typ zprávy v rozmezí 0-127), jedná se o zprávu chybovou. V opačném případě (128-255) je zpráva informační (RFC 4443, s. 3).

Seznam typů a kódů zpráv je podrobně rozebraný v RFC 4443.

3.4.3 Objevování sousedů

Funkce objevování sousedů (Neighbour Dicsovery) je obdobou klasického ARP protokolu v IPv4. Využívá se pro hledání linkové adresy na základě znalosti adresy síťové, kdy uzel, který chce navázat komunikaci, hledá cílový uzel na stejné lince (tzv. vyzývaný uzel) (Satrapa, 2008, s. 98-99).

Formát adresy vyzývaného uzlu vychází ze skupinové adresy. Pohybuje se v oblasti adres od:

ff02::1:ff00:0 do ff02::1:ffff:ffff,

přičemž posledních 24 bitů se používá k identifikaci vyzývaného uzlu a vychází z posledních 24 bitů jeho síťové individuální nebo výběrové adresy (RFC 4291, s. 16). Takové adrese můžeme také říkat adresa pro vyzývaný uzel.

Odpověď cílového uzlu je realizována prostřednictvím paketu s ohlášením souseda. Ten obsahuje především informace o cílové IP adrese vyhledávaného uzlu, jeho linkové adrese a také příznak, zda je hledaný uzel směrovačem nebo ne (Satrapa, 2008, s. 99-100).

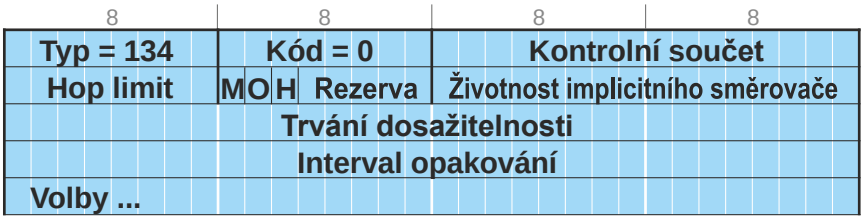
Hledání cílového uzlu neprobíhá před každým spojením, ale každý uzel má zapsanou tabulku s linkovými adresami svých sousedů, tzv. cache sousedů. Neznamená to ale, že by neprobíhalo ověřování těchto informací. Právě naopak, cache je stále ověřována ze dvou zdrojů. Prvním je informace z vyšších vrstev, že komunikace s cílem probíhá a ten je tudíž dosažitelný. Druhým je vyslání výzvy sousedovi, čímž se ověří jeho dostupnost. Jestliže soused neodpoví, je jeho linková adresa z cache vyřazena (Satrapa, 2008, s. 100-101).

3.4.4 Automatická konfigurace a DHCP

Jednou z velkých výhod IPv6 je implementace automatické konfigurace, přesněji bezstavové automatické konfigurace. Naopak stavová konfigurace je obdoba DHCP protokolu IPv4. Kvůli jednoznačnosti se v poslední době začíná stavová konfigurace označovat jako DHCPv6, podle protokolu, kterým je realizována (Satrapa, 2008, s. 111). Hlavním cílem automatické bezstavové konfigurace je schopnost uzlu, určit si vlastní adresu, bez potřeby jakéhokoliv nastavení uzlu, minimálního nebo žádného nastavení směrovače a bez potřeby serveru (RFC 4862, s. 3).

Chce-li jakýkoliv uzel komunikovat se svým okolím, vytvoří si nejprve svou lokální linkovou adresu pomocí identifikátoru EIU-64 nebo pseudonáhodného čísla (viz kapitolu 3.3.3), před který se vloží standardní prefix individuálních lokálních linkových adres fe80::/10. Pro ověření unikátnosti adresy v síti se následně využije objevování sousedů. Uzel vyšle dotaz na adresu, kterou sám sobě vygeneroval a pokud se vrátí ohlášení souseda, je třeba vygenerovat adresu novou (Satrapa, 2008, s. 114-115; RFC 4862, s. 12-13).

Po vytvoření individuální lokální linkové adresy čeká uzel na ohlášení směrovače, které s sebou nese všechny potřebné informace pro vytvoření adresy. Toto ohlášení je vysíláno v náhodných intervalech a jeho podoba je vidět na obrázku 13.



Obrázek 13: Ohlášení směrovače (Upraveno dle: Satrapa, 2008, s. 112)

V základním paketu pro ohlášení směrovače je nejdůležitější informací **životnost implicitního směrovače**, což je čas v sekundách, jak dlouho bude ještě tento směrovač sloužit jako implicitní pro uzly aktuální sítě. Údaj **hop limit** (počet skoků) oznamuje, jakou životnost mají uzly nastavovat pro své pakety. V obrázku 13 dále najdeme příznak **M**, informující, že se jedná o stavovou konfiguraci a všechny důležité informace poskytne DHCPv6. **O** rozhoduje o přidělení všech dalších informací, jako např. adresy lokálních DNS serverů, pomocí DHCPv6. **H** byl poměrně nedávno přidán a

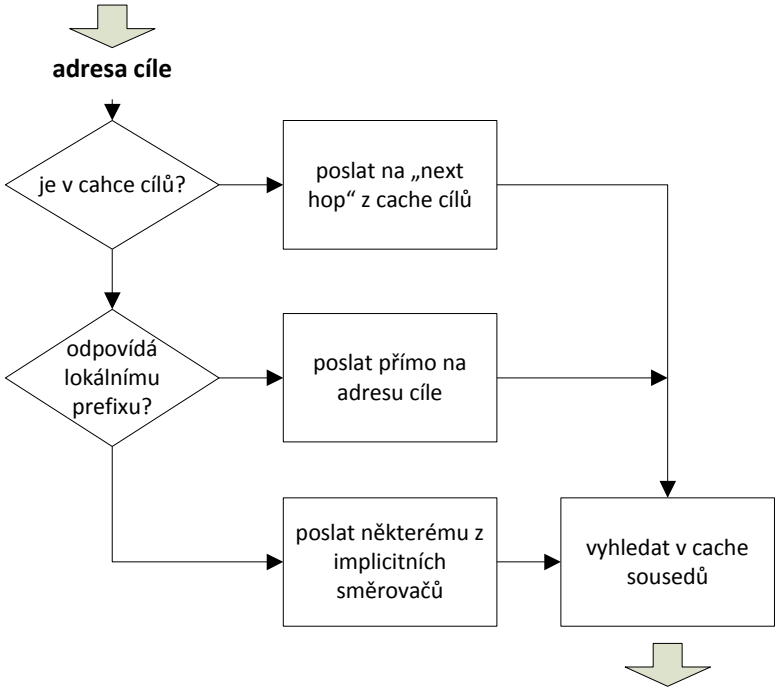
slouží pro podporu mobility. **Trvání dosažitelnosti** uvádí, po jak dlouhou dobu má být uzel požadován za dosažitelný od posledního ověření a **interval opakování** je interval mezi dvěma výzvami sousedovi. V poli **volby** může směrovač například připojit svoji linkovou adresu, MTU sítě a prefix IP adresy. (Satrapa, 2008, s. 112-113).

Uzel, který se chce připojit do sítě, zjistí z ohlášení směrovače prefixy adres a také, jestli má pro adresu použít bezstavovou konfiguraci. Pokud ano, připojí k ní svůj identifikátor (Satrapa, 2008, s. 114 – 115).

3.4.5 Směrování v IPv6

IPv6 přináší také novinku ve směrování – jednotlivé uzly se mohou naučit směrovat ve své síti. Předpokladem to tuto funkcionalitu je to, že si každý uzel bude udržovat čtyři typy informací. **Cache sousedů** obsahuje linkové adresy cílových uzlů, s nimiž nedávno probíhala komunikace, a také informace, zda se jedná o klasický uzel nebo směrovač. **Cache cílů** obsahuje obdobné informace, jako cache sousedů, ale ke každému cíli je zde uvedena adresa prvního uzlu, který je po cestě (next hop). **Seznam prefixů** slouží k rozhodnutí, zda se cíl nachází ve stejné síti nebo ne a **seznam implicitních směrovačů**, obsahující seznam všech směrovačů na síti, které se v ohlášení směrovače přihlásili jako implicitní (viz obrázek 13) (RFC 4861, s. 33 – 34; Satrapa, 2008, s. 115 – 116).

Uvedené datové struktury jsou ideální a nemusí být vždy implementovány právě v této podobě. Lze je nahradit například směrovací tabulkou (Satrapa, 2008, s. 116). Vlastní algoritmus hledání popisuje obrázek 14, ve kterém je pro přehlednost vynechána fáze vyhledávání mobilního uzlu na začátku algoritmu. Před vlastním směrováním dochází ještě ke kontrole, zda je uzel opravdu připojen do lokální sítě a nepřistupuje do ní mobilně.



Obrázek 14: Postup při odesílání paketu (Upraveno dle: Satrapa, 2008, s. 117)

3.4.6 DNS a IPv6

DNS je velmi důležitá součást IPv6. Jeho funkcí je, stejně jako u DNS na IPv4, překlad doménových jmen na standardní IPv6 adresu. Podíváme-li se na tvar takové adresy, můžeme konstatovat, že DNS je, na rozdíl od IPv4, téměř nepostradatelný.

Na základních funkcích DNS serveru se prakticky nic nemění a tak, jak ho definuje RFC 3596 (s. 1), se jedná prakticky o úpravu stávajících služeb. Jeho úloha je ale nyní ztížena o to, že poskytuje potřebné informace (IP adresy nebo doménová jména) současně pro protokoly IPv4 a IPv6.

K existujícím záznamům A, MX, NS nebo SRV se přidává nový záznam AAAA, který uchovává právě informaci o IPv6 adrese uzlu. Modifikací stávajícího typu záznamu lze velmi jednoduše docílit, že DNS server může pracovat jak na IPV6, tak na IPv4 protokolu současně a dokonce například poskytovat IPv6 záznamy přes IPv4 protokol či naopak (RFC 3596, s. 2-4).

Výhoda současné podoby záznamu je ta, že A i AAAA záznam mohou existovat vedle sebe. Záznam pro uzel *pc1.unas.cz* může vypadat například následovně:

pc1	*A*	*10.0.0.3*
	AAAA	*2001:db8:89ab::93e5:5d6f*

Uzel, který bude chtít komunikovat se svým partnerem, obdrží od DNS serveru oba dva záznamy a podle typu svého připojení se pak rozhodne, jakým protokolem bude komunikovat (Satrapa, 2008, s. 183-184).

Součástí DNS systému jsou také zpětné dotazy, pomocí nichž lze ze záznamu získat jméno uzlu na základě znalosti jeho IP adresy. K tomu se využívá tzv. PTR záznam, vedený jako doménové jméno vytvořené z převrácené IPv6 adresy, jejíž čtyřbitové položky jsou od sebe odděleny tečkou. Za toto doménové jméno se přidává sufix .IPV6.ARPA (RFC 3596, s. 3; Satrapa, 2008, s. 182).

Budeme-li chtít zobrazit reverzní záznam uzlu *pc2* s adresou 4321:0:1:2:3:4:567:89ab, bude informace DNS serveru obsahovat záznam:

b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA PTR pc2

Nevýhodou DNS záznamů v kombinaci s IPv6 adresami je možnost (nebo dokonce nutnost) uzlu mít více adres, jelikož soubor, obsahující záznamy, rychle nabývá na velikosti. Zároveň ale nemá cenu vkládat do DNS všechny adresy každého uzlu. Vynechat můžeme například lokální linkové adresy nebo pseudonáhodně generované krátkodobé adresy na základě RFC 4941 (viz kapitolu 3.3.4). Naopak vhodnými kandidáty pro zařazení do DNS jsou všechny dlouhodobé globální individuální adresy nebo dlouhodobě platné adresy přechodových mechanismů (Satrapa, 2008, s. 183.

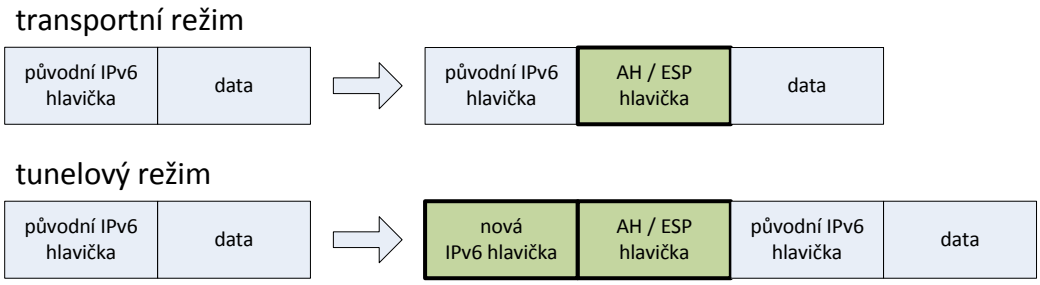
3.4.7 Zabezpečená komunikace protokolu IP - IPsec

IPsec nabízí svým uživatelům možnost autentizace a šifrování dat. Občas se můžeme setkat s tvrzením, že IPv6 na rozdíl od IPv4 přináší bezpečnou komunikaci, tedy IPsec. Tato není tak úplně pravdivá. Jediný rozdíl IPv6 oproti verzi 4 je ten, že nový protokol musí integrovat IPsec povinně. Nic ale nebrání tomu, provozovat jej na IPv4 a na druhou stranu se v současné době nelze spolehnout na to, že IPsec bude v rámci zařízení, podporujících IPv6, plně implementován (Satrapa, 2008, s. 189).

Bezpečnost protokolu IP je v praxi realizována systémem dvou bezpečnostních rozšiřujících hlaviček, označovaných AH (Autenthication header) a ESP (Encapsulating

Security Payload)[1]. Hlavička ESP přitom nabízí obdobné služby jako AH plus rozšiřující výhody. Proto je také její implementace podle RFC 4301 povinná, zatímco u AH je dobrovolná (Satrapa, 2008, s. 189). V následujícím textu se budu spíše zabývat principy, aplikovanými na ESP hlavičku.

Bezpečnostní hlavičky IPsec je možné doplňovat do paketu dvěma možnostmi. V transportním (tedy standardním) režimu se vkládají do paketu jako součást rozšiřujících hlaviček. Naopak v případě tunelového spojení IPsec část „obalí“ celý paket a tomu je následně vygenerována nová IPv6 hlavička. Rozdíl je vidět na obrázku 15.



Obrázek 15: Vložení hlaviček IPsec do paketu (Upraveno dle: Satrapa: 2008, s. 190)

Paketyy nemusí být pomocí IPsec chráněny po celou cestu sítí. Máme-li například společnost se dvěma pobočkami, nebudeme chtít šifrovat a autentizovat obsah v rámci vlastní sítě na jednotlivých pobočkách, ale až v momentě, kdy paket opustí „hranice pobočky“ a poputuje na pobočku jinou. Na „hranicích“ je směrovač, který působí jako tzv. bezpečnostní brána a paket zašifruje. Na hranici sítě cílové pobočky je opět bezpečnostní brána, která se naopak stará o rozšifrování a autentizaci odesilatele. Je-li vše v pořádku, paket je postoupen dál. V opačném případě dojde k jeho zahození a v určitých případech je odesílateli poslána ICMP zpráva.

Důležitou rolí IPsec jsou bezpečnostní asociace – spojení dvou uzlů, které zajišťuje bezpečný přenos dat. Pro každý směr se přitom vytváří vlastní přenos. Na každé straně pak bezpečnostní spravuje systém, nazvaný databáze bezpečnostní politiky (SPD – Security Politics Database). Databáze je sada pravidel, na základě nichž dochází

[1] problematice AH hlaviček se věnuje RFC 4302 IP Authentication Header, zatímco ESP hlavičky podrobně rozebírá RFC 4303 IP Encapsulating Security Payload (ESP)

k rozhodnutí, jak se uzel zachová k přicházejícím nebo odcházejícím paketům. Pravidlo se dále může odkazovat na příslušnou bezpečnostní asociaci, uloženou v databázi bezpečnostních asociací (SAD).

Každé pravidlo může mít jednu z následujících podob:

- pakety, směřující na adresu XY zahodit
- pakety, směřující do jiné pobočky společnosti, podrobit pravidlům IPsec. Pravidlo odkazuje na odpovídající uloženou bezpečnostní asociaci.
- paket je dále propuštěn bez použití IPsec a bez omezení

V praxi se tyto kombinace pravidel vrství za sebe podle priority (Satrapa, 2008, s. 191 – 192).

Použití hlavičky ESP (Encapsulating Seciruty Playload) v paketu umožňuje data jak šifrovat, tak pomocí ní autentizovat odesílatele. Na rozdíl od ostatních hlaviček se ESP liší tím, že pojme celý původní paket do sebe. Celý vnitřní obsah paketu je zašifrován a vložen jako nesená data. Hlavička nově zašifrovaného paketu nese kromě standardních informací také index bezpečnostních parametrů a pořadové číslo. V indexu jsou definovány informace o klíči a algoritmu, který se použije pro zašifrování / rozšifrování dat. Pořadové číslo slouží k ochraně proti opakování.

Průběh odeslání a příjmu paketu je pak následující: Odesílatel vloží ESP hlavičku a podle parametrů, daných bezpečnostní asociací, jej zašifruje. Vygeneruje pořadové číslo (zvětšuje se vždy o 1). Pokud je požadována autentizace odesilatele, vygeneruje kontrolní hodnotu a uloží ji do ESP.

Příjemce si vyhledá příslušnou bezpečnostní asociaci. Když tato neexistuje, paket je zahozen. Dále zkontroluje pořadové číslo (pokud bylo již použito, paket je zahozen). Následuje autentizace na základě autentizačních dat v ESP. Pokud paket prošel celým sítem a byl autentizován, proběhne dešifrování a odstraní se ESP hlavička. Výsledek je dále předán pro standardní zpracování, například odeslán dále (Satrapa, 2008, s. 192-199).

3.5 Přechodové mechanismy mezi IPv6 a IPv4

Jak již bylo naznačeno v předchozím textu, málo kdy se v dnešní době setkáme se sítí, která by byla provozována pouze na IPv6. Pokud ano, jedná se spíše o experimentální záležitost, než o „ostrý“ provoz. Proto je nutné věnovat dostatečnou pozornost přechodovým mechanismům, umožňujícím souběžný provoz sítí IPv6 a IPv4.

V současné době se můžeme setkat se dvěma základními řešeními. První možností přenosu je standardní tunelování. S jeho principem můžeme přenášet jakákoliv „zabalená“ data prostřednictvím jiného protokolu. Další variantou jsou pak zařízení, fungující jako překladače.

3.5.1 Dual stack

Dvojí zásobník (dual stack) je metoda, která umožňuje, aby uzel komunikoval paralelně jak prostřednictvím protokolu IPv4, tak IPv6. Jako konkrétnější překlad do češtiny můžeme použít výraz dvojitá IP vrstva.

K fungování dvojího zásobníku musí uzel nejen podporovat oba protokoly, ale také mít oba typy adres. Samozřejmostí je také požadavek na uzel, umět vyhledávat v DNS záznamech typu A a AAAA. V případě, že je cílový uzel dostupný na obou dvou sítích, pořadí DNS záznamů rozhoduje o tom, jestli bude komunikace zahájena přes IPv6 nebo IPv4 (Štorková, 2012).

Spolupráce a předávání dat mezi oběma protokoly pak funguje převážně na čtvrté, aplikační, vrstvě protokolu TCP/IP. Příslušná aplikace upraví data, která dorazila jedním protokolem, a pošle je jiným protokolem zamýšlenému příjemci (Satrapa, 2008, s. 236).

3.5.2 6to4

6to4 je základní jednoduchý tunelovací mechanismus, který více popisuje RFC 3056. Umožňuje koncovým sítím, fungujícím na IPv6, komunikovat mezi sebou prostřednictvím IPv4 protokolu. Pro tuto komunikaci není třeba zakládat explicitně tunelové spojení. Protokol si jej vytvoří sám automaticky (RFC 3056, s. 1).

Prefix IPv6 adresy pro 6to4 se skládá z počáteční dvoubajtové hodnoty *2002*, následované IPv4 adresou cílového 6to4 směrovače – příjemce, zabírající další 4 bajty. Pokračující 2bajtová položka je rezervována pro podsíť a konečně, posledních 8 bajtů je standardně rezervováno pro identifikátor rozhraní (Satrapa, 2008, s. 241).

Obrázek 16: struktura 6to4 adresy (Upraveno dle: Satrapa, 2008, s. 241)

Spojení 6to4 je realizováno pomocí 6to4 směrovače, který je umístěn na rozhraní IPv6 (vnitřní) a IPv4 (vnější) sítě. Je třeba, aby každý směrovač měl jednu unikátní globální IPv4 adresu, která bude následně součástí IPv6 adresy sítě, ležící za směrovačem. Přijde-li ke směrovači odesilateli požadavek k odeslání dat, zabalí je tento do standardního IPv4 paketu a odešle na IPv4 adresu příjemce[1]. Zde následuje rozbalení a přeposlání IPv6 paketu dále cílovému uzlu. Spojení v tomto případě není navazováno trvale, ale pouze v případě potřeby – každý paket je IPv4 hlavičkou obalen samostatně. Nezanedbatelnou výhodou 6to4 je tedy jeho nenáročnost jak na výkon, tak na nastavení. Kromě potřeby zavézt 6to4 adresy do DNS není třeba provádět žádné specifická nastavení nebo konfigurace (Satrapa, 2008, s. 241).

Existuje nebezpečí, že přenosová trasa na IPv4 nebude mít dostatečnou MTU (přenosovou kapacitu). V tomto případě je paket standardně fragmentován (RFC 3056, s. 7).

3.5.3 ISATAP

ISATAP[2] zajišťuje spojení jednoho počítače, využívajícího IPv6 s okolím v rámci IPv4 sítě. Stává se tak doplňkem mechanismu 6to4 a velmi často se setkáme právě s variantou, kdy spolu oba dva mechanismy fungují společně.

ISATAP zavádí novou podobu adresy rozhraní. Počáteční 4 bajty obsahují konstantu *0000:5efe*, která je doplněna dalšími 4 bajty s IPv4 adresou uzlu v hexadecimálním tvaru. V případě, že je identifikátor rozhraní odvozen od globální adresy, mají jeho 4

[1] zjištěnou z prefixu 6to4 adresy

[2] zkratka Intra-Site Automatic Tunnel Adressing Protocol

počáteční bajty hodnotu *200:5efe*. Identifikátor rozhraní je následně připojen k potřebnému (linkovému, 6to4, atd.) IPv6 prefixu, získaného manuálně nebo automatickou konfigurací. Výsledná adresa, obsahující kombinaci IPv4 a IPv6 může mít například tvar

2002:93e6:1707:1:0:5efe:10.1.2.3 (Satrapa, 2008, s. 244 – 245).

To, že je ISATAP postaven na IPv4 s sebou nese některá omezení. Problémem může být skupinové doručování, jelikož IPv6 nepodporuje multicastové adresy. Stejně tak není jak posílat výzvy a ohlášení směrovače. ISATAP proto zavádí tzv. seznam potencionálních směrovačů (PRL), který v sobě obsahuje seznam všech směrovačů, podporujících ISATAP a jejich IPv4 adresy. Uzel posílá výzvy směrovači už jen na adresy, uvedené v PRL. Ohlášení směrovače jsou posíláná individuálně na jednotlivé adresy uzlů.

Naplnění PRL se děje většinou za přispění DNS na IPv4. DNS záznamy pro ISATAP směrovače mají v tabulce A záznam pod názvem *isatap* (Satrapa, 2008, s. 246 – 248).

6to4 a ISATAP jsou velmi dobře použitelné v ideálních IPv4 sítích, ale v praxi naráží na jeden veliký problém. Tím je používání NATu. Oba dva koncepty totiž předpokládají, že každý vstupní bod sítě má svou unikátní globální IPv4 adresu, což dnes velmi často není pravda.

3.5.4 Teredo

Řešení, jak projít skrze NAT nabízí Teredo. Základní myšlenkou je, že NAT nepropustí zvenku komunikaci, která předtím nebyla zahájena uzlem zevnitř. Takový uzel je pak zvnějšku sítě nedosažitelný. V praxi pak rozlišujeme NAT trychtýřový, který přidělí klientovi určitou adresu a port a propustí k němu libovolný paket, NAT restriktivní, který taktéž přiřadí klientovi adresu a port, ale předá mu pouze pakety z adresy, na kterou dříve něco poslal a nakonec NAT symetrický, který klientovi přiděluje pro komunikaci s různými cíli různé adresy a porty. S posledně jmenovaným typem si Teredo poradit neumí. K přenosu dat je používán protokol UDP (Satrapa, 2008, s. 246 – 247).

Počítač, ležící za NATem, který chce zahájit komunikaci, označujeme pojmem klient. Jako první odešle klient výzvu směrovači na adresu Teredo[1] serveru, kterou zabalí do UDP datagramu. Server po obdržení výzvy odešle ohlášení směrovače. Součástí této tzv. kvalifikační procedury je také ověření, jestli klient leží za trychtýřovým, restriktivním nebo symetrickým NATem (Satrapa, 2008, s. 248).

Formát adres je poměrně složitý. Prvních 32 bitů tvoří prefix Teredo služeb, následovaný IPv4 adresou Teredo serveru. Prefix je v tomto případě neměnný a má hodnotu 2001:000/32. Dále je vloženo 16 bitů příznaků, které mimo jiné určují, jestli je NAT, za kterým leží klient-odesílatel, trychtýřový, nebo jiný. Pokračuje 16 bitů s číslem UDP portu a posledních 32 bitů s adresou NATu, za kterým klient leží. Posledních 48 bitů je invertovaných (Satrapa, 2008, s. 247; RFC 4380, s. 11 - 12).

Chtějí-li spolu komunikovat dva Teredo klienti, pak je situace poměrně jednoduchá a mohou komunikovat přímo. Před zahájením je ale třeba, aby se spojili s Teredo serverem a navzájem si „otevřely“ NATy.

První klient vyšle tzv. bublinu – paket na adresu NATu klienta 2. Zde je paket zahozen, protože ještě není vytvořeno propojení. NAT klienta 1 odteď propouští pakety od klienta 2. Druhá bublina je vypuštěna přes Teredo server, který ji přesměruje na adresu klienta 2. Tentokrát bublina NATem projde a klient 2 odpoví na adresu klienta 1. Tím otevře také NAT na své straně a nyní již mohou klienti komunikovat bez podpory serveru.

V případě, že klient chce navázat spojení s uzlem, ležícím v IPv6 síti a bez Teredo adresy, je třeba využít vhodný směrovač (tzv. relay), který tuto funkci nabízí. Vhodný směrovač pro klienta najde Teredo server a následně probíhá komunikace mezi směrovačem a klientem podle dříve popsaného vzorce (Satrapa, 2008, s. 248 – 250).

Řešení Teredo je do reálného provozu poněkud zdlouhavé. Na druhou stranu se s ním nepočítá jako s dlouhodobým řešením, ale slouží k překlenutí období, kdy budou vedle sebe ve velké míře koexistovat IPv4 a IPv6 sítě.

[1] adresu Teredo serveru musí klient znát dopředu. Na systémech Windows se například přednastavená adresa serveru *teredo.ipv6.microsoft.com*.

3.5.5 SIIT

Předchozí řešení se zabývala především způsobem, jakým způsobem navázat komunikaci dvou uzlů nebo sítí přes prostředí, které daný protokol komunikace nepodporuje. Ne vždy je ale situace taková, že spolu potřebují komunikovat pouze uzly, ovládající stejný protokol. Situaci do určité míry řeší metoda dvojího zásobníku, ale pokud ji uzel nemá implementovanou, se stávajícími možnostmi není možné, aby byla navázána komunikace mezi zařízeními na IPv4 a IPv6. Tuto, v praxi velmi rozšířenou, variantu řeší právě Stateless IP/ICMP Translation, zkráceně SIIT.

Komunikace mezi oběma protokoly je řešená dočasně přidělenými adresami. Jedná se o adresy ipv4-mapované (viz kapitolu 2.3.3) a o adresy IPv4-překládané.

Mapované adresy slouží k označení uzlů, které nepodporují IPv6. Takové zařízení se pak na SIIT směrovači (nebo jiném zařízení, podporujícím SIIT) v IPv6 síti tváří, jako by mělo adresu ve tvaru ::ffff:a.b.c.d, kde a.b.c.d je jeho původní IPv4 adresa.

Překládané adresy jsou přidělovány IPv6 uzlům ve tvaru ::ffff:0:a.b.c.d a slouží pro jejich identifikaci v IPv4 světě. a.b.c.d je dočasná IPv4 adresa IPv6 uzlu (Satrapa, 2008, s. 251).

Vlastní překlad je poměrně jednoduchý. Pokud na SIIT směrovač dojde paket z IPv6 sítě na nějakou IPv4-mapovanou adresu, SIIT paket přeloží a pošle do IPv4 sítě. Naopak funguje mechanismus obdobně.

Podíváme-li se na princip SIIT, zjistíme, že není možné využívat nadstandardních možností ani jednoho protokolu. SIIT se stará pouze o překlad základních informací a rozšiřující hlavičky IPv6 nebo volby IPv4 zahazuje (Satrapa, 2008, s 251 - 252).

3.5.6 NAT-PT a NAT64

NAT-PT využívá základy standardního NATu, známého z IPv6 sítí, ke kterému přidává SIIT a pár doplňujících nástrojů, umožňující přechod mezi IPv6 a IPv4. V současné době je tento způsob prohlášený na odmítnutý podle RFC 4966, ale jelikož zatím kromě jeho nástupce NAT64 není obdobná náhrada, stále se používá, například také ve směrovačích Cisco (Satrapa, 2008, s. 252; Cisco Systems, 2012b).

Podmínkou fungování NAT-PT je to, že všechny pakety jednoho spojení budou procházet přes jeden NAT-PT směrovač. Ten má k dispozici rozsah IVp4 adres, které může použít pro jednotlivé uzly ze své IPv6 sítě a také *libovolný* IPv6 prefix, který bude přidělovat adresám z IPv4 sítě. Další podmínkou je, že se mapovaná adresa nesmí uprostřed komunikace měnit.

Vlastní překlad pak probíhá podle následujících pravidel: Pokud paket zahajuje spojení, jeho odesílatel dostane přidělenou IPv4 adresu. Informaci o přidělené adrese si směrovač uloží a použije ji pro další pakety. Dále je ipv6 paket prostřednictvím SIIT převeden na IPv4 a dostane cílovou IPv4 adresu, získanou z posledních 4 bajtů původní cílové adresy IPv6.

V opačném směru probíhá překlad analogicky. IPv4 paket je prostřednictvím SIIT převeden na IPv6 a cíl je nastaven podle předem uložených informací o směrování.

Nepříjemnou vlastností NATu je, že umožňuje navazovat spojení pouze v jednom směru. Má-li být možné spojení iniciovat obousměrně, je potřeba upravit informace v DNS. DNS server pak musí ležet uvnitř NATované IPv6 sítě proto, aby všechny jeho odpovědi procházely přes stejný NAT-PT (Satrapa, 2008, s. 253 - 255).

Jak bylo již uvedeno na začátku této kapitoly, NAT-PT byl prohlášený za odmítnutý a jeho místo nahradil NAT64, který se dělí na bezstavový (RFC 6145) a stavový (RFC 6146). V dalším textu se budu zabývat především stavovým NAT64, jelikož podle Cisco Systems (2012b, s. 5) dokáže překládat více druhů spojení a Cisco jej tím pádem ve svých zařízeních preferuje.

Zásadní rozdíl mezi NAT-PT a NAT64 je ve skutečnosti, že umožňuje navázat spojení pouze z IPv6 do IPv4, nikoliv naopak. Každý NAT64 překladač v síti má svůj 96-bitový prefix, který používá pro mapování IPv4 adres.

Službu DNS pro NAT64 zajišťuje standard, označovaný jako DNS64. Princip fungování je takový, že požaduje-li klient z vnitřní IPv6 sítě adresu cíle, DNS64 dotaz předá nejdříve ve formě AAAA záznamu. Pokud nedostane odpověď, pošle dotaz na A záznam pro stejné jméno. Příchozí odpověď pak upraví na AAAA záznam a připojí k adrese potřebný prefix (Satrapa, 2008, s. 156 – 157).

3.5.7 Dual stack lite

Řešení dual stack lite uvádím až nakonec všech přechodových mechanismů. Na rozdíl od předchozích mechanismů umožňuje DS lite tunelovat IPv4 protokol přes nativní IPv6 síť. Můžeme jej tedy chápat jako „zadní vrátka“, jejichž primárním účelem je poskytnout IPS možnost tunelovat zákaznické IPv4 sítě skrz jejich IPv6 infrastrukturu (Štorková, 2012).

Tunelovaný provoz ze všech koncových zařízení, označených jako CPE (Consumer Premises Equipment), je sveden do centrálního prvku AFTR (Adress Family Transition Router). Ten se nachází na rozhraní IPv4 internetu a IPv6 sítě ISP. AFTR obsahuje tabulku NAT, ve které ukládá informace o IPv6 adresách příchozích spojení.

V případě DS lite je potřeba aby u koncového uživatele fungoval povoz standardním způsobem. Proto se CPE kombinuje s IPv4 DHCP serverem, IPv4 proxy a IPv6 DNS (Štorková, 2012).

4 Návrh řešení

V této kapitole uvedu návrhy řešení implementace protokolu IPv6 ve firemní síti podniku Teplárny Brno, a.s. na základě předchozí analýzy. Vzhledem ke komplexnosti návrhu a složitosti stávající sítě není možné plnohodnotný přechod realizovat okamžitě. Místo toho se nabízejí tři varianty:

a) varianta přechodu na IPv6 v co největší míře
b) varianta koexistence stávající sítě, založené na IPv4 s novou sítí, založenou na IPv6

4.1 Varianta maximálního přechodu na IPv6

Tato varianta počítá s maximálním nasazením protokolu IPv6. Všechny dostupné prvky sítě budou nahrazeny zařízeními, která nový protokol podporují a přechod na IPv4 bude prováděn ve velmi omezených případech, kdy současné řešení nenabízí jinou alternativu.

4.1.1 Páteřní síť, podsítě a uzly

Topologie páteřní sítě zůstává stále zachována. Stejně tak je vhodné zachovat logické rozdělení hlavních segmentů sítě na kancelářskou a technologickou část.

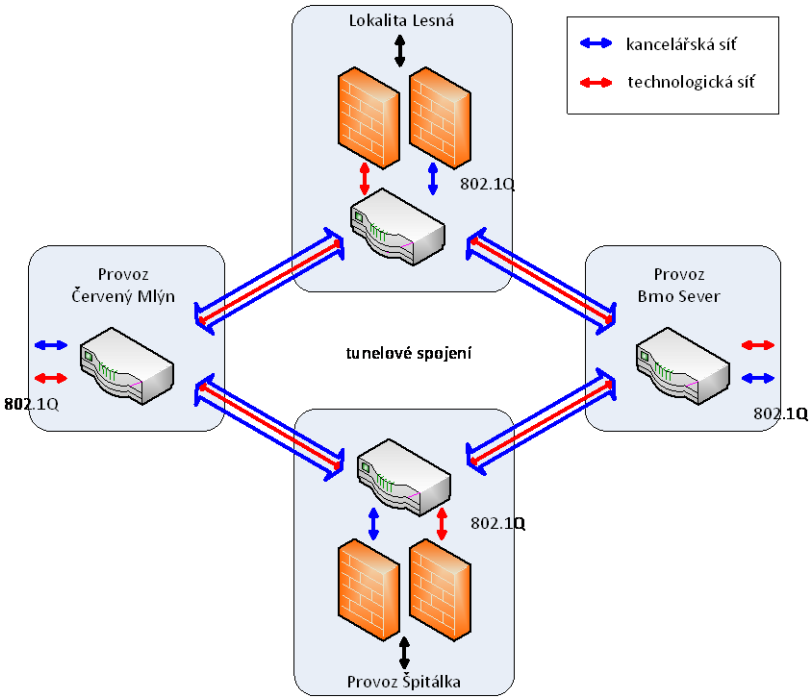
Kancelářská a technologická síť tedy budou provozovány jako dvě standardní separátní IPv6 VLAN, k čemuž v jednotlivých lokalitách poslouží IEEE 802.1Q. Konfigurace jednotlivých VLAN bude prováděna na úrovni portu Cisco přepínače.

Problém je tyto sítě oddělit v rámci 3. vrstvy za jednotlivými směrovači. V současné době Cisco nenabízí alternativu VRF-Lite pro IPv6 (Cisco Systems, 2012a). Možnost řešení nabízí technologie MPLS[1], která podporuje, obdobně jako VRF-Lite, oddělení jednotlivých sítí v infrastruktuře. Směrovače, integrující v sobě funkce MPLS se v současné době pohybují nad hladinou 350 tisíc Kč za kus[2] a jsou koncipovány spíše

[1] Multiprotocol Label Switching – technologie, umožňující od sebe oddělit virtuální sítě v rámci sítě nadřazené. Každý paket dostane jednoznačnou značku (Label) a pomocí ní je identifikován. Tím pádem nevadí, když se adresní prostory různých podsítí prolínají (Petřík, 2007).

[2] Platí pro řadu Cisco 7200 v roce 2012.

jako řešení pro ISP, než jako směrovače do páteřní sítě středního podniku. Budeme-li chtít zachovat stávající směrovače, je řešením provozovat na nich standardně kancelářskou IPv6 síť a síť technologickou mezi nimi tunelovat. Situace je zobrazena na obrázku 17.



Obrázek 17: Oddělení kancelářské a technologické sítě (Zdroj: vlastní)

Rozdělení sítě do dílčích podsítí bude respektovat předchozí stav, popsaný v kapitole 2.3.2. Infrastruktura kancelářské sítě zůstává beze změny. V technologické části sítě vyvstává nutnost změny hardware a změny IP adres. Proto bude možné sloučit staré a nové podsítě pro měřící prvky a převodníky. Výsledkem sloučení budou dvě základní podsítě technologického charakteru – jedna bude zahrnovat všechna technická zařízení, převodníky a technologická PC a druhá bude sloužit pro správu aktivních prvků. Další podsítě vycházejí z potřeb konkrétních lokalit.

Fyzické propojení mezi lokalitami, které zajišťují Teplárny Brno svépomocí, bude využívat protokolu IPv6. Stejně tak lokality, které jsou připojeny prostřednictvím sítě poskytovatele Faster CZ. V případě sítě Netbox, která aktuálně nepodporuje provoz IPv6, bude protokol tunelován podle standardu 6to4.

Každý uzel bude mít k dispozici několik IP adres, z nichž část bude závislá na jeho podsíti.

Globální individuální adresa se odvíjí od poskytovatele připojení. Budou-li Teplárny Brno využívat služeb Faster CZ, jejich prefix globální individuální adresy bude *2a02:0e98:xxxx::/48*. První část prefixu je přidělena operátorovi Faster CZ (Hurricane Electric, 2012) a další část, momentálně vyjádřená čtveřicí znaků X, bude záležet na ISP. Posledních 16 bitů z adresy zůstává podniku na definici podsítí podle vlastního uvážení.

Navrhuji oddělit od sebe technologickou a kancelářskou síť pomocí prvního bitu 7. bajtu prefixu. Hodnota 0 bude používání pro kancelářskou část sítě, hodnota 1 pro technologickou. Dále budou sítě rozděleny podle plánu v tabulkách 11 a 12.

Tabulka 11: Návrh prefixů pro kancelářskou síť

Lokalita	**Kancelářské**	**IPv6 prefix**
Správa společnosti	servery + PC + tiskárny	2a02:0e98:xxxx:1001::/64
	bezdrátová síť zaměstnanci	2a02:0e98:xxxx:2001::/64
	bezdrátová síť návštěvy	2a02:0e98:xxxx:3001::/64
Provoz Špitálka	servery + PC + tiskárny	2a02:0e98:xxxx:1002::/64
	bezdrátová síť zaměstnanci	2a02:0e98:xxxx:2002::/64
	bezdrátová síť návštěvy	2a02:0e98:xxxx:3002::/64
Provoz Brno-Sever	PC + tiskárny	2a02:0e98:xxxx:1003::/64
Provoz Červený Mlýn	PC + tiskárny	2a02:0e98:xxxx:1004::/64
	bezdrátová síť zaměstnanci	2a02:0e98:xxxx:2004::/64
	bezdrátová síť návštěvy	2a02:0e98:xxxx:3004::/64
Provoz Staré Brno	PC + tiskárny	2a02:0e98:xxxx:1005::/64

Zdroj: vlastní

Pro odlišení účelu sítě slouží první 4 bity, pro lokalitu pak následujících 12. Toto rozdělení adresního prostoru se na první pohled může zdát jako plýtvání, protože spousta bitů zůstává nevyužita, ale koncept počítá s tím, že každá lokality bude identifikována svým vlastním číslem podsítě. Vzhledem k tomu, že některé převodníky na technologické síti mohou být lokalizovány pouze na základě IP adresy, přináší tento systém také přehlednost. Podle prvního čísla lze rychle identifikovat typ sítě nebo zařízení a podle posledních tří pak lokalitu, ve které se nachází.

V síti Tepláren Brno jsou kromě lokalit, uvedených v tabulkách 11 a 12, také lokality, uvedené v příloze 1. U dalších lokalit bude číslování prefixu pokračovat podle navrženého schématu a každá z nich tak získá svou adresu pro snadnou identifikaci.

Tabulka 12: Návrh prefixů pro technologickou síť

Lokalita	Technologické	IPv6 prefix
Správa společnosti	směrovače + UPS + doch.	2a02:0e98:xxxx:9001::/64
	přepínače	2a02:0e98:xxxx:a001::/64
	bezpečnost	2a02:0e98:xxxx:c001::/64
Provoz Špitálka	stanice operátorů	2a02:0e98:xxxx:b002::/64
	kamery + měřící stanice + UPS + docházka	2a02:0e98:xxxx:9002::/64
	přepínače	2a02:0e98:xxxx:a002::/64
Provoz Brno-Sever	převodníky + měřící stanice + UPS + docházka	2a02:0e98:xxxx:9003::/64
	přepínače	2a02:0e98:xxxx:a003::/64
Provoz Červený Mlýn	převodníky + měřící stanice + UPS + docházka	2a02:0e98:xxxx:9004::/64
	přepínače	2a02:0e98:xxxx:a004::/64
Provoz Staré Brno	převodníky + docházka	2a02:0e98:xxxx:9005::/64
	přepínače	2a02:0e98:xxxx:a005::/64

Zdroj: vlastní

Závěrečných 64 bitů globálních individuálních adres uzlů bude tvořeno z EUI-64. Kromě globálních individuálních adres bude mít každý uzel samozřejmě přiřazeny ještě další adresy podle standardu IPv6, na kterých bude dosažitelný. Lokální linkovou adresu ve tvaru fe80::/10 (respektive fe80::/64), unikátní lokální adresu s prefixem fd00::/8, popřípadě skupinové adresy.

Problém s připojením protokolem IPv6 může nastat u zařízení, která jej neumí, ale zároveň v současné době neexistuje přijatelná náhrada. Typickým příkladem je dálková správa jednotlivých antén. V tomto případě navrhuji na nejbližším směrovači využít SIIT a s anténou navázat komunikaci přes IPv4.

Jedním z logických požadavků na přechod, aby vlastní přechodová fáze způsobila minimální omezení běžného provozu. Po dobu, než budou vyřešeny nedostatky nového protokolu tak doporučuji provozovat paralelně také síť IPv4 jako záložní variantu. Hlavní provoz bude směrován přes IPv6 a IPv4 bude vypnuto v momentě, kdy bude provoz přes IPv6 dostatečně odladěn.

4.1.2 Upgrade zařízení

Podstatnou částí přechodu je také upgrade stávajících nevyhovujících zařízení za nová. V oblasti SW doporučuji náhradu stávajících serverových řešení, založených na Windows Server 2003, upgradovat na verzi Windows Server 2008 R2 nebo na

Windows Server 8. Pokud neposkytuje server funkci, spojenou s Active Directory, DHCP nebo obdobným, není třeba jej měnit. Jedná se např. o servery, na kterých běží SAP nebo jeho testovací provoz. Konkrétně doporučuji vyměnit OS u serverů, na kterých je provozován Domain Controller, DNS, WINS, Exchange Server a RADIUS.

Pokud budou upgradovány servery s OS Windows 2003 na verzi 2008 R2, bylo by vhodné pořídit rovnou nový HW. Investice bude nutná minimálně u doménového kontroleru s Active Directory, u kterého je třeba data přehrát na nový stroj. Vedlejší výhodou masivního upgrade hardwaru a operačního systému je příležitost pro začátek virtualizace serverů (Morimoto, 2010).

Stávající stanice, běžící na Windows XP budou schopny na IPv6 pracovat v potřebném rozsahu.

V oblasti HW bude třeba nahradit nebo upravit ty prvky kancelářské sítě, které nemají povahu koncových PC stanic. Jedná se o nekompatibilní prvky, uvedené v tabulce 6 kapitoly 2.3.3.

Největší nekompatibilitu s IPv6 v kancelářské síti vykazují tiskárny. Zde se nabízí řešení použití jednoduchého tiskového serveru. Cenové rozpětí se pohybuje od 1500 Kč (Edimax PS320) až do 10 000 Kč (řada HP Jetdirect). U většiny použitých typů tiskáren se ovšem při využití zařízení z horní cenové hranice jednoznačně vyplatí nahradit danou tiskárnu novým typem.

Technologická síť na rozdíl od kancelářské využívá specializovaných zařízení, která na přechod nejsou připraveny vůbec. Setkáváme se tu se dvěma typy zařízení. První je komplexní řešení MetaSys firmy Johson Controls a druhý typ zastupují samostatné měřiče, které komunikují především na RS-232 a RS-485. Do podnikové sítě jsou připojeny přes převodníky, které komunikují pouze na IPv4.

Řešením pro zařízení na standardu RS-232 je velmi malý převodník XPort Pro, který využívá k běhu Linuxové jádro s podporou protokolu IPv6. Další výhoda tohoto modelu je možnost nahradit s ním současně používaný převodník XPort v docházkových terminálech aniž by bylo třeba je měnit celé. Cena jednoho kusu je 1 950 Kč bez DPH (Papouch, 2012).

Obrázek 18: Převodník RS-232 na Ethernet XPort Pro (Zdroj: Papouch, 2012)

Pro RS-485 zatím neexistuje malé řešení v podobě převaděče XPort Pro. Lze ale využít přípravek Triton od výrobce Papouch, který umožňuje do jednoho zařízení připojit 4 linky na standardu RS-232 nebo po dodání vhodných modulů 4 linky na standardu RS-422/485. Cena zařízení je 7 950 Kč a cena jednoho modulu se pohybuje kolem 800 Kč bez DPH (Papouch, 2012)

K dispozici je také kombinované řešení, které umožňuje převod signálu RS-485 na RS-232 a tento dále pomocí zařízení XPort převést do IPv6 sítě. V tomto případě se ale cenově dostáváme mírně pod cenu přípravku Triton s nebezpečím, že je signál dvakrát převáděn. Proto tento způsob nedoporučuji.

Obrázek 19: Přípravek Triton (Zdroj: Papouch, 2012)

V technologické části převodníků se setkáváme ještě s problémem teploměrů. Jelikož v současné době není na trhu teploměr, podporující IPv6 připojení, jediným vhodným řešením je nasazení teploměru, komunikujícího přes RS-232 a jeho propojení se sítí zařídit pomocí komunikačního modulu XPort Pro. Příkladem může být teploměr TM-RS232 od výrobce Papouch, který posílá naměřenou teplotu jako řetězec v ASCII přes sériovou linku RS-232. Cena obdobných teploměrů se pohybuje okolo 500 Kč bez DPH. Cena převodníku XPort Pro je 1 950 Kč bez DPH.

Poslední a zároveň nejdůležitější část technologické sítě jsou převodníky ze sítě MetaSys na Ethernet NCM350. Ty je možné nahradit dalšími moduly od výrobce Johnsons Control. Konkrétně se jedná o moduly NCE25, sloužících pro převod informací ze sítí N2Bus, BACNet a LonWorks na Ethernet, a NIE, sloužící pro připojení zařízení třetích stran. NCE25 dokáže zprostředkovat připojení k síti až pro 32 zařízení, které zastřešuje. Zároveň nové moduly podporují protokol IPv6 (Johnson Controls, 2010; Šesták).

Kromě prvků technologické a kancelářské sítě je třeba nahradit také IPv6 nekompatibilní směrovač Cisco 1605, jehož úkolem je momentálně směrovat provoz z provozu Špitálka na provoz Staré Brno. Tento směrovač doporučuji nahradit typem Cisco 2901. Do všech existujících směrovačů Mikrotik na technologické části sítě bude potřeba zavést nový Mikrotik RouterOS s podporou IPv6.

Při změně hardwaru na úseku technologické sítě je třeba také myslet na obslužný SW. Jelikož se jedná převážně o jednoduché a jednoúčelové technologické programy, můžeme se v této oblasti také setkat s nekompatibilitou.

4.1.3 Náklady na přechod

Přibližné náklady na plný přechod jsou zobrazeny v tabulce 13. Ceny jednotlivých kusů HW jsou počítány podle zaokrouhlených cen, obvyklých v internetových obchodech v první polovině roku 2012.

Součástí výpočtů v tabulce 13 také nejsou CAL licence na systém Windows Server 2008 R2. Protože servery, založené na tomto systému v podniku již fungují, předpokládám, že jsou licence zakoupeny.

Cena za hodinu práce je stanovena na základě údajů o hrubé mzdě konzultanta IT, kterou na svých stránkách uvádí Český statistický úřad (2011). Ta vychází na částku 43 000 Kč za měsíc v roce 2010. Vydělíme-li částku počtem pracovních hodin v měsíci (42,5 * 4), výsledná částka činí přibližně 250 Kč za hodinu.

Tabulka 13: Přibližná kalkulace nákladů na přechod

Položka	Náklady
Kancelářská část celkem	**1 329 000 Kč**
Windows Server 2008 R2 (7 licencí á 92 000 Kč)	644 000 Kč
Server (př. Dell PowerEdge R310 QC-X3430) 7 ks á 53 000 Kč	371 000 Kč
Print server HP JetDirect EN1700 45 ks á 6 000 Kč	270 000 Kč
Práce	
... instalace serverů, migrace služeb (7 ks * 10 hodin)	17 500 Kč
... nastavení tisku a síťových služeb (50 hodin)	12 500 Kč
... nastavení IPv6 na stanicích s Windows XP (15 hodin)	3 750 Kč
... odladění nedostatků (50 hodin)	10 250 Kč
Technologická část celkem	**65 250 Kč**
Lantronix XPort pro 13 ks á 2 000 Kč (docházka)	26 000 Kč
Teploměr + Lantronix XPort 7 ks á 2 500	17 500 Kč
Převaděč RS-485 – Ethernet Papouch Triton	8 000 Kč
Práce	
... úprava docházkového systému (40 hodin)	10 000 Kč
... výměna teploměrů + konfigurace (5 hodin)	1 250 Kč
... konfigurace routerů Mikrotik (10 hodin)	2 500 Kč
Páteřní síť a aktivní prvky	**52 500 Kč**
Cisco 2901 1 ks	40 000 Kč
Práce	
... konfigurace ostatních serverů (30 hodin)	7 500 Kč
... konfigurace aktivních prvků (20 hodin)	5 000 Kč
Předpokládané náklady celkem	**1 381 500 Kč**

Upraveno dle: svetsoftware.cz; czc.cz; papouch.com; c-shop.cz

V tabulce není zahrnutá nejdůležitější součást technologické sítě, výměna převodníků NCM350 za NCE25. Kalkulace ceny probíhá na základě analýzy firmy Johnson Control u konkrétního zákazníka. Dá se ale předpokládat, že cenová nabídka se bude pohybovat v jednotkách milionů včetně instalace zařízení a bude největší položkou, vynaloženou na přechod na IPv6.

4.2 Varianta částečného přechodu

Druhá varianta je oproti předchozí možnosti méně zaměřená na maximální využití IPv6 protokolu ve firemní síti. Soustřeďuje se spíše na možnosti okamžité implementace IP protokolu příští generace do kancelářské sítě, zatímco technologická síť bude z větší části stále setrvávat na IPv4.

Výhoda částečné varianty oproti předchozímu modelu spočívá v nižší finanční náročnosti a také menší potřebě nahrazovat zařízení na technologickém úseku sítě. Jak

bylo nastíněno v předchozím případě, může se totiž stát, že konkrétní řešení momentálně na trhu nejsou dostupná a bylo by třeba ji nahrazovat ne úplně ideálním řešením.

4.2.1 Sítě, podsítě a uzly

Aby bylo možné na současném hardwaru oddělit technologickou síť a případné další pomocné sítě, bude na páteřní síti Tepláren Brno nadále provozován VRF-lite. Nebude ale zasahovat do kancelářské sítě, jejíž vydělení z IPv4 provozu je dané typem protokolu. Kancelářská síť bude tedy provozována čistě na protokolu IPv6. Osazené směrovače Cisco 3620 dokáží komunikovat pomocí dvojího zásobníku, takže v důsledku vedle sebe mohou na páteřní síti fungovat dva protokoly, IPv4 a IPv6. Oddělení sítí na portech přepínačů bude probíhat jako dosud, za použití IEEE 802.1Q.

Rozhraní jednotlivých zařízení na úseku technologické sítě budou využívat svoje stávající IP adresy. Kancelářská část sítě bude využívat adresní rozsahy podle návrhu z tabulky 11 kapitoly 4.1.1 s tím, že pro budoucí převedení dalších segmentů sítě může být využito započaté IPv6 číslování. Nepočítá se tedy pouze se sítí kancelářskou, ale do budoucna i s převedením sítě technologické.

Pro směrování paketů mezi kancelářskou a technologickou sítí bude třeba na jednotlivých páteřních směrovačích nasadit buďto NAT-PT nebo NAT 64. Oba dva jsou směrovači Cisco podporovány. Doporučuji zvolit NAT-PT. Nevýhoda nekonzistentních DNS záznamů je vyvážena možností navázat spojení i z IPv4 sítě, což v případě NATu64 nelze. Bude tak možné navazovat spojení z technologické sítě do kancelářské.

Podmínka u NAT-PT, aby DNS servery ležely uvnitř IPv6 kancelářské sítě, je v tomto případě splněna. Řešení bude využívat IPv4 mapovaných adres ve tvaru ::ffff:a.b.c.d, kde a, b, c, d jsou označením pro IPv4 adresu uzlu v technologické síti. Jedná se o standardní adresu, generovanou SIIT.

Výhodou přechodu na částečný model je skutečnost, že přechod nemusí proběhnout okamžitě. Většinu kancelářské sítě lze i nadále ponechat na protokolu IPv4 a díky systému dvojího zásobníku a jeho podpoře na koncových stanicích lze IPv6 síť rozbíhat paralelně. Moderní systémy na platformě Windows automaticky upřednostňují IPv6 síť,

ale v případě, že se jim přes ni nepodaří navázat požadované spojení, dokáží komunikovat zároveň přes IPv4.

4.2.2 Upgrade zařízení

Upgrade zařízení odpovídá požadavkům na plný přechod. V tomto případě se ale nebude realizovat technologická část sítě, pouze kancelářská. Změna se týká především některých serverových stanic na úseku kancelářské sítě a síťových tiskáren tamtéž, které budou osazeny tiskovým serverem s podporou IPv6.

Docházkové terminály i další podpůrné služby jsou v jednotlivých lokalitách provozovány v rámci technologické sítě, která v tomto případě zůstává zachovaná v původní podobě.

Nespornou výhodou částečného přechodu je skutečnost, že většina kancelářské části sítě je na přechod relativně připravena. Jedinou nepřiměřeně velkou položkou v tomto případě bude nákup nových systémů Windows Server 2008 R2 spolu s CAL licencemi pro jednotlivé uživatele či přístroje.

4.2.3 Náklady na přechod

Náklady na částečný přechod jsou obdobné, jako v případě přechodu segmentu kancelářské sítě a páteřní sítě v tabulce 13 v kapitole 4.2.3. Přibližná cena činí 1 316 250 Kč.

Velký cenový rozdíl oproti předchozí variantě není v tabulce vidět a sestává hlavně z implementace nové verze převodníků (nyní NCM350), který se n tomto případě nebude realizovat.

5 Závěr

Ve své práci jsem analyzoval současnou podobu sítě Tepláren Brno, a.s. a následně se pokusil vytvořit dvě základní varianty, jakými lze přechod realizovat – maximální a částečnou.

Maximální varianta klade velké požadavky na hardware a jeho kompatibilitu s novým protokolem, což je v dnešní době u specifických zařízení stále nesplnitelné. Setkáváme se také s případy, kdy sice zařízení IPv6 podporuje, nicméně ještě není vyroben ovládací SW, který je schopen s ním komunikovat. Přechod na IPv6 v této úrovni je tedy možný, ale s určitými výhradami. Některé části sítě by musely být překládány do verze IPv4, což je v tomto případě krok zpátky a mohla by být potíž s kompatibilitou. Hrozí zde reálné riziko, že v rámci přechodu by mohlo dojít ke snížení komfortu práce pro uživatele počítačové sítě, zvláště na technologickém úseku.

Částečný přechod spočívá v ponechání páteřní sítě a technologické části na stávajícím protokolu IPv4 a převedením kancelářské sítě na IPv6. Toto řešení má oproti předchozímu výhodu v tom, že kancelářská síť nedisponuje takovým množstvím specializovaných zařízení, u kterých bychom mohli očekávat velké problémy s přechodem. Další pozitivní přínos je, že se při provozování na kancelářském segmentu mohou odladit specifika protokolu a pozdější nasazení na technologické části bude snadnější.

Také u částečného přechodu ale hrozí, že komunikaci pro monitorování a řízení technologických zařízení bude nutné tunelovat na IPv4. Může tak vzniknout situace, kdy se po vynaložení velkých prostředků na přechod budou hledat cesty, kterými bude možné nadstavit IPv6 starší verzí protokolu. Proto na závěr této práce doporučuji jakýkoliv přechod za současné technologické situace v oboru teplárenství obecně odložit. Zároveň je ale v případě nákupu nových nebo upgrade stávajících řešení nutné myslet na to, aby byla kompatibilní s IPv6 a chystat si cesty, kterými bude v pozdější době možné pohodlně a bez větších problémů přejít.

Seznam použitých zdrojů

APC. *APC Česká republika* [online]. 2012 [cit. 2012-01-30]. Dostupné z: http://www.apc.com/site/apc/

CISCO SYSTEMS. *Cisco Systems* [online]. 2012a [cit. 2012-02-16]. Dostupné z: http://www.cisco.com

CISCO SYSTEMS. *NAT64 Technology: Connecting IPv6 and IPv4 Networks*. [b. m.], 2012b. Dostupné z: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-676278.pdf

ČESKÝ STATISTICKÝ ÚŘAD. *Mzdy IT odborníků v České Republice v roce 2010*. [b. m.], 2011. Dostupné z http://www.czso.cz/csu/redakce.nsf/i/mzdy_it_odborniku_v_ceske_republice/$File/2_ito_platy_11.pdf

DOSTÁLEK, Libor; KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. aktualizované vydání. Praha: Computer Press, 2000. 426 s. ISBN 80-7226-323-4.

EDIMAX TECHNOLOGY. *Edimax Technology* [online]. 2012 [cit. 2012-02-16]. Dostupné z: http://www.edimax.com

HAEUSSER, Babette. *IBM System Storage Tape Library guide for open systems*. 7th ed. United States: IBM, International Technical Support Organization, 2008, 544 s. ISBN 07-384-3155-9. Dostupné z: http://my.safaribooksonline.com/book/operating-systems-and-server-administration/storage-systems/0738431559

HURRICANE ELECTRIC. AS24641 This is AS for ISP Faster, Brno, CZ. *Hurricane Electric Internet Services* [online]. 2012 [cit. 2012-01-30]. Dostupné z: http://bgp.he.net/AS24641#_prefixes6

HUSTON, Geoff. IPv4 Adress Report: *Geoff Huston - potaroo.net* [online]. 2011 [cit. 2011-11-12]. Dostupné z: http://ipv4.potaroo.net/

IANA. Protocol Numbers. *InternetAssigned Numbers Authority* [online]. 2011 [cit. 2011-11-12]. Dostupné z: http://www.iana.com/assignments/protocol-numbers/protocol-numbers.xml

IEEE. *Guidelines for 64-bit Global Identifier (EUI-64™) Registration Authority*. [b. m.], 1997. Dostupné z: http://standards.ieee.org/develop/regauth/tut/eui64.pdf

KRČMÁŘ, Petr. *Linux: postavte si počítačovou síť.* Brno: Grada, 2008. 182 s. ISBN: 80-247-1290-3.

KYOCERA. *Kyocera Document Solutions Europe* [online]. 2012 [cit. 2012-01-30]. Dostupné z: http://www.kyoceradocumentsolutions.eu/index/service/dlc.html

LANTRONIX. *Embedded networking modules*. [b. m.], 2011. Dostupné z: http://www.lantronix.com/pdf/misc/Embedded-Module-Matrix.pdf

MICROSOFT. TechNet: *Exploring IPv6* [online]. 2003 [cit. 2011-11-12]. Dostupné z: http://technet.microsoft.com/en-us/library/cc776103%28v=ws.6%29.aspx

MIKROTIK. MikroTik Wiki: *Manual: IPv6 Overview* [online]. 28.11.2011 [cit. 2012-03-16]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:IPv6_Overview2

MORIMOTO, Rand. Secrets of Windows BackOffice Servers: *Migrationg to Active Directory 2008 R2*. [online]. 2010 [cit. 2012-05-13]. Dostupné z: http://www.networkworld.com/community/node/56345

NETAPP. *NetApp.com* [online]. 2012 [cit. 2012-01-30]. Dostupné z: http://www.netapp.com/

PACKET LIFE. Intro to VRF lite. *Packet Life* [online]. 30.4.2009 [cit. 2012-03-17]. Dostupné z: http://packetlife.net/blog/2009/apr/30/intro-vrf-lite/

PAPOUCH. *Papouch.com* [online]. 2012 [cit. 2012-01-30]. Dostupné z: http://www.papouch.com/

PETERKA, Jiří. Principy počítačových síti. *Jiří Peterka – eArchiv.cz* [online]. 1997 [cit. 2012-02-16]. Dostupné z: http://www.earchiv.cz/i_pri.php3

PETŘÍK, Michal. ČVUT. *Technologie MPLS*. [b. m.], 2007. Dostupné z: https://dsn.felk.cvut.cz/wiki/_media/vyuka/cviceni/x36mti/petrim2-doc.pdf

RFC 2460. *Internet Protocol, Version 6 (IPv6) Specification*. [b. m.]: Network Working Group, 1998. 39 s. Dostupné z: http://www.ietf.org/rfc/rfc2460.txt

RFC 3056. *Connection of IPv6 Domains via IPv4 Clouds*. [b. m.]: Network Working Group, 2002, 7 s. Dostupné z: http://www.ietf.org/rfc/rfc3306.txt

RFC 3306. *Unicast-Prefix-based IPv6 Multicast Addresses*. [b. m.]: Network Working Group, 2001, 23 s. Dostupné z: http://www.ietf.org/rfc/rfc3056.txt

RFC 3596. *DNS Extensions to Support IP Version 6.* [b. m.]: Network Working Group, 2003, 8 s. Dostupné z: http://www.ietf.org/rfc/rfc3596.txt

RFC 3697. *IPv6 Flow Label Specification*. [b. m.]: Network Working Group, 2004. 9 s. Dostupné z: http://www.ietf.org/rfc/rfc3697.txt

RFC 4193. Unique Local IPv6 Unicast Addresses. [b. m.]: Network Working Group, 2005, 16 s. Dostupné z: http://www.ietf.org/rfc/rfc4193.txt

RFC 4291. *IP Version 6 Addressing Architecture.* [b. m.]: Network Working Group, 2006. 25 s. Dostupné z: http://www.ietf.org/rfc/rfc4291.txt

RFC 4380. *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*. [b. m.]: Network Working Group, 2006, 53 s. Dostupné z: http://www.ietf.org/rfc/rfc4380.txt

RFC 4443. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.* [b. m.]: Network Working Group, 2006, 24 s. Dostupné z: http://www.ietf.org/rfc/rfc4443.txt

RFC 4786. Operation of Anycast Services. [b. m.]: Network Working Group, 2006, 24 s. Dostupné z: http://www.ietf.org/rfc/rfc4786.txt

RFC 4862. *IPv6 Stateless Address Autoconfiguration.* [b. m.]: Network Working Group, 2007. 30 s. Dostupné z: http://www.ietf.org/rfc/rfc4862.txt

RFC 4862. *IPv6 Stateless Adress Autoconfiguration.* [b. m.]: Network Working Group, 2007, 30 s. Dostupné z: http://www.ietf.org/rfc/rfc4862.txt

RFC 5735. *Special Use IPv4 Adresses.* [b. m.]: Internet Eningeneering Task Force, 2010. 11 s. Dostupné z: http://www.ietf.org/rfc/rfc5735.txt

RFC 5952. *A Recommendation for IPv6 Address Text Representation.* [b. m.]: Internet Engineering Task Force, 2010. 14 s. Dostupné z: http://www.ietf.org/rfc/rfc5952.txt

SATRAPA, Pavel. *Internetový protokol verze 6.* Praha: CZ.NIC, 2008. 357 s. ISBN: 978-80-904248-0-7.

SCHNEIDER ELECTRIC. *Overview of PowerChute Network Shutdown Installation for ESXi*. [b. m.], 2012. Dostupné z: http://www.apcmedia.com/salestools/PMAR-8RNGUL_R0_EN.pdf

ŠTORKOVÁ, Veronika. Netguru: *Techniky a řešení paralelního fungování a přechodů mezi IPv4 a IPv6* [online]. 2012 [cit. 2012-05-02]. Dostupné z: http://www.netguru.cz/odborne-clanky/techniky-a-eeni-paralerniho-fungovani-a-pechodu-z-v4-a-v6.html

Telefonický rozhovor s p. Martinem ŠESTÁKEM, systems managerem spol. Johnson Controls. Brno: 12.3.2012.

TEPLÁRNY BRNO. Historie společnosti. *Teplárny Brno* [online]. 2011 [cit. 2011-11-12]. Dostupné z: http://www.teplarny.cz/?page=historie

TEPLÁRNY BRNO. Provoz Červený mlýn. *Teplárny Brno* [online]. 2011 [cit. 2011-11-12]. Dostupné z: http://www.teplarny.cz ?page=cerveny-mlyn

TEPLÁRNY BRNO. Přehled historických milníků. *Teplárny Brno* [online]. 2011 [cit. 2011-11-12]. Dostupné z: http://www.teplarny.cz/?page=milniky

TEPLÁRNY BRNO. *Výroční zpráva za období 10/2008 – 9/2009*. [Brno]: 2009. 94 s. Dostupné z: http://www.teplarny.cz/?download=_/vyrocni-zpravy/telp_vz_09_cmyk_low.pdf

TEPLÁRNY BRNO. *Výroční zpráva za období 10/2009 – 9/2010*. [Brno]: 2010. 70 s. Dostupné z: http://www.teplarny.cz/?download=_/vyrocni-zpravy/tb-vz2010_low-single.pdf

TULLOCH, Mitch. IPv6 Support in Microsoft Windows. *WindowsNetworking.com* [online]. 2006 [cit. 2011-11-12]. Dostupné z: http://www.windowsnetworking.com/articles_tutorials/ipv6-support-microsoft-windows.html

Seznam obrázků a tabulek

Seznam obrázků

Seznam tabulek

Příloha 1: Seznam malých lokalit Tepláren Brno, a.s.

Číslo	Lokalita	Číslo	Lokalita
1	Bystrc	32	PK, Libušino údolí 154a
2	PK, Absolonova 93a	33	POS, Mozolky
3	PK, Axmanova 12a	34	HO, Nejedlého 5
4	PK, Bellova 38a	35	VS, Novolíšeňská 5
5	HO, Bieblova 38	36	PK, Opálkova 6a
6	VO, Čejkovická 8	37	PK, Pastviny 3a
7	PK, Čoupkových 10a	38	PK, Pavlovská 5a
8	PK, Dědická 1a	39	POS, Plovdivská 7
9	VSHO, Došlíkova 31a	40	PK, Polívkova 12
10	PK, Dunajská 47	41	POS, Poznaňská 10
11	VS, Elplova 38	42	PK, Prostějovská 20
12	VS, Elišky Krásnohorské 22	43	PK, Renčova 32a
13	PK, Fryčajova 145a	44	PK, Řezáčova 24a
14	HO, Halasovo nám. 3	45	POS, Sabinova 1
15	HO, Herčíkova 17	46	VS, Souběžná 11
16	PK, Heyrovského 30a	47	Stamicova 5
17	VS, Hochmanova 8	48	VS, Synkova 24a
18	VS, Húskova 4	49	VS, Štefáčkova 13
19	Jánošíkova 41	50	PK, Švermova 12
20	TB Služby s.r.o.	51	PK, Švermova 15
21	PK, Jasanová 26a	52	HO, Třískalova 14
22	HO-8, Jurkovičova	53	PK, Ukrajinská 1a
23	PK, K Rybníku 1	54	PK, Valouškova 2a
24	PK, Kamínky 5a	55	PK, Vaňhalova 1a
25	VS, Kosmákova 46a	56	PK, AC Platinium
26	VS5, Kotlanova 10	57	VS, Vlkova 2
27	VS12, Kubíkova 22	58	POS, Vychodilova 17
28	KR5, Kunštátská 11a	59	Sovinec
29	PK, Kyjevská 3a	60	PK, Za mostem 22
30	PK, Labská 8	61	POS, Zborovská 43
31	PK, Laštůvkova 75a	62	VS, Zikova 34

HO	Hospodářský objekt
VO	Výměníkový objekt
VS	Výměníková stanice
PK	Plynová kotelna
POS	Pavilon otopné soustavy