Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Monitorování parametrů připojení na Internet

Milan Martinec

Bakalářská práce
2012

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2011/2012**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Milan MARTINEC**
Osobní číslo:	**E09919**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informatika ve veřejné správě**
Název tématu:	**Monitorování parametrů připojení na Internet**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Návrh systému pro monitorování a logování parametrů připojení k Internetu (rychlost stahování dat, rychlost odezvy serverů - ping, identifikace výpadků,...).
Implementace s minimálními pořizovacími náklady (tj. za pomoci volně šiřitelného software a volně šiřitelného operačního systému).
Provedení monitorování za určité období (minimálně 1 měsíc), porovnání automatického sledování s ručním za sledované období, vyhodnocení výsledků.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

ZANDL, PATRICK., Bezdrátové sítě WiFi Praktický průvodce. 1. Vyd. Brno: Computer Press, 2003, 190 s., ISBN: 80-7226-632-2.

DOSTÁLEK, LIBOR, KABELOVÁ, ALENA, Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualizované vydání Brno: Computer Press, 2008, 488 s., ISBN: 978-80-251-2236-5.

SCHRODER, CARLA, Linux Kuchařka administrátora sítě. Vydání první Brno: Computer Press, 2009, 608 s., ISBN: 978-80-251-2407-9.

Vedoucí bakalářské práce: **Ing. Martin Novák**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **3. října 2011**

Termín odevzdání bakalářské práce: **30. dubna 2012**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. října 2011

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 28. 6. 2012 Milan Martinec

PODĚKOVÁNÍ:

Tímto bych rád poděkoval svému vedoucímu práce Ing. Martinu Novákovi za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Tato bakalářská práce se zabývá návrhem a implementací monitoringu připojení na Internet, jmenovitě rychlosti stahování, odezvy serverů a identifikace výpadků připojení. Za tímto účelem je zde navržen a realizován monitorovací systém využívající Cacti a RRDTool, implementovaný v operačním systému Linux. Tímto způsobem lze snadno dosáhnout nejnižších pořizovacích nákladů.

KLÍČOVÁ SLOVA

Internet, Wi-Fi, monitoring, Open-Source, Cacti, PHP

TITLE

Monitoring Internet connection parameters

ANNOTATION

This bachelor thesis deals with the design and implementation of Internet connection monitoring, namely download speed, server response time and identification of connection failures. To fulfil this task a monitoring system has been designed and constructed using Cacti and RRDTool on a Linux operating system base. In this way it is easy to attain the lowest implementation costs.

KEYWORDS

Internet, Wi-Fi, monitoring, Open-Source, Cacti, PHP

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

ÚVOD

Kvalita připojení k Internetu, především rychlost stahování, rychlost odezvy a množství výpadků zajímá každého klienta. Ve své práci se zabývám monitoringem připojení vytvořeného pomocí bezdrátové technologie Wi-Fi, protože jiné připojení nemám k dispozici. Tento druh připojení je zároveň nejrozšířenějším typem připojení domácností v České republice.[1] Tato technologie je velmi specifická a kvalita připojení není závislá pouze na použitém technickém vybavení, ale vzhledem k přenosovému médiu také na prostředí implementace, povětrnostních podmínkách a ročním období. Jinak se chová signál v husté zástavbě s množstvím odrazů a rušení, jinak ve volném prostranství, za slunečného dne, nebo hustého sněžení. Pro účel této práce však vlastní technologie připojení není podstatná a funkčnost navrhovaného systému je vždy identická.

Cílem práce je navrhnout monitorovací systém, výběr monitorovaných bodů v síti z hlediska identifikace výpadku. Vlastní realizace systému prostřednictvím PC s Linuxovým operačním systémem, volně šiřitelným monitorovacím software a jeho provozování. Vyhodnocení naměřených údajů a jejich porovnání s ručním sledováním připojení.

[1] Zdroj: [3] Informační a komunikační technologie

1. INTERNET

Pro získání komplexního pohledu na problematiku je nutné objasnit, co je vlastně monitorováno.

1.1. Historie Internetu

Historie Internetu sahá do 60. let 20. století, kdy se americká vláda začala zajímat o vývoj počítačové sítě, která by umožňovala komunikaci mezi vojenskými systémy a hlavními vzdělávacími institucemi. Koncem 60. let se badatelé a vědci pracující v Massachusetts Institute of Technology (MIT), v RAND Institute a UCLA zabývali myšlenkou vytvoření decentralizované sítě s přepojováním paketů. Tato myšlenka byla finančně podpořena americkou institucí Advanced Research Project Agency (ARPA). První úspěch však zaznamenali Britové, jejichž testovací síť byla instalována v roce 1968 v National Physical Laboratory. V roce 1969 byla vytvořena síť nazvaná ARPANET zpočátku propojující pouhé čtyři uzly, avšak v roce 1972 již spojovala 50 výzkumných a vojenských center. Později došlo k jejímu rozdělení na dvě sítě: Arpanet a Milnet (armádní síť). V roce 1981 přibyla síť Bitnet, která propojovala americké vysoké a střední školy. Problémem byla potřeba vzájemné komunikace mnoha různých platforem. Proto byly v roce 1973 zahájeny práce na sadě protokolů TCP/IP, které umožnily připojit jakýkoli systém k jinému systému, prostřednictvím libovolné síťové topologie. V roce 1978 byla dokončena IP verze 4 (stejná verze, kterou používáme dodnes).[2] Domain Name System (DNS) byl představen v roce 1984, čímž byl nabídnut mnohem elegantnější způsob „přívětivého" přístupu k IP adresám, což bylo mnohem pohodlnější a efektivnější, než metody předchozí. V roce 1984 bylo na síti již více než 1000 počítačů.[3] Ačkoliv v polovině 80. let existovalo několik sítí, stále ještě nebyly předmětem zájmu veřejnosti, protože nebyly volně přístupné. V roce 1986, US National Science Foundation (NSF) vytvořil páteřní síť NSFNET propojující superpočítače pěti univerzit, což se následně ukázalo jako velmi důležitý krok v historii Internetu, protože toto řešení bylo natolik výhodné, že v roce 1990 byla síť Arpanet zrušena a nahrazena právě sítí NSFNET a síť byla zpřístupněna veřejnosti. V roce 1991 nad ní byla vytvořena nová síť NREN (National Research and Education Network). V roce 1994 NSFNET přešel na komerční provoz a v roce 1995 je síť otevřena pro podnikání. Přístup k Internetu je mnohem důležitější i pro úspěch ostatních sítí, včetně Usenet, BITNET a různých komerčních sítí založených na X.25. Přestože současný Internet představuje celou řadu služeb, zcela zásadním pro jeho

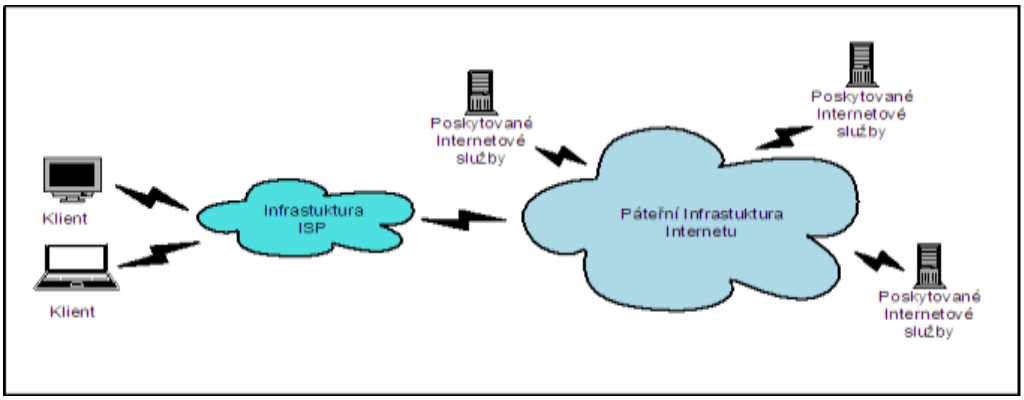
[2] Zdroj: [5] TCP/IP to the Rescue, strana 3
[3] Zdroj: [13] Stručná historie počítačových sítí, strana 39

rozvoj je vznik služby WWW. Již v roce 1980 přišel ve švýcarském institutu pro jaderný výzkum CERN **Tim Berners-Lee** s myšlenkou hypertextu, což mělo usnadnit sdílení a aktualizaci informací mezi výzkumníky. V souvislosti s rozvojem sítí tuto myšlenku oživil a 6. srpna 1991 na adrese http://info.cern.ch spustil první webové stránky. První webový prohlížeč s názvem WorldWideWeb byl textový. V roce 1992 počal vývoj grafického browseru Mosaic, vytvořeného na půdě NCSA (National Center for Supercomputing Applications). Společně s browserem Mosaic vznikla společnost Mosaic Communications, která je později spolu s prohlížečem přejmenována na Netscape Communications. Institucí, která od poloviny roku 1994 dohlíží na vývoj standardu WWW, je WWW Consorcium (W3C). Konsorcium sdružuje lidi, kteří se podíleli v ústavu CERN na vzniku WWW, techniky z MIT a z francouzského institutu INRIA. Ředitelem konsorcia je tvůrce WWW Tim Berners-Lee.

1.2. Jak funguje Internet

1.2.1. Spojení sítí

Internet je tvořen spojením tisíců velkých a malých sítí, které jsou dislokovány po celém světě. Propojené počítače lze z funkčního hlediska hrubě rozdělit na servery a klienty, tedy poskytovatele služeb a příjemce služeb. Poskytovatelé služeb mohou mít servery umístěny ve své firmě, většinou však využívají hostingová centra, která poskytují prostor na svých serverech za úplatu, ve specifických případech i zdarma. Poskytované služby jsou využívány „klientskou“ částí Internetu, tedy jednotlivými PC připojenými k síti Internet. Co do počtu je samozřejmě tato část v drtivé převaze. Vlastní připojení k Internetu je realizováno zpravidla prostřednictvím ISP (Internet Service Provider), tedy někoho, kdo nabízí připojení k Internetu a sám je připojen buď přímo k páteřní síti, v České Republice tedy připojen do peeringového centra NIX.CZ (Neutral Internet eXchange), nebo využívá konektivitu většího poskytovatele.



Obrázek 1: Zjednodušený příklad struktury Internetu

Zdroj: Vlastní zpracování

1.2.2. Protokoly

Při komunikaci v počítačových sítích je využíváno více vrstev. Počet vrstev závisí na tom, která soustava síťových protokolů je použita. Nejčastěji využívanou soustavou je rodina protokolů TCP/IP, která je čtyřvrstvá. Mimo protokolů TCP/IP lze narazit na sedmivrstvou soustavu ISO OSI, kterou standardizovalo ISO. Jejich porovnání ukazuje tabulka číslo 1.

Tabulka 1: Porovnání rodiny protokolů TCP/IP a ISO OSI

Sada protokolů	
TCP/IP	ISO OSI
Aplikační	Aplikační
	Prezentační
	Relační
TCP/IP	Transportní
Internet (IP)	Síťová
Linková a fyzická	Linková
	Fyzická

Zdroj: upraveno podle [1]

Na Internetu se používá mix rodiny protokolů TCP/IP, protokolů ITU a ISO. Přitom protokoly ITU a ISO se vyskytují zejména na spodních dvou vrstvách, fyzické a linkové.[1] Připojené počítače a servery využívají nejrůznější operační systémy, společným komunikačním jazykem je rodina protokolů TCP/IP. Ještě pod nimi na úrovni linkové a fyzické vrstvy lze nalézt i protokoly ITU a ISO jako např. Ethernet, Token Ring, ATM, Wi-Fi.

1.2.3. Transportní protokoly

TCP (Transmission Control Protocol) - protokol pro řízení přenosu, zajišťuje správnou cestu pro tok dat a zodpovídá za poskytování spolehlivé komunikace mezi dvěma body. Protože různé aplikace mohou zasílat nebo přijímat zprávy zároveň, protokoly transportní vrstvy používají porty pro oddělení jejich komunikace. Ke každému paketu je přidána sekvenční informace, tak aby mohly být části zprávy opět složeny ve správném pořadí. Tato informace také umožňuje přijímajícímu počítači zjistit, zda nechybějí nějaké pakety.

IP (Internet Protocol) zabezpečuje doručení všech paketů dat na správné místo, ve správném pořadí a tam jejich opětovné poskládání, tedy dopravuje data mezi dvěma libovolnými počítači v Internetu, vlastně tím umožňuje spojit jednotlivé lokální sítě do celosvětového Internetu.

IP protokol se skládá z několika dílčích protokolů:

- Vlastního protokolu IP.

- Z protokolu ICMP (Internet Control Message Protocol) sloužícího zejména pro signalizaci mimořádných stavů.
- Služebního protokolu IGMP (Internet Group Management Protocol) sloužícího pro dopravu adresných oběžníků.
- Služebních protokolů ARP (Address Resolution Protocol) a RARP (Reverse Address Resolution Protocol), které jsou často vyčleňovány jako samostatné, na IP nezávislé protokoly, protože jejich pakety nejsou vkládány do IP datagramu, ale přímo do linkového rámce.

UDP (User Datagram Protocol) je bezespojový. Nesekvencuje pakety, ve kterých přicházejí data, to znamená, že je vhodný pro malé zprávy, které mohou být přenášeny v jednom paketu. Ve srovnání s protokolem TCP nezaručuje, zda se přenášený datagram neztratí, zda se nezmění pořadí doručených datagramů nebo zda se některý datagram nedoručí vícekrát. Poskytuje však kontrolní součet, aby zajistil nedotčenost dat při příchodu. Tak jako TCP poskytuje čísla portů.

1.2.4. Aplikační protokoly

Aplikační protokol (Aplication Protocol) je specifický komunikační protokol například pro jednotlivé služby Internetu, HTTP (Hyper Text Transfer Protocol), používaný ve WWW, FTP (File Transfer Protocol) pro přenos souborů po Internetu, SMTP, IMAP a POP3 pro elektronickou poštu. Existuje celá řada dalších aplikačních protokolů.

1.2.5. Adresace

Aby mohla nějaká komunikace vůbec probíhat, komunikující body musí mít svoji adresu. Funkce adresace je vykonávaná na více vrstvách, podle potřeb každé jednotlivé vrstvy. Zatímco pro uživatele je vhodné označování jednotlivých síťových zařízení popisnými jmény, komunikační systémy používají adresy číselné.

Linkové adresy - (MAC adresy) jsou fyzické, hardwarové adresy, unikátní pro každé síťové zařízení. Ve skutečnosti jsou napevno „vypáleny" v obvodech rozhraní síťového adaptéru. Počítačové systémy s jedním fyzickým připojením k síti mají jednu linkovou adresu. Routery a ostatní síťová zařízení připojená k několika fyzickým sítím mají odpovídající množství linkových adres. Linkové adresy existují na druhé úrovni referenčního modelu OSI. Obvyklá je forma zápisu prostřednictvím hexadecimálního čísla, například: 00-50-F1-0D-0F-3C.

Síťové adresy - (logické adresy, IP adresy) existují na úrovni třetí vrstvy referenčního modelu OSI. Na rozdíl od linkových adres, které tvoří plochý adresní prostor, síťové adresy jsou většinou hierarchické. Část adresy tvoří tedy například adresu sítě, podsítě, konkrétního zařízení. Síťové adresy jsou nutné pro nalezení cesty od zdrojové k cílové síti, proto na jejich základě pracují směrovače. Příklad zápisu síťové adresy: 77.75.72.3.

Jmenné adresy - protože není v lidských silách zapamatovat si množství IP adres a tyto adresy navíc nemusí být statické, byla zavedena služba DNS (Domain Name Service), která umožňuje přiřadit každé číselné adrese jmenný název ve tvaru jednoho, častěji však několika slov oddělených tečkami. Například jmenná adresa www.seznam.cz může být směrována na počítač s IP adresou 77.75.72.3 (není podmínkou, pod danou jmennou adresou se v tomto případě skrývá více IP adres). Největším kladem systému doménových jmen je jeho hierarchičnost.

1.3. Technologie připojení k Internetu

Pro připojení klientů k Internetu jsou využívány různé drátové a bezdrátové technologie, k použití té které technologie jsme někdy nuceni územní nedostupností jiného řešení, jindy nás limituje technické vybavení připojovaného zařízení (mobilní telefony).

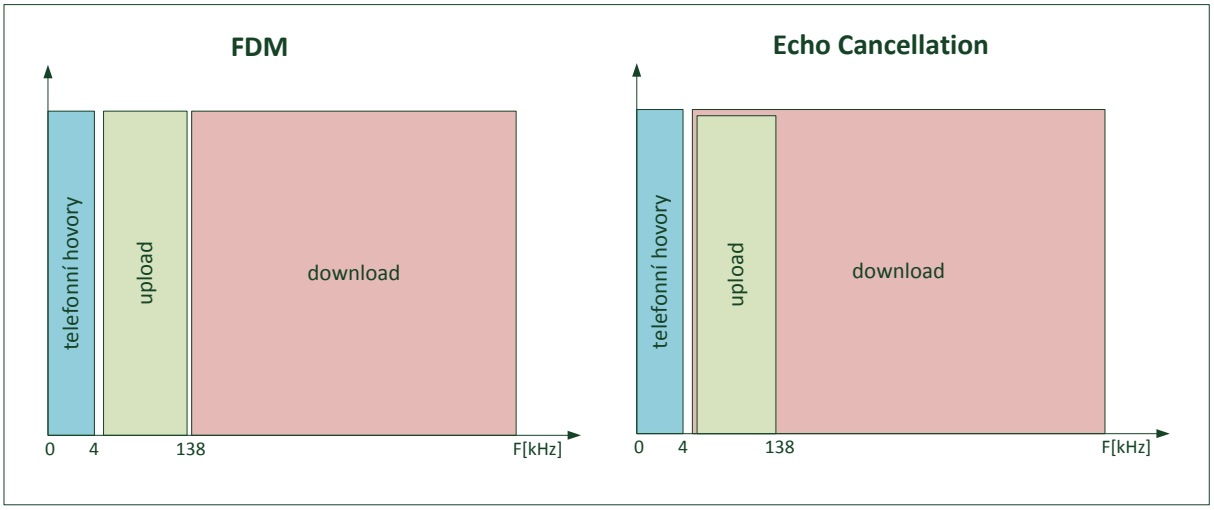
Vytáčené připojení dial-up - pravděpodobně nejstarší masově rozšířené a dnes již v podstatě historické domácí připojení, využívající k datovému přenosu modulaci přenášených paketů na analogový signál. Připojení je realizováno prostřednictvím pevné telefonní linky, ke které je připojen modem, využívající frekvenční pásmo běžně určené pro hlasový přenos. Maximální rychlost linky byla 64 kbps.

euroISDN - opět je využívána pevná telefonní linka, tentokrát je již pro přenos využito digitálního signálu a lze být zároveň připojen i telefonovat. Typ připojení, kdy ve fyzicky jednom vedení jsou dva datové kanály (označované jako kanály B), každý o kapacitě 64 kb/s, a jeden signalizační kanál D o kapacitě 16 kb/s.[4]

ADSL (Asymmetric Digital Subscriber Line) - Fyzicky je realizováno ADSL modemem, připojeným k telefonní lince, na které poběží současně stávající telefonní komunikace (analogová nebo ISDN) a datová komunikace. Komunikace je na obou stranách poměrně snadno oddělena, protože každá využívá jiné frekvenční pásmo. Asymetrie v názvu znamená rozdílnou rychlost downloadu a uploadu dat. Nejvyšší dosahovaná rychlost verze ADSL2+ činí 24 Mbit/s.

[4] Zdroj: [4] ISDN, strana 55

Na obrázku 2 jsou znázorněny dvě metody rozdělení přenosového pásma:



Obrázek 2: Metody rozdělení pásma ADSL

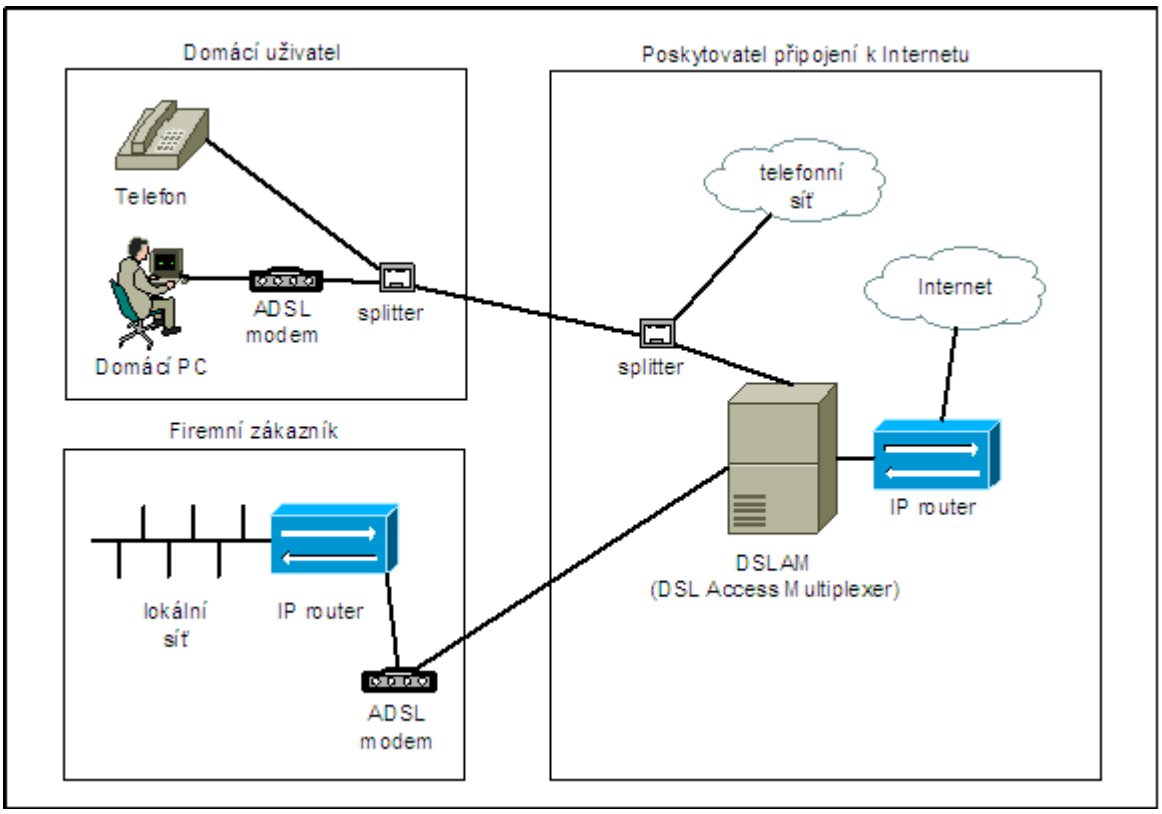
Zdroj: upraveno podle [1]

a) FDM (Frequency Division Multiplexing): Tato metoda přiřadí každému kanálu vlastní část kmitočtového spektra, jedno pásmo pro upload a jiné pro download. Download pásmo je pak metodou TDM (Time Division Multiplexing) rozděleno do jednoho nebo více vysokorychlostních kanálů a do jednoho nebo více nízkorychlostních kanálů. Také upload pásmo je rozděleno do odpovídajícího počtu nízkorychlostních kanálů.

b) EC (Echo Cancellation): Tato metoda přiřadí uploadu pásmo částečně překrývající spodní část pásma pro download na základě metody echo cancellation, dobře známé již z dob standartu V.32 a V.34 modemů (modemů pro vytáčené připojení). V podstatě ADSL modemy na počátku komunikace otestuji linku a pro další komunikaci využijí jen ty kanály, na kterých jsou schopny kvalitně komunikovat. Kanály nižších frekvencí pak využijí pro upload a horní pro download.[5]

V obou případech ADSL odřezává dolní 4kHz pásmo určené pro základní telefonní služby. Na obrázku 3 je vidět typická topologie ADSL připojení.

[5] Zdroj: [4] ADSL, strana 58



Obrázek 3: Typická topologie připojení ADSL

Zdroj: Vlastní zpracování

Kabelový Internet[6] - připojení je realizováno prostřednictvím přípojky kabelové televize, která je předělána tak, aby obsahovala i konektor pro připojení kabelového modemu. Připojení je spolehlivé a rychlé, přenosová rychlost u koncového klienta dosahuje až 100 Mbit/s. Přenosové pásmo je opět rozděleno do jednotlivých kanálů o šířce 6 MHz, respektive 8 MHz, v závislosti na použitém standartu. Moderní kabelové rozvody dosahují přenosové frekvence až 850 MHz. Kanály v dolním frekvenčním pásmu, zhruba do 50 MHz jsou určeny pro upstream, zbylé pásmo je rozděleno přibližně do stovky kanálů pro downstream, z nichž většina je využita pro distribuci TV programů a jeden, případně více spojených, pro zvýšení přenosové kapacity na Internet. Maximální přenosová rychlost závisí také na použité modulaci. Na nižších frekvencích, kde dochází k mnohem většímu rušení, je výhodnější použít pomalejší, ale odolnější modulaci (kódování) a naopak.

Mobilní připojení k Internetu[7] - Mobilní Internet prošel vlastním prudkým vývojem, podobně jako jeho pevná varianta. Mobilní operátoři dnes nabízejí různé technologie pro připojení k Internetu. Každá z těchto mobilních technologií zastupuje určitou generaci vývoje, přičemž v médiích je většinou uváděno generační označení namísto použité

[6] Zdroj: [7] Jak se připojit: kabelový Internet
[7] Zdroj: [8] Mobilní Internet v České republice – kompletní přehled

technologie (např. Internet 3G znamená technologii UMTS, nebo CDMA 1xEV-DO) - rozdělení v tabulce 2.

Tabulka 2: Rozdělení technologií dle generací

Označení Generace	2G	2.5G	2.75G	3G	3.5G	3.75G
Název technologie	CSD, HSCSD	GPRS	EDGE, CDMA 1xRTT	UMTS, CDMA 1xEV-DO	HSPDA	HSUPA
Název mobilní sítě	GSM	GSM	GSM, CDMA2000	UMTS, CDMA2000	UMTS	UMTS

Zdroj: Vlastní zpracování

CSD (Circuit Switched Data) - přenos dat v síti s přepínáním okruhu využívá jeden timeslot k datovému přenosu o rychlosti 9.6 kbit/s do GSM sítě.

HSCSD (High-Speed Circuit-Switched Data) - opět systém založený na přenosu dat s přepojováním okruhu (CSD). Tentokrát ovšem s využitím kódování pro navýšení datové propustnosti, v rámci jednoho timeslotu bylo dosaženo rychlosti 14.4 kbit/s. Umožňuje současné využití až 4 timeslotů, v takovém případě dosahuje nejvyšší rychlost 57.6 kbit/s.

GPRS (General Packet Radio Service) - jak již název napovídá, tentokrát je již použita technologie přepínání paketů. Protože při optimálních podmínkách je možné snížit režii na zajištění přenosu, a při horších podmínkách naopak zvětšit, zavádí GPRS čtyři kódová schémata. CS 1 – CS 4 s rozdílnou užitečnou přenosovou rychlostí. Zařízení jsou dále rozdělena do tříd dle využívané kombinace timeslotů. Dosahovaná rychlost 80 kbsp / 40 kbps.

EDGE (Enhanced Data rates for Global Evolution) - vylepšení systému GPRS, využívá osmistavové fázové modulace (8-PSK), díky které přenáší tři informační bity pomocí jednoho symbolu. Rozšíření EDGE zahrnuje dvě hlavní části:

- EGPRS (Enhanced GPRS) – pro přepojování paketů
- ECSD (Enhanced Circuit Switched Data) – pro přepojování okruhů

Maximální přenosová rychlost činí až 236.8 kbps.

CDMA2000 1xEV-DO / 1xRTT - služba realizována na frekvenci 450 – 2100 MHz. Technologie 1xEV-DO slouží pouze k datovému přenosu o rychlosti až 2.4 Mbps, technologie 1xRTT umožňuje realizovat přenos hlasový i datový, při maximální dosahované rychlosti 307 kbps.

UMTS (Universal Mobile Telecommunication Systém) - mobilní síť 3. generace provozovaná na frekvencích 1885 – 2200 MHz využívá technologie UMTS s přenosem dat

metodou tzv. frekvenčního dělení FDD (Frequency Division Duplex). Rychlost přenosu dat je až 2 Mbps, s technologií HSDPA až 14.4 Mbps. S technologií HSUPA je teoreticky možné dosáhnout rychlosti uploadu až 1.4 Mbps.

Bezdrátové Wi-Fi připojení - bezdrátová komunikace v ISM (Industrial Scientific and Medical) pásmu, podle standardů IEEE 802.11. Neboli v bezlicenčním pásmu pro průmyslové, vědecké a lékařské potřeby 2,4 GHz (2,4–2,485GHz), později 5 GHz (5,1–5,3 a 5,75–5,825 GHz). Vývoj technologie přinesl několik standardů rozvíjejících původní specifikaci 802.11, přehled nejdůležitějších zobrazuje tabulka 3.

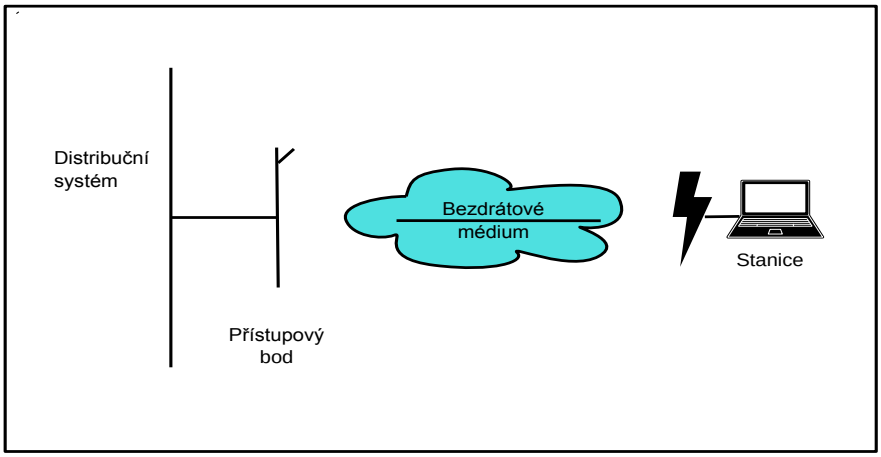
Tabulka 3: Vývoj standardu IEEE 802.11

Standard	Rok vzniku	Pásmo [GHz]	Maximální Rychlost [Mbit/s]
IEEE 802.11	1997	2,4	2
IEEE 802.11a	1999	5	54
IEEE 802.11b	1999	2,4	11
IEEE 802.11g	2003	2,4	54
IEEE 802.11n	2009	2,4 nebo 5	108

Zdroj: Vlastní zpracování

Dosah sítí činí ve venkovním prostředí při použití všesměrové antény od 100–350 m, v budovách od 20–100 m. Pomocí směrové antény lze dosáhnout vzdálenosti až 20 km. Každá Wi-Fi síť, sloužící k připojení na Internet, obsahuje čtyři hlavní komponenty:[8]

- Distribuční systém
- Přístupový bod
- Bezdrátové médium
- Stanice



Obrázek 4: Komponenty Wi-Fi sítě

Zdroj: upraveno podle [16]

[8] Zdroj: [16] Komponenty sítě, strana 5

Distribuční systém - logická komponenta standardu 802.11 používaná k přesměrování datového toku na stanici. V naprosté většině systémů se skládá z bridge a páteřní sítě pro přenášení dat mezi přístupovými body. Bridge, neboli most spojuje dva segmenty sítě, na základě MAC dokáže rozdělit provoz na těchto sítích, komunikace mezi počítači jednoho segmentu probíhá pouze v tomto segmentu a nikoliv v celé síti. Někdy je páteřní síť tvořena Ethernetem, jindy vysokorychlostním bezdrátovým spojem, nebo jejich kombinací.

Přístupový bod (Access point) - zajišťuje komunikaci mezi stanicí a distribučním systémem. AP je pevná stanice s rozhraním do distribučního systému, představuje bridge v komunikaci.

Bezdrátové médium - je nosičem dat při jejich přesunu od stanice ke stanici (AP). Zde je představováno nosnou vlnou radiové frekvence 2.4 GHz respektive 5 GHz.

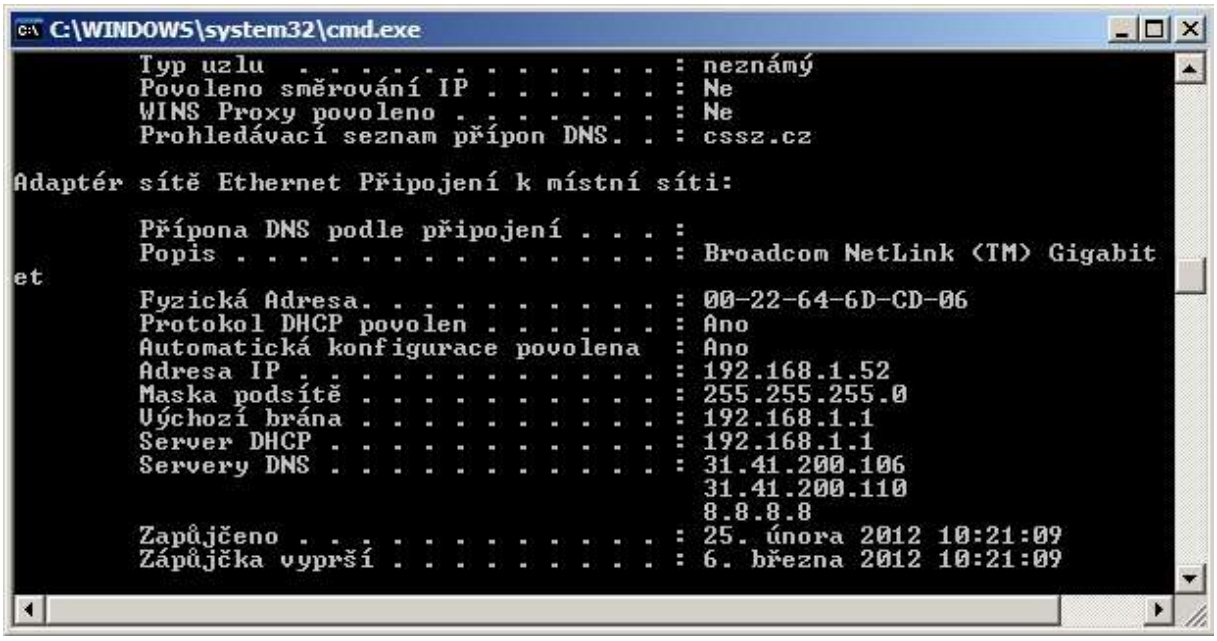
Stanice - jakékoliv zařízení: počítač, notebook, netbook, PDA, telefon s Wi-Fi, ale například i tiskárna.

2. CHARAKTERISTIKA VLASTNÍHO PROSTŘEDÍ

Monitorované připojení je vytvořeno pomocí bezdrátového Wi-Fi routeru, který zabezpečuje připojení pro sedm počítačů ve vnitřní síti. Poskytovatel připojení využívá bezdrátovou technologii v rámci téměř celé infrastruktury distribučního systému. Jelikož je vycházeno z pohledu běžného uživatele, není známa topologie sítě a nelze tedy sestavit schéma.

2.1. Výběr monitorovaných bodů

Uživateli je známa adresa jeho vlastního routeru a adresy DNS serverů. To jsou informace, které jsou snadno zjištěny příkazem ipconfig /all, jak ukazuje obrázek číslo 5.



Obrázek 5: Nastavení sítě v PC

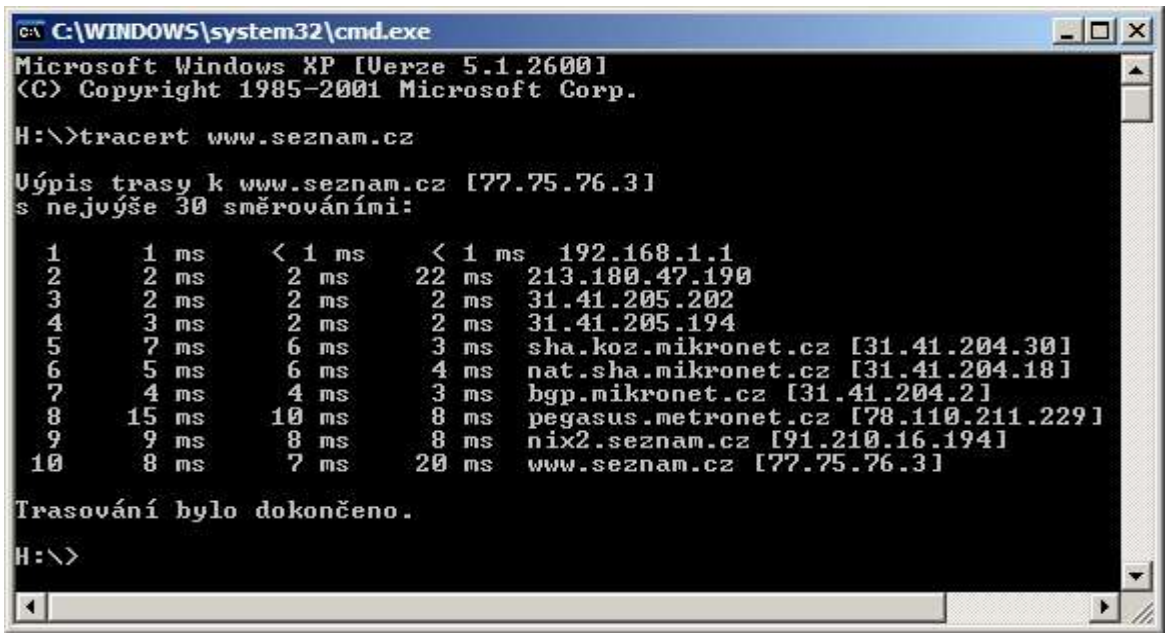
Zdroj: Vlastní zpracování

Tímto jsou určeny tři možné body k monitorování:

- Adresa vlastního routeru 192.168.1.1
- Adresa DNS1 31.41.200.106
- Adresa DNS2 31.41.200.110

Adresy dalších bodů určíme pomocí trasování cesty k libovolné adrese v Internetu. Za tímto účelem je využíván například program traceroute, nebo méně známý pathping. Program traceroute odesílá ze zdrojového počítače na cílový počítač ICMP pakety „Žádost o echo". Namísto odeslání prvního paketu s hodnotou TTL rovnou 255 pošle klient paket

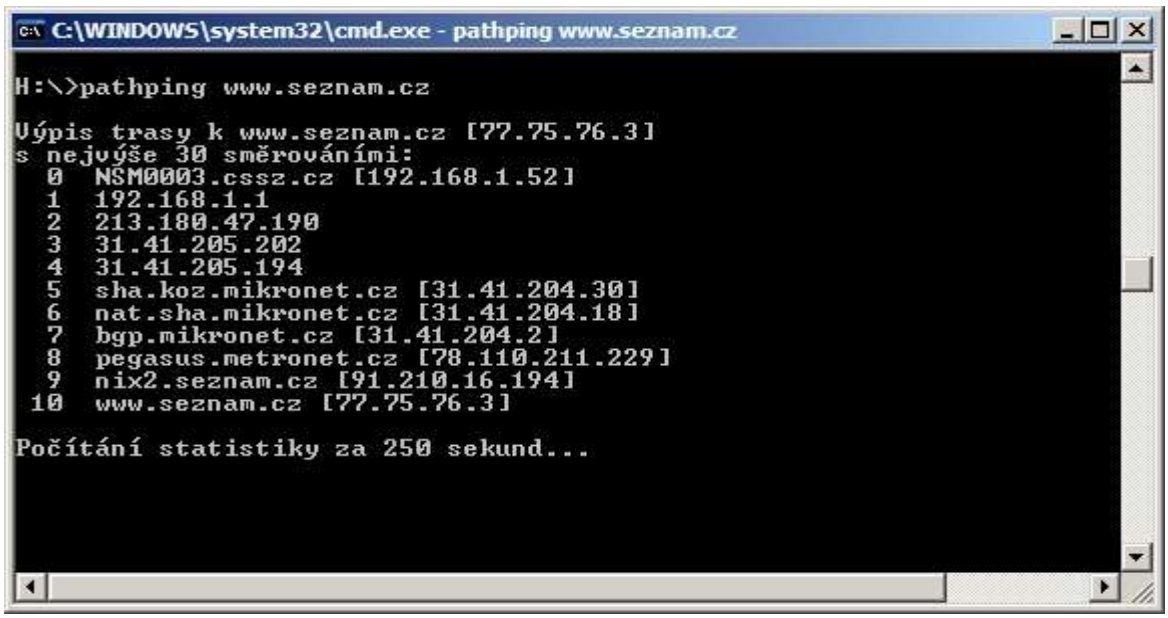
s TTL rovným 1. Jelikož hodnota TTL představuje povolené množství směrování, která paket může podstoupit předtím, než je zahozen, hned první směrovač po cestě sníží hodnotu na nulu a následně paket zahodí a klientovi pošle chybovou zprávu, jejíž součástí je IP adresa. Postupným zvětšováním hodnoty TTL může příkaz traceroute získat zprávu z každého směrovače nebo jiného zařízení, kterým paket musí projít, jak ukazuje obrázek číslo 6.



Obrázek 6: Výstup příkazu traceroute

Zdroj: Vlastní zpracování

Obdobným způsobem pracuje program pathping, který na závěr ještě spočítá celkovou statistiku komunikace, příklad je na obrázku číslo 7.



Obrázek 7: Výstup příkazu pathping

Zdroj: Vlastní zpracování

Příkaz traceroute však na Internetu nemusí správně fungovat, neboť mnoho směrovačů je nastaveno tak, aby ignorovaly jeho datagramy UDP. Alternativně lze využít příkaz tcptraceroute, který vysílá pakety TCP, a nedá se tedy prakticky nijak ignorovat.[9]

Takto jsou určeny další vhodné body k monitoringu:

- Přístupový acespoint 213.180.47.190
- Router_01 31.41.205.202
- Router_02 31.41.205.194
- Router_03 31.41.204.30
- NAT 31.41.204.18
- Router_04 31.41.204.2

Pro úplnost monitorování jsou zvoleny ještě dva servery umístěné v Internetu. Vybrány byly servery známých vyhledávačů, jejichž vysokou dostupnost lze předpokládat, www.seznam.cz a www.google.cz. Pro měření rychlosti stahování a kontrolu stavu systému bude monitorován také vlastní monitorovací systém, localhost. Localhost odkazuje na právě používaný počítač se speciální vyhrazenou IP adresu 127.0.0.1. Konečný výběr bodů k monitoringu uvádí tabulka číslo 4.

Tabulka 4: Vybrané body k monitorování

Monitorovaný systém	Označení v Cacti	Adresa systému
Localhost	Localhost	127.0.0.1
Vlastní router	Vlastni_AP	192.168.1.1
Přístupový acespoint	Pristupove_AP	213.180.47.190
Router_01	Router_01	31.41.205.202
Router_02	Router_02	31.41.205.194
Router_03	Router_03	31.41.204.30
NAT	NAT	31.41.204.18
DNS1	Kozakov_DNS	31.41.200.106
DNS2	Mikroservis_DNS	31.41.200.110
www.seznam.cz	Seznam	www.seznam.cz
www.google.cz	Google	www.google.cz

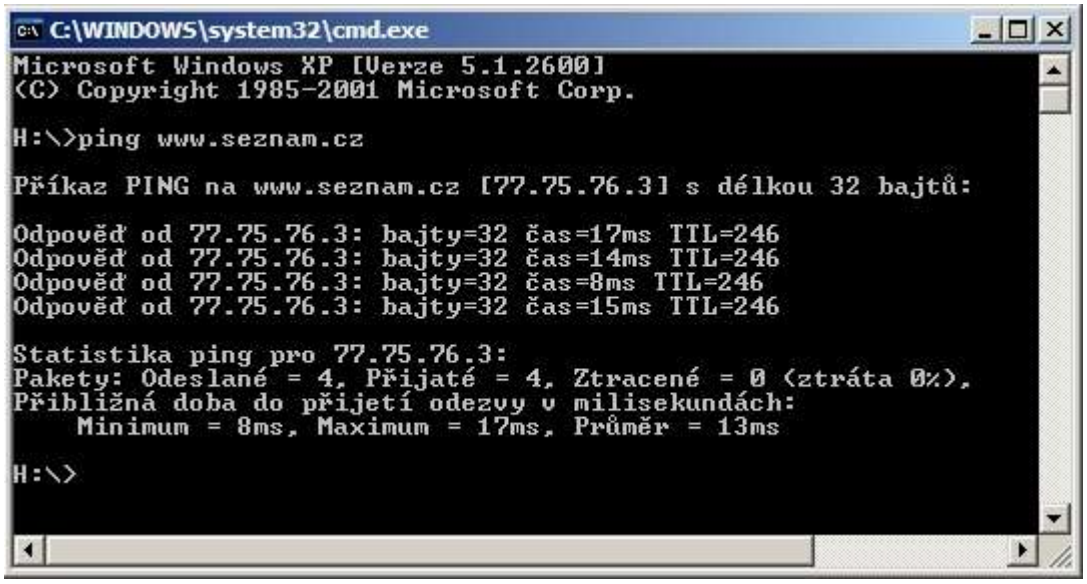
Zdroj: Vlastní zpracování

[9] Zdroj: [14] Používání nástrojů traceroute, tcpf raceroute a mtr pro zjišťování problémů v sítích, strana 518

2.2. Monitorovací nástroje

Jelikož není k dispozici žádný oprávněný přístup k získávání dat z jednotlivých kontrolních bodů pomocí protokolu SNMP, který by byl pro tyto účely nejvhodnější, bude pro monitoring přístupového bodu, převaděčů, DNS a webových serverů využíván protokol ICMP, jmenovitě příkaz ping. Pro měření rychlosti stahování byl využit nástroj wget. Pro uchování dat, vizualizaci a vlastní sledování bude využíván vybraný Open-Source systém implementovaný v operačním systému Linux.

Internet Control Message Protocol (ICMP) - poskytuje chybové zprávy a zpětnou odezvu o provozu sítě.[10] Je používán pro účely řízení, zasílání zpráv a diagnostiku. Protokol je definován v RFC 792 a patří do síťové vrstvy modelu OSI. Pro doručování zpráv využívá protokol IP, typ protokolu v hlavičce IP je u ICMP vždy 1. Typů zpráv ICMP je velmi mnoho, nejběžnější je žádost o echo (echo request). Žádost o echo lze použít jako diagnostický nástroj prověřující existenci spojení mezi koncovými počítači. Příkaz ping využívá zprávy ICMP typu 0 (echo) a 8 (žádost o echo). Je-li spuštěn příkaz ping a zadána adresa či název vzdáleného počítače, je na tento počítač odeslána série zpráv ICMP typu 8 (Žádosti o echo). Cílový počítač na tyto zprávy reaguje zasláním série zpráv ICMP typu 0 (odpověď). Příklad výstupu příkazu ping ukazuje obrázek 8.



Obrázek 8: Výstup příkazu ping

Zdroj: Vlastní zpracování

Wget - volný software pod GNU licencí, díky čemuž je snadno portovatelný do různých operačních systémů a je součástí asi každé linuxové distribuce. Jedná se o neinteraktivní

[10] Zdroj: [6] Internet Control Message Protocol, strana 97

utilitu příkazového řádku s širokými možnostmi nastavení, lehce použitelnou samostatně nebo jako součást komplexních skriptů. Nejdůležitější vlastnosti wget:

- Stahuje odkazy uvedené v souboru s jejich seznamem
- Navazuje přerušená stahování
- Lze používat zástupné znaky a rekurzivní stahování do určené hloubky
- Podporuje proxy servery
- Podporuje cookies
- Podporuje persistentní http připojení
- Lze spustit na pozadí
- Při mirroringu využívá časová razítka lokálních souborů

2.3. Nejpoužívanější Open-Source monitorovací systémy

Prostřednictvím Internetu lze nalézt různé typy volně dostupného monitorovacího software uvolněného pod některou z Open-Source licencí. Vyznačují se různými možnostmi monitoringu, rozdílnou robustností a rozšířeností využívání. Přičemž platí, že čím je systém více rozšířen, tím více je komunitou podporován a lze snadněji nalézt, nebo vytvořit implementaci požadovaného systému.

Cacti

Cacti je Open-Source nástroj pro monitorování zařízení v síti.[11] Získané údaje ukládá v databázi a do souborů, zprostředkovává jejich zobrazení v podobě přehledných grafů. Systém je velice univerzální a umožňuje sledovat obrovskou škálu zařízení. Komunita uživatelů okolo systému Cacti vytváří nejrůznější moduly a šablony pro další snadné využití. Cacti je vytvořen pomocí jazyka PHP a pro vlastní měření a grafické výstupy využívá další Open-Source nástroj RRD-Tool, dá se říci že Cacti je frontend pro RRD-Tool. Převážnou většinu údajů získává pomocí protokolu SNMP (Simple Network Management Protocol), ale umožňuje využívat například ping pro sledování dostupnosti, nebo další vlastní skripty, vytvořené v Perlu nebo pomocí shellu, jejichž prostřednictvím získává informace. Ke svému běhu potřebuje PHP, MySQL, RRD tool, Net-SNMP a web server, například Apache. Systém lze nalézt na stránce http://www.cacti.net/.

[11] Zdroj: [10] What is Cacti?, strana 6

MRTG

Multi Router Traffic Grapher, získává data ze směrovačů a dalšího síťového hardwaru prostřednictvím protokolu SNMP. Každých pět minut vysílá SNMP dotazy a výsledky ukládá ve specializovaném datovém formátu. Díky tomuto formátu dokáže MRTG zobrazovat denní, týdenní, měsíční a roční grafy, aniž by velikost datových souborů donekonečna narůstala. Podle potřeby totiž starší data sumarizuje. Samotné grafy jsou generovány ve formátu PNG (Portable Network Graphics) a lze je zobrazovat na webových stránkách, nebo použít v jiných aplikacích.[12] Umožňuje pro svoji činnost využívat RRD-Tool. Ve srovnání s Cacti lze však považovat za předešlý krok ve vývoji monitorovacích nástrojů. Dokumentaci a instalaci lze nalézt na http://oss.oetiker.ch/mrtg/

Nagios

Nagios je výkonný monitorovací systém, který umožňuje organizacím identifikovat a řešit problémy IT infrastruktury dříve, než ovlivní kritické obchodní procesy.[13] Nagios kontroluje, zda host nebo služba pracuje správně a uloží jeho stav. Aby bylo možné odhalovat náhodné a dočasné problémy, Nagios používá takzvané měkké a tvrdé stavy, pro určení, co současný stav hostitele nebo služby znamená. V případě výpadku některé z monitorovaných služeb umí systém poslat varování správcům systému, či provést jiné definované akce, například restartovat problémovou službu nebo zařízení. Pro své grafické výstupy rovněž umožňuje využít RRD-Tool. Je poměrně složitě konfigurovatelný. Stránky projektu lze nalézt na adrese http://www.nagios.org/

Zabbix

Zabbix poskytuje mnoho způsobů, jak sledovat různé aspekty IT infrastruktury a opravdu může monitorovat téměř cokoliv. Lze charakterizovat jako semidistribuovaný monitorovací systém s centralizovaným řízením. Přestože většina instalací využívá jednu centrální databázi, je možné použít distribuované monitorování s uzly a proxy servery a většina instalací pak používá Zabbix agenty.[14] Vlastní stažení či zakoupení placené podpory lze nalézt na http://www.zabbix.com/

Zenoss

Zenoss Core je Open-Source síťový monitorovací systém sponzorovaný Zenoss Inc, která vyvíjí dvě verze: Core a Enterprise. Verze Core náleží komunitě a je komunitou podporována. Umožňuje monitorovat celou IT infrastrukturu, nejen sítě, ale také servery, virtuální servery

[12] Zdroj: [9] Seznámení s programem MRTG, strana 48
[13] Zdroj: [11]
[14] Zdroj: [12] Zabbix features and architecture, strana 9

a různé aplikace. Zenoss Core je monitorovací řešení, které může být nakonfigurováno od jednoduchého systému po velmi komplexní strukturu. Umožnuje využívat pluginy Nagios a Cacti. Má poměrně komplikované rozhraní.[15] http://www.zenoss.com/

[15] Zdroj: [1] Network and System Monitoring with Zenoss Core, strana 7

3. INSTALACE MONITOROVACÍHO SYSTÉMU

Pro vlastní monitoring byl zvolen Cacti, protože tento software umožňuje provádět monitoring dle zadání, je volně šiřitelný, zároveň je velmi rozšířený a jeho podpora ze strany uživatelů ve formě různých doplňků a šablon je značná. Po zvážení možností hardware, viz tabulka číslo 5 a při dodržení minimálních pořizovacích nákladů, byla zvolena specializovaná distribuce operačního systému Linux CactiEZ, který lze nalézt na adrese http://cactiez.cactiusers.org/.

Tabulka 5: Hardware monitorovacího PC

Fujitsu Siemens scovery xs 1215	
CPU	Intel Celeron 900MHz
RAM	512 MB
HDD	20 GB

Zdroj: Vlastní zpracování

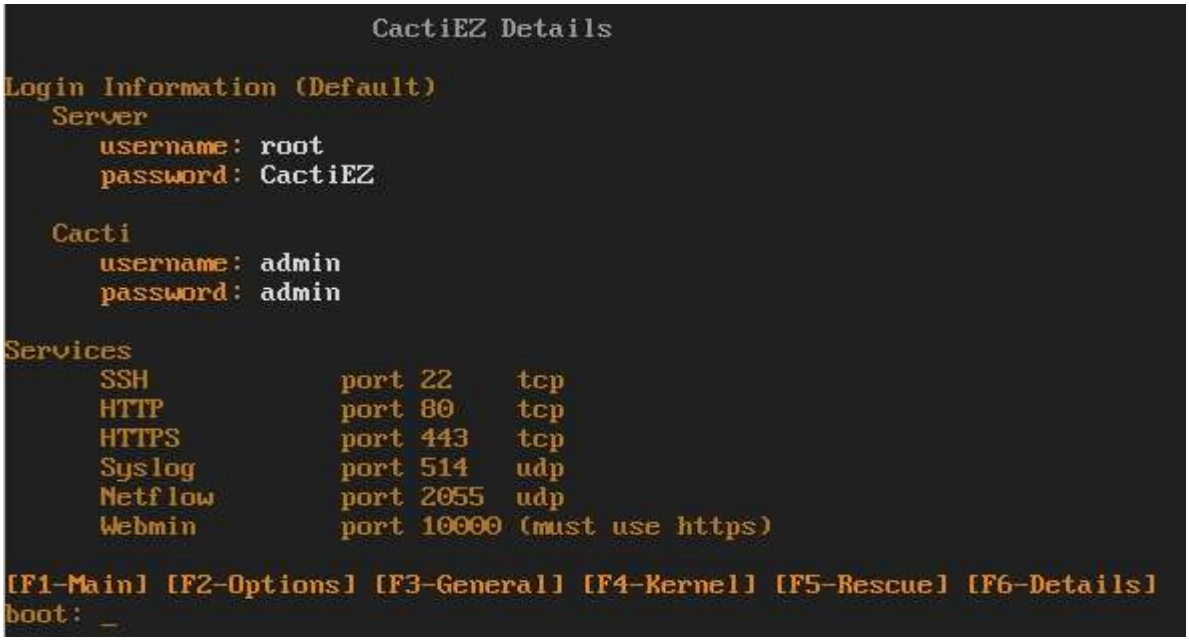
3.1. Instalace operačního systému

Jedná se o samoinstalační linuxovou distribuci, založenou na Linuxové distribuci CentOS, která nastavuje a konfiguruje upravenou instalaci Cacti. Vše je nastaveno zcela automaticky a pracuje ihned po instalaci systému. Pojem samoinstalační je nutno chápat doslovně, po startu PC z instalačního CD dojde k instalaci systému bez jediného dotazu na konfiguraci. Včetně konfigurace diskového prostoru. Na tuto skutečnost CactiEZ upozorňuje na první instalační obrazovce, jak lze vidět na obrázku číslo 9.

Obrázek 9: Úvodní instalační obrazovka CactiEZ

Zdroj: Vlastní zpracování

Zajímavou volbu hned na první obrazovce představuje klávesa F6, po jejím stisknutí jsou zobrazena uživatelská jména a příslušná hesla, použitá jako výchozí poté, co dojde k instalaci systému. Zároveň jsou zobrazeny služby a jejich porty, které v nainstalovaném systému nalezneme po prvním startu spuštěné a funkční tak, jak ukazuje obrázek číslo 10.



Obrázek 10: Volba F6 – informace o službách a heslech

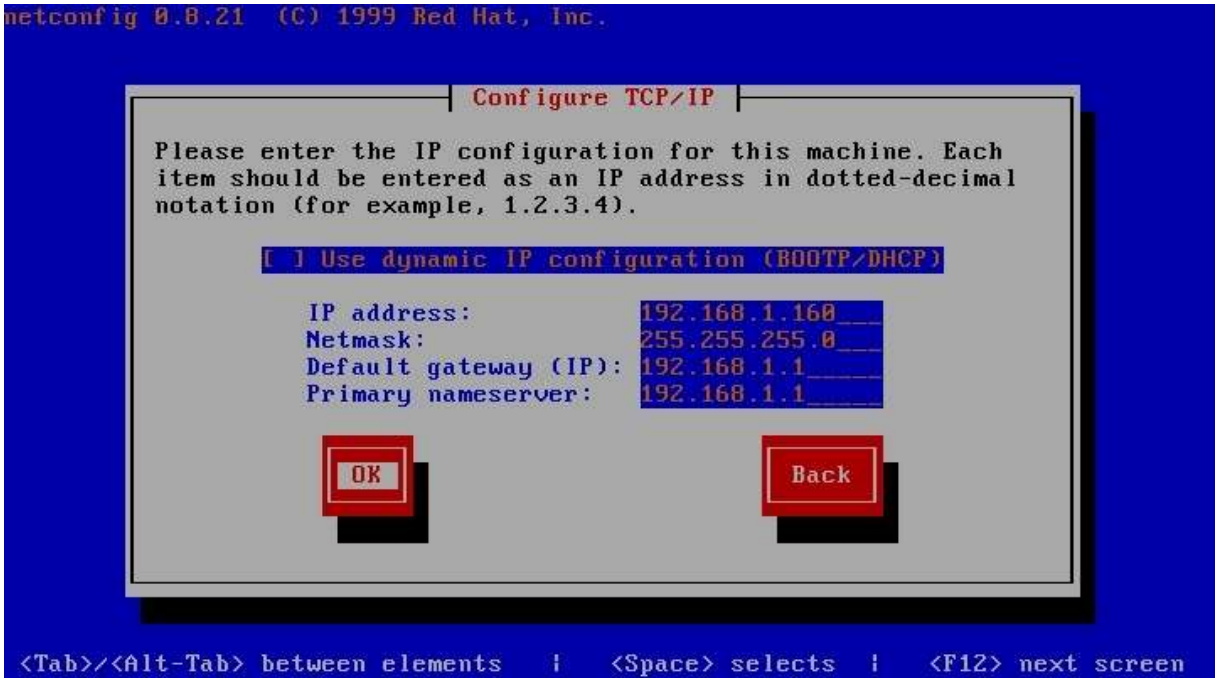
Zdroj: Vlastní zpracování

Po zformátování souborového systému dojde k instalaci všech balíčků tvořících distribuci CactiEZ, průběh instlace je celou dobu zobrazován, příklad na obrázku číslo 11.

Obrázek 11: Průběh instalace systému CactiEZ

Zdroj: Vlastní zpracování

Na závěr instalace proběhne restart systému, při prvním spuštění nastaví nástroj Kudzu nově detekovaný hardware. Před vlastním používáním je nutné změnit hesla do operačního systému a systému Cacti. Poté provést nastavení nové IP adresy, protože používat na systému ve funkci serveru adresu přidělovanou pomocí DHCP není rozumné, pokud není provedena rezervace této adresy pro MAC adresu monitorovacího PC. Změnu lze provést příkazem *netconfig*, jehož uživatelské rozhraní je velmi snadno použitelné jak ukazuje obrázek číslo 12.



Obrázek 12: Rozhraní nástroje netconfig

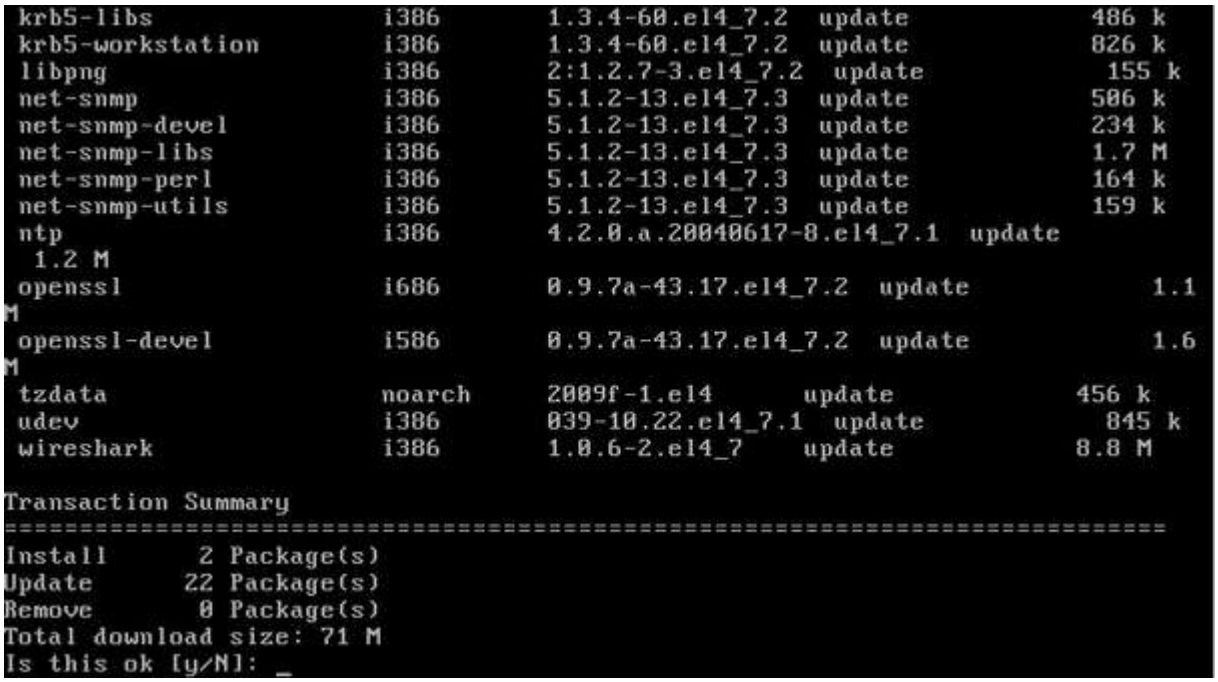
Zdroj: Vlastní zpracování

Poté příkazem: *service network restart* dojde k nastavení sítě dle nové konfigurace. Následuje aktualizace systému. Bohužel aktualizační balíky Centos 4.7, na kterém je CactiEZ verze 0.6 postaven, jsou přesunuty na novou adresu. Před vlastní aktualizací je třeba přenastavit cesty k repozitáři v souboru /etc/yum.repos.d/CentOS-Base.repo takto:[16]

```
[base]
name=CentOS-$releasever - Base
baseurl=http://vault.centos.org/4.7/os/$basearch/
gpgcheck=1
gpgkey=http://mirror.centos.org/centos/RPM-GPG-KEY-centos4
priority=1
protect=1
enabled=1
```

[16] Zdroj: [1] CactiEZ 0.6 yum troubles

Ve všech sekcích je nutné nastavit cestu na: baseurl=http://vault.centos.org/4.7/ …….. , poté již lze spustit příkaz *yum update* a odsouhlasit následnou instalaci nalezených aktualizací, jak ukazuje obrázek číslo 13.



Obrázek 13: Aktualizace systému

Zdroj: Vlastní zpracování

Po provedeném restartu systému příkazem *init 6*, může započít nastavení systému Cacti pro monitoring sítě. Pro snadnější manipulaci se soubory lze případně ještě provést instalaci souborového commanderu „Midnight Commander“, příkazem *yum install mc.*

3.2. Cacti a jeho použití

Činnost Cacti je rozdělena do tří odlišných oblastí:[17]

- Sběr dat
- Ukládání dat
- Prezentace dat

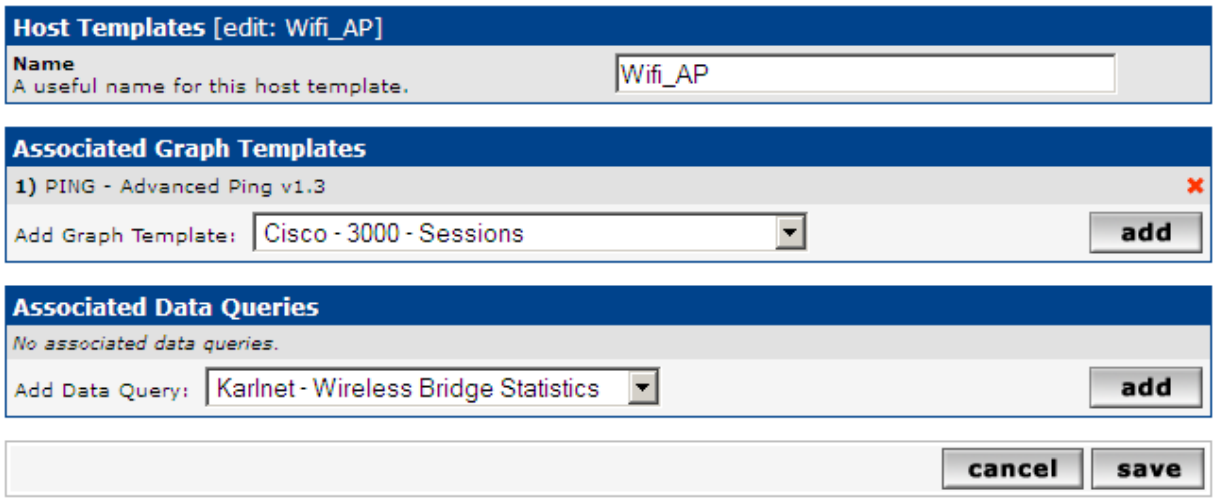
Pro sběr dat z monitorovaných zařízení slouží poller, který je spouštěn v pravidelných intervalech. Zde jsou k dispozici dvě možnosti skript cmd.php nebo zkompilovaný binární poller spine. Druhý jmenovaný je vhodný pro vyšší zátěž, sám také méně zatěžuje systém, proto je vhodný též pro méně výkonná zařízení. Poller získává data prostřednictvím

[17] Zdroj: [10] Cacti operation, strana 7

standartních nástrojů PHP, nebo pomocí pluginů. Hlavní data jsou uložena pomocí RRDTool do kompaktních souborů o pěvně dané velikosti, další data se ukládají do SQL databáze. K vlastnímu zobrazení grafů slouží RRDTool. Důležité je, že je zobrazena i historie provozu, snadno lze sledovat zatížení sítě v čase a odhalit různé anomálie. Na základě okamžitých hodnot lze jen těžko říci, zda se síť chová normálně. Má-li být zařízení v Cacti sledováno, je nutno provést několik kroků pro jeho vložení:

- zadat zařízení (Devices), které bude monitorováno
- vytvořit zdroj dat Data Source z datového zdroje
- vytvořit graf v Graph Management

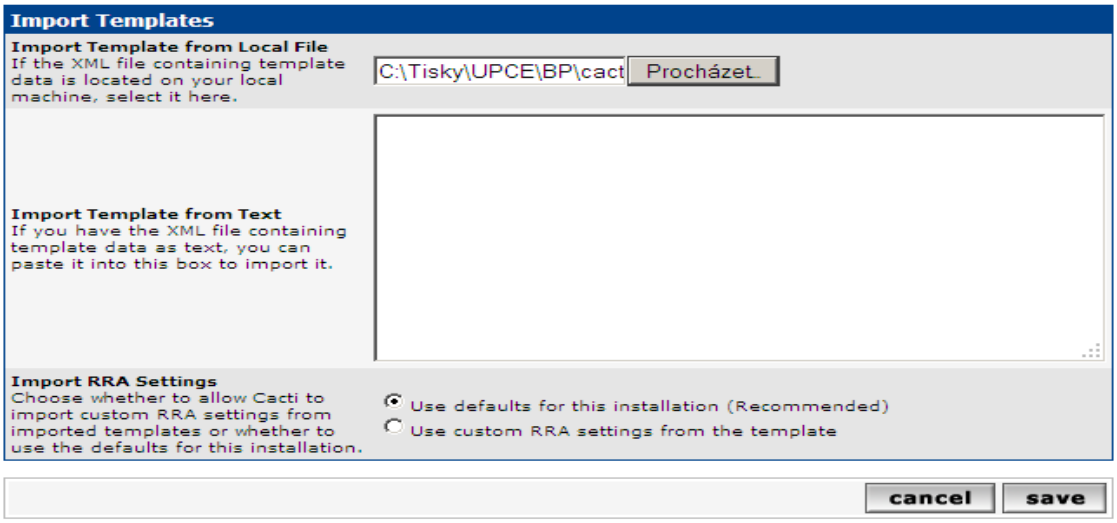
Zařízení je vloženo ručně, poté co je mu přiřazena šablona hosta (Host Template), budou se k danému zařízení nabízet vybrané šablony pro grafy (Graph Template) a dotazy (Data Queries). Šablona grafu je automaticky zřetězena s datovou šablonou (Data Templates) a vytváří zdroj dat. Lze využít šablony, které jsou součástí instalace, nebo vytvořit vlastní, jak ukazuje obrázek číslo 14, kdy je s hostem *Wifi_AP* asociována šablona grafu *Advanced Ping*.



Obrázek 14: Vytvoření šablony hosta

Zdroj: Vlastní zpracování

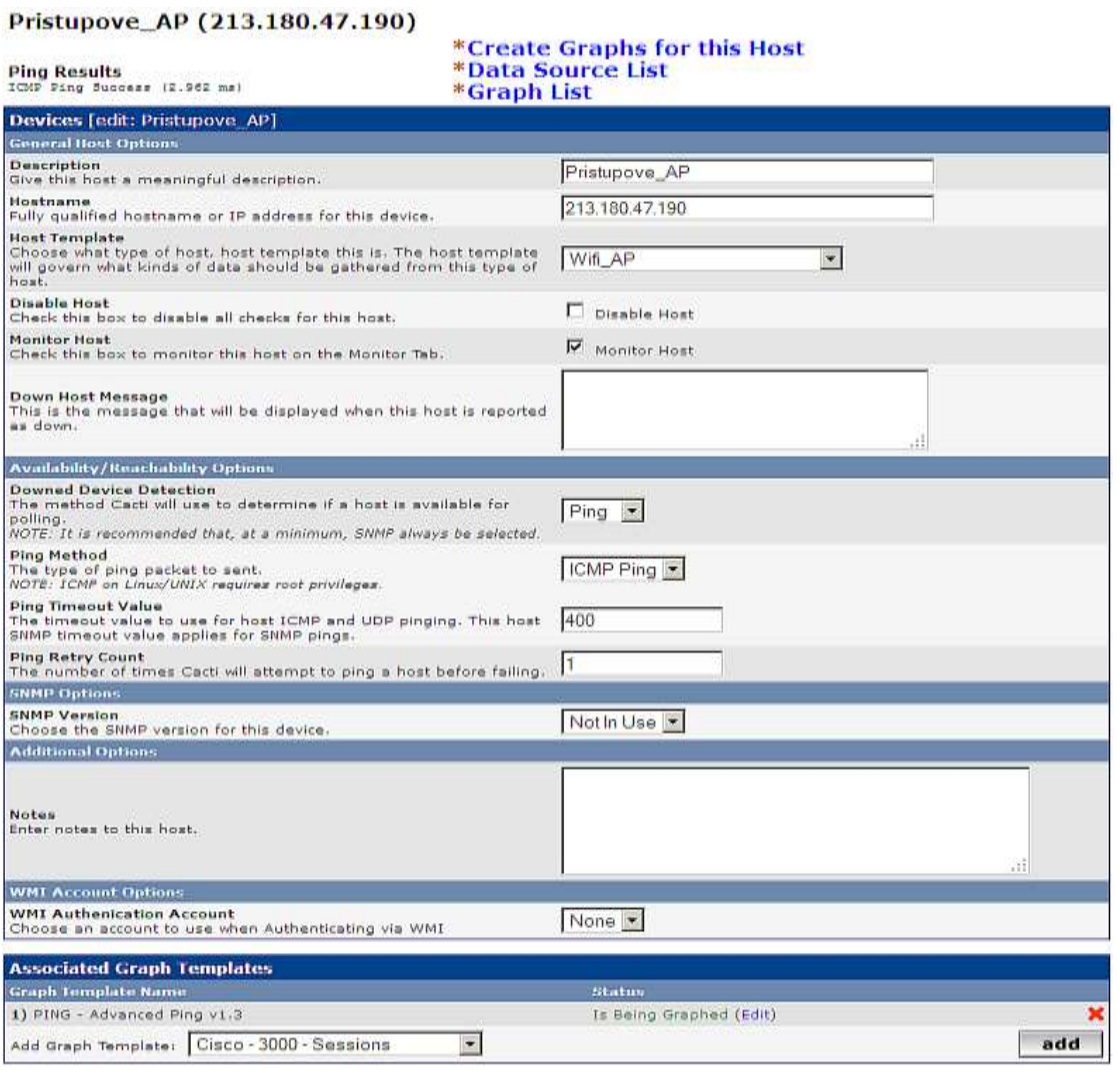
Vytvořená šablona hosta *Wifi_AP* je následně využita v novém zařízení *Pristupove_AP*. Vložené zařízení bude tedy monitorováno pomocí ICMP ping a graf vytvořen pomocí šablony *Advanced Ping Template*. Informace o šabloně a její stažení lze nalézt na stránce http://forums.cacti.net/about10049.html. Šablonu lze do systému snadno doinstalovat pomocí volby „ImportTemplates“, stačí ji rozbalit na PC, ze kterého je systém Cacti spravován a naimportovat jak lze vidět na obrázku číslo 15.



Obrázek 15: Importování šablony do Cacti

Zdroj: Vlastní zpracování

Příklad vytvoření nového zařízení *Pristupove_AP* ukazuje obrázek číslo 16.



Obrázek 16: Vložení nového zařízení

Zdroj: Vlastní zpracování

Popis polí Device

Každé přidávané zařízení je definováno pomocí různých atributů a hodnot. Následující tabulka charakterizuje jednotlivé atributy, které je dobré znát před vložením zařízení do Cacti.:

Tabulka 6: Vybrané atributy „Device“

Název pole	Popis
Description	Smysluplný název hosta. Tento název je zobrazován v prvním sloupci na panelu Devices
Hostname	Plné doménové jméno (Fully qualified hostname) nebo IP adresa. Je-li použito doménové jméno, musí být funkční DNS
Host Template	Host template je zodpovědný za typy dat, které je třeba získat z určitého druhu hostitele.
Disable Host	Zaškrtnutí vypíná monitoring tohoto zařízení.
Monitor Host	Po zaškrtnutí je zařízení zobrazeno v záložce „*monitor*“
Down Host Message	Zpráva, která se zobrazí, je-li zařízení mimo provoz
Downed Device Detection	NONE: vypíná detekci nedostupných zařízení Ping and SMNP: provádí oba testy SNMP: provádí SNMP kontrolu Ping: využívá příkaz *ping*
Ping Method	ICMP Ping: provádí ICMP ping (na linuxu vyžaduje root oprávnění) TCP Ping: provádí TCP test UDP Ping: provádí UDP test
Ping Timeout Value	Definuje čas, po jehož uplynutí test skončí chybou
Ping Retry Count	Definuje, kolikrát se Cacti pokusí provést ping, než ohlásí chybu
SNMP Version	Verze SNMP (nebude využíváno)
Notes	Cokoliv co blíže specifikuje hosta
WMI Authenication Account	Účet, který je využíván při monitoringu Windows zařízení, přes rozhraní ***Windows Management Interface (WMI)***[18]
Add Graph Template	Vybírá šablonu grafu
Add Data Query	Přidá dotaz na data

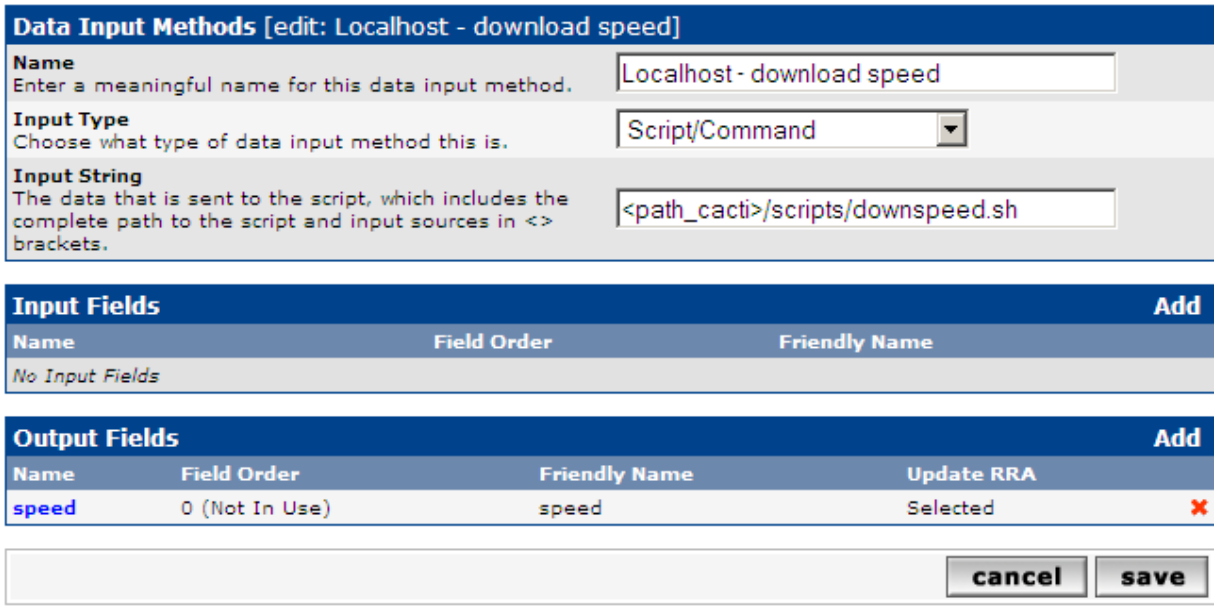
Zdroj: Vlastní zpracování

[18] Zdroj: [15] Windows monitoring, strana 150

Po vložení je zařízení připraveno k použití a může být monitorováno. Tento postup je následně využit pro vložení všech monitorovaných bodů. O něco složitější je situace v případě sledování rychlosti stahování, využívající nástroj *wget*. Pro tento účel jsem vytvořil vlastní stahovací skript, který slouží zároveň jako zdroj dat. Za tímto účelem je na server v Internetu umístěn soubor o velikosti 100 kB, soubor je šifrován a komprimován, aby nebyl jeho přenos ovlivněn případnou komprimací během stahování. Rychlost stahování vypočítá samotný *wget*. Nelze však zapomenout, že stahovaná data jsou v případě existence měsíčního limitu objemu stahovaných dat ze strany poskytovatele Internetu také započítávána. Následující skript je spouštěn v pětiminutových intervalech.

```
#!/bin/sh
wget http://www.superkoralky.cz/rss/100K.zip -o wget.log -O /dev/null;
cat wget.log | grep saved | awk '{printf $2}' | cut -c2-
```

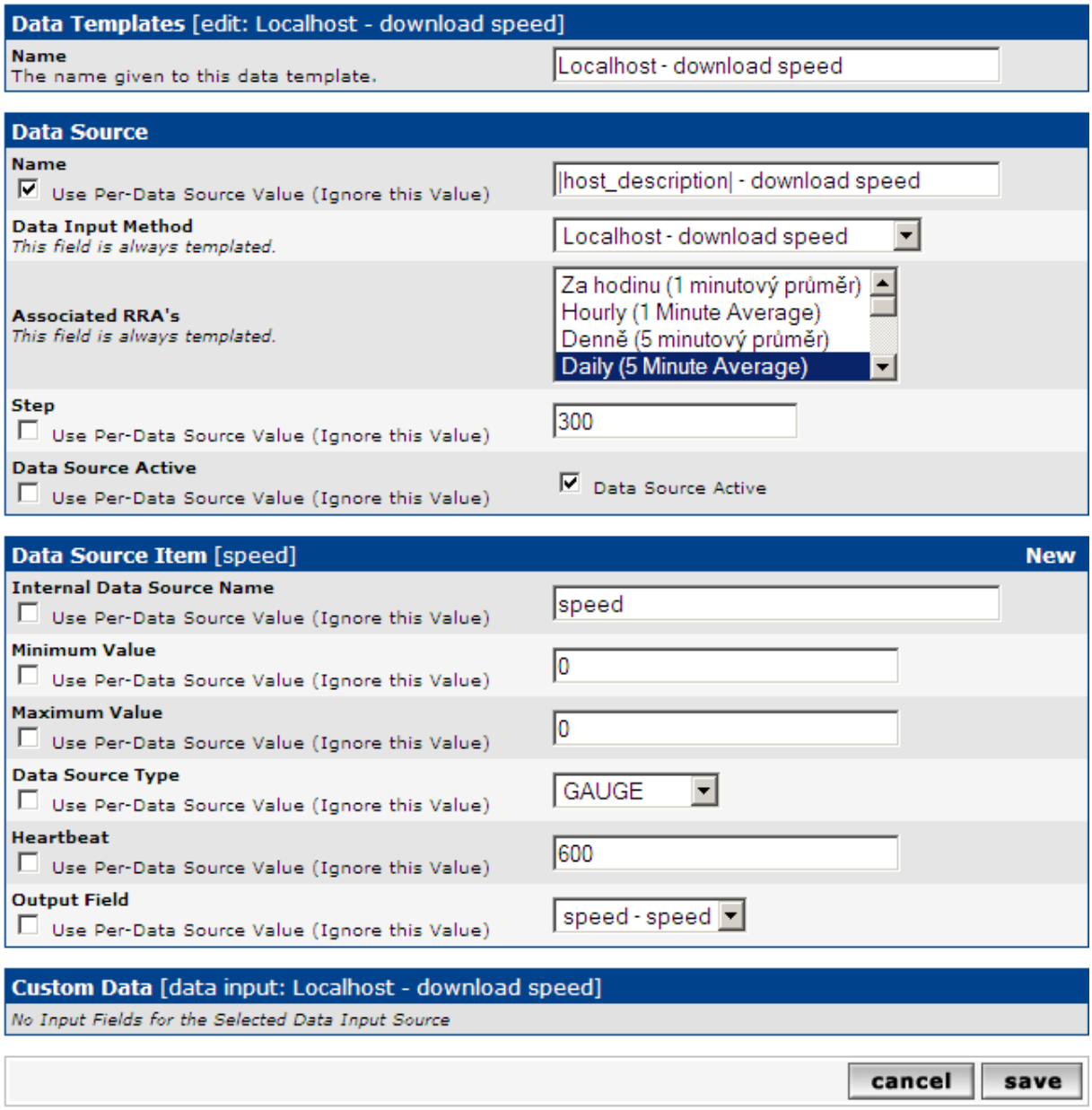
Soubor je nejprve stažen a uložen do /dev/null, protokol o stažení je zapsán do pomocného souboru wget.log, z něhož je následně kombinací příkazů a nástrojů „cat, grep, awk a cut“ vybrána hodnota rychlosti stahování. Hodnota je výstupem skriptu a je přebírána systémem Cacti pomocí vstupní datové metody (Data Input Method), jejíž vytvoření ukazuje obrázek 17.



Obrázek 17: Vytvoření nové vstupní metody

Zdroj: Vlastní zpracování

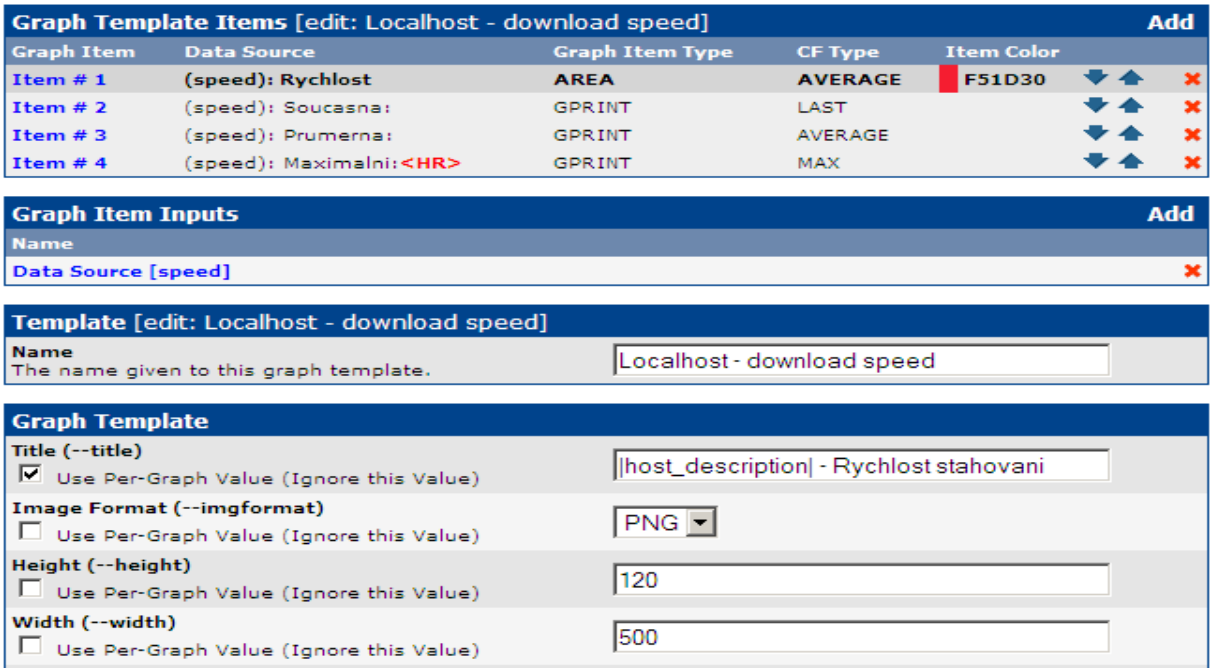
Vstupní metoda je následně využita v datové šabloně, obrázek 18.



Obrázek 18: Vytvoření datové šablony pro rychlost stahování

Zdroj: Vlastní zpracování

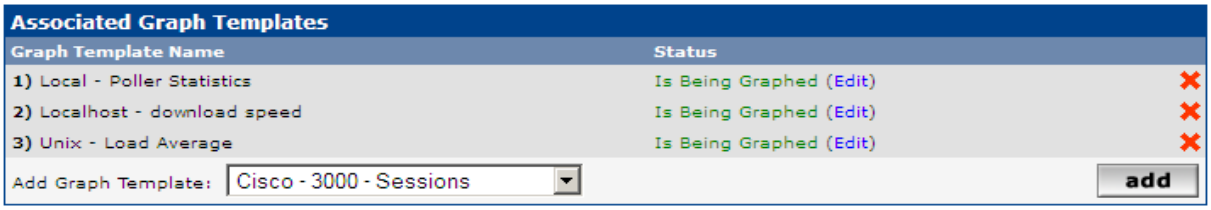
Zdroj dat „speed“ je využit v šabloně grafu dle obrázku 19.



Obrázek 19: Vytvoření šablony grafu pro rychlost stahování

Zdroj: Vlastní zpracování

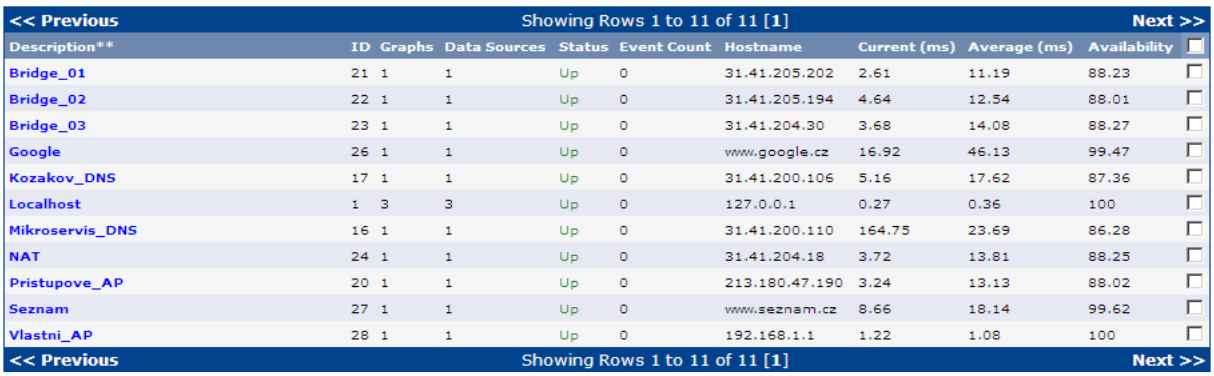
Tato šablona je následně obvyklým způsobem využita v novém zařízení *Localhost*, které sdružuje více sledovaných veličin nastavených dle obrázku 19. Detailní popis spuštění vykreslování grafických výstupů je uveden v příloze A.



Obrázek 20: Vytvoření Graph Template

Zdroj: Vlastní zpracování

Po vložení všech monitorovaných bodů vypadá tabulka zařízení následně:



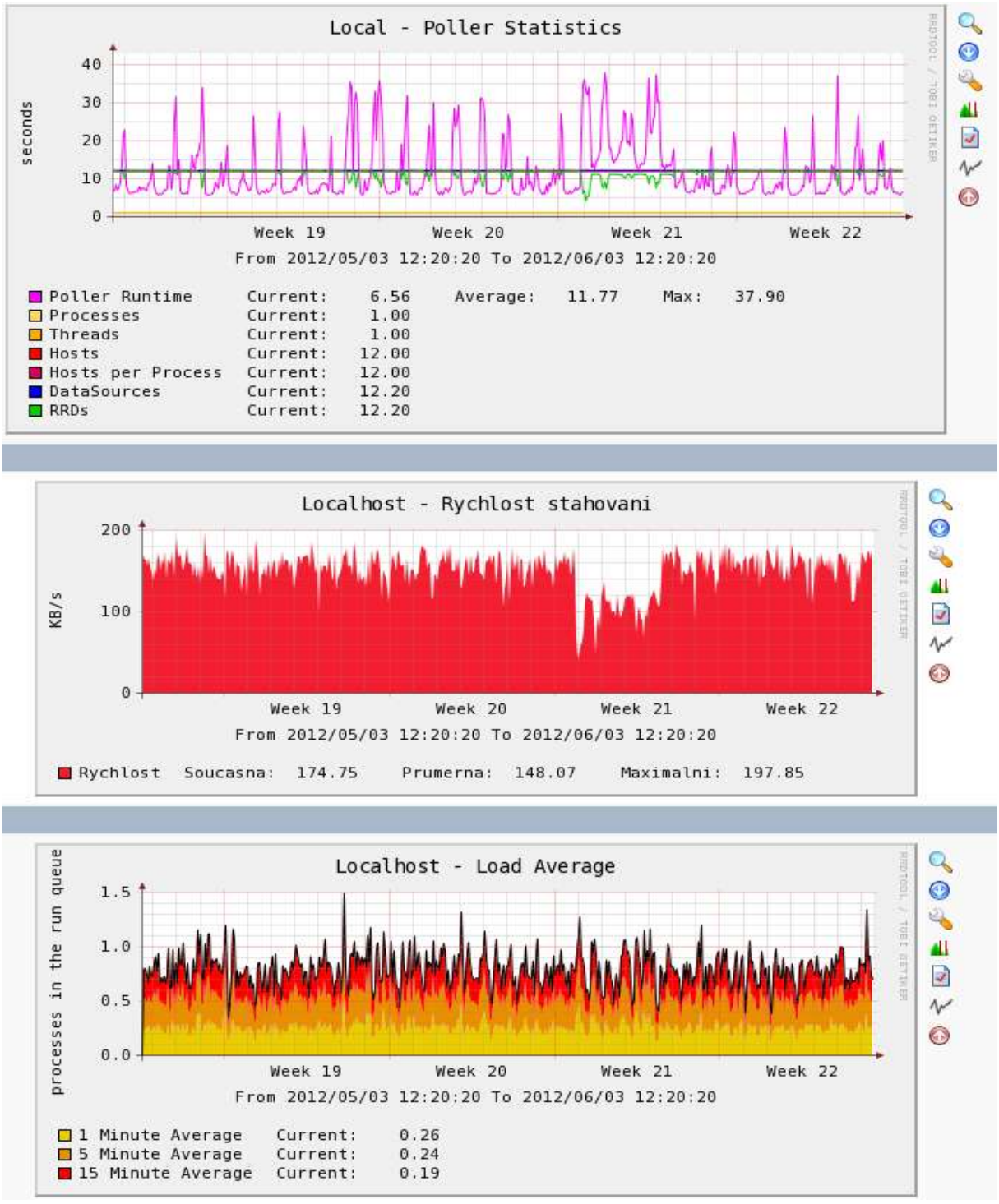
Obrázek 21: Seznam všech monitorovaných bodů

Zdroj: Vlastní zpracování

4. MONITORING SÍTĚ A RYCHLOSTI STAHOVÁNÍ

4.1. Monitorování localhost

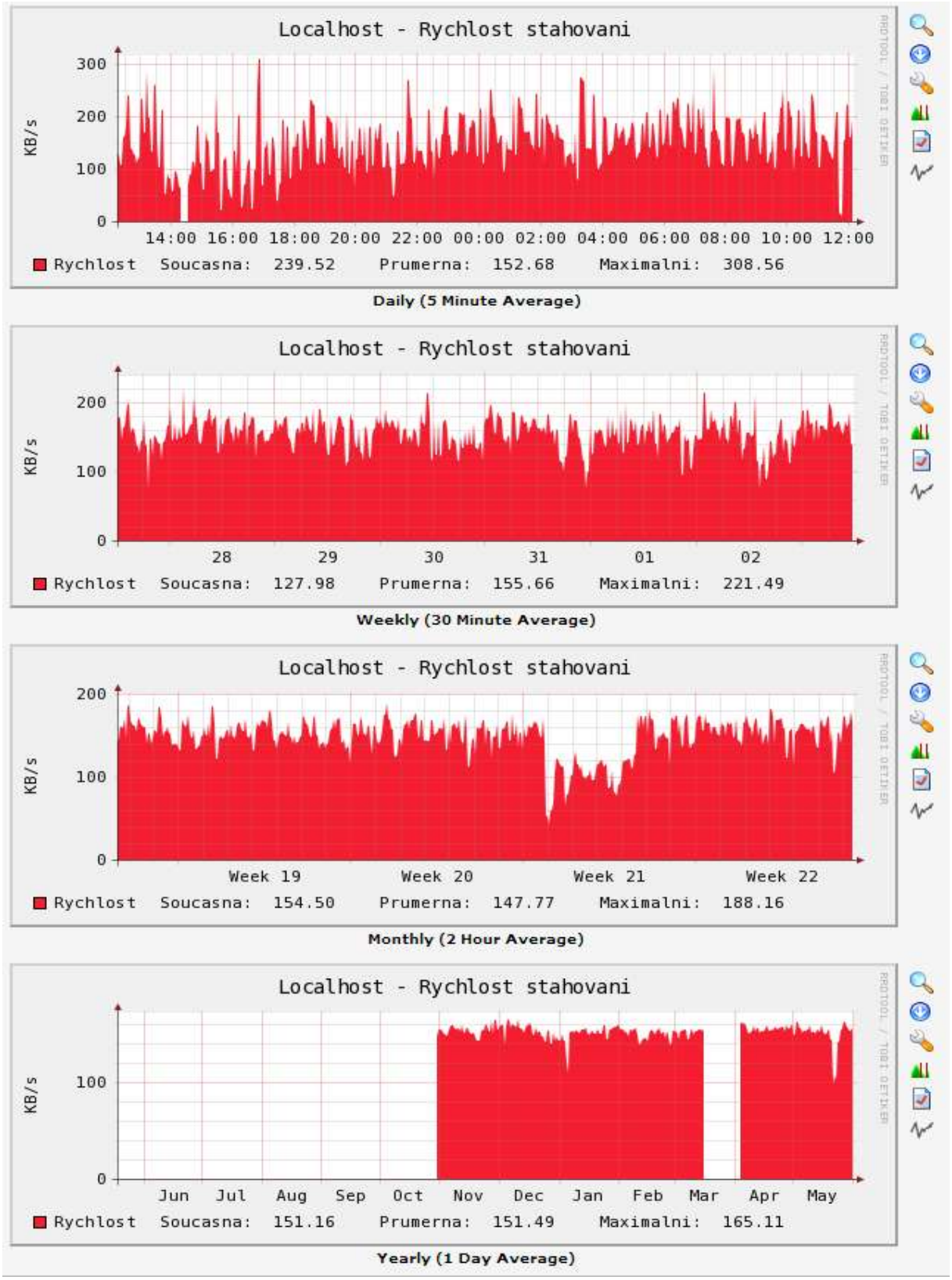
Na vlastním monitorovacím PC probíhá sledování celkového vytížení PC, vytížení poller a měření rychlosti stahování. Měsíční výstupy jsou zobrazeny na následujícím obrázku číslo 22.



Obrázek 22: Localhost Leden 2012

Zdroj: Vlastní zpracování

Rychlost stahování v kompletním přehledu zobrazení, ve kterém lze vidět aktuální zobrazený den, týdenní přehled, měsíční přehled a roční přehled. Na obrázku je zachycen několikatýdenní výpadek z důvodu nefunkčnosti hardware, kdy byl systém vypnut.



Obrázek 23: Kompletní přehled rychlosti stahování

Zdroj: Vlastní zpracování

Na vybraných datech za měsíc listopad 2011 (částečně říjen i prosinec, tak aby mohlo být použito pět kompletních týdnů) byl proveden test, zda spolu nějak souvisí den v týdnu a rychlost stahování, zároveň bylo otestováno, zda nějak souvisí maximální dosažená hodnota s průměrnou denní hodnotou v tabulce číslo 7.

Tabulka 7: Rychlost stahování

Den v týdnu [1-7]	Průměrná rychlost [KB/s]	Max. rychlost [KB/s]
1	153,43	201,6
2	154	196,06
3	151,24	190,99
4	150,83	193,81
5	147,46	186,22
6	151,36	203,81
7	158,3	205,23
1	157,42	200,91
2	156,12	208,77
3	154,45	193,55
4	153,81	200,8
5	151,72	201,28
6	159,27	211,77
7	151,24	197,83
1	155,79	203,55
2	153,43	211,58
3	150,5	204,6
4	149,42	194,76
5	149,34	200,68
6	147,36	212,59
7	141,81	207,75
1	143,41	196,08
2	153,15	208,48
3	152,97	200,95
4	157,38	199,32
5	158,77	221,75
6	152,78	197,72
7	160,84	212,44
1	150,96	201,24
2	162,26	205,94
3	154,23	202,13
4	154,58	190,75
5	157,92	190,98
6	159,08	212,47
7	138,55	190

Zdroj: Vlastní zpracování

Provedená korelační analýza ukazuje, že není žádný vztah mezi dnem v týdnu a sledovanými veličinami, ani mezi sledovanými veličinami navzájem, jak dokládá tabulka číslo 8.

Tabulka 8: Korelační matice

X	*Den v týdnu*	*Průměrná rychlost*	*Max. rychlost*
Den v týdnu	1		
Průměrná rychlost	-0,131985735	1	
Max. rychlost	0,097564652	0,4007168	1

Zdroj: Vlastní zpracování

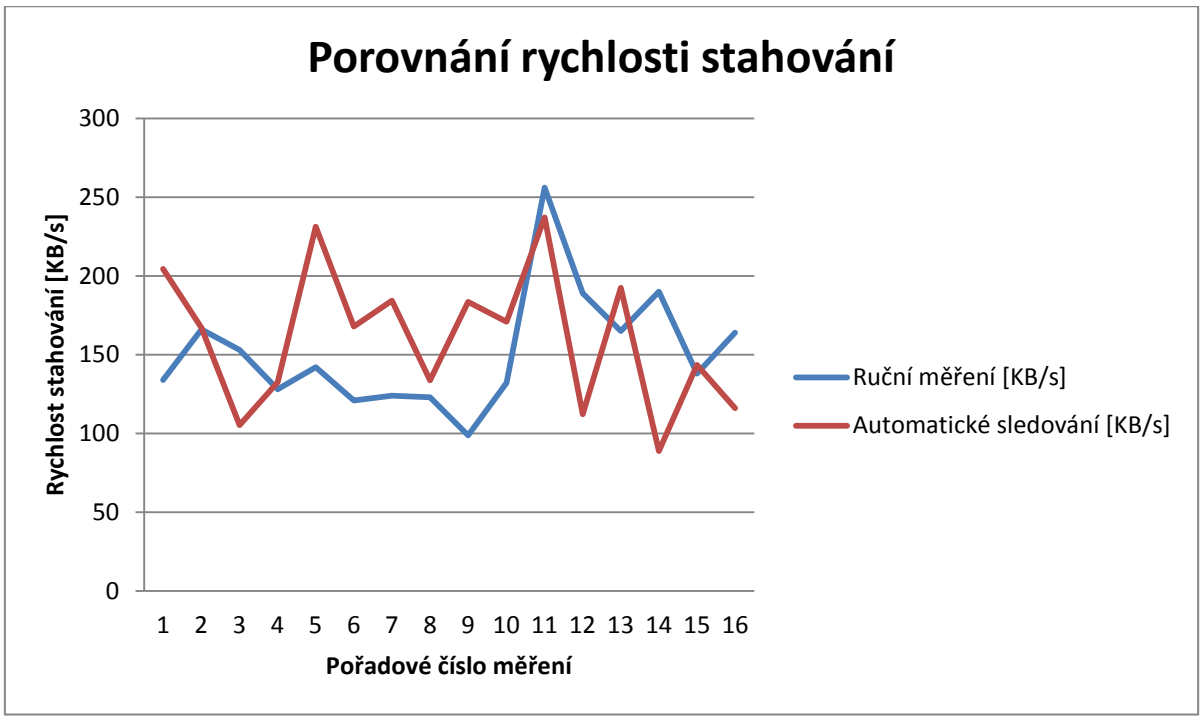
Porovnání automatického měření rychlosti stahování s ručním bylo prováděno stahováním identického souboru přibližně v pětiminutových intervalech, rychlost stažení byla zaznamenána do tabulky. Pro porovnání byla vyexportována data z monitorovacího PC ve formátu csv a porovnána s daty ze stejného časového intervalu. Porovnávaná data uvádí tabulka číslo 9.

Tabulka 9: Data ručního a automatického měření

Měření	Ruční měření [KB/s]	Automatické sledování [KB/s]
1	134	204,5
2	166	167,1
3	153	105,2
4	128	132,5
5	142	231,2
6	121	167,8
7	124	184,3
8	123	133,8
9	98,7	183,4
10	132	171,0
11	256	237,2
12	189	112,2
13	165	192,4
14	190	88,7
15	138	143,4
16	164	116,1

Zdroj: Vlastní zpracování

Průběh porovnávaných rychlostí ukazuje obrázek číslo 24



Obrázek 24: Graf rychlostí stahování

Zdroj: Vlastní zpracování

Přestože průběhy veličin jsou poměrně rozdílné, rozdíl v průměrné rychlosti stahování činí 5,72%, jak ukazuje tabulka číslo 10 a lze předpokládat, že s rostoucím objemem porovnávaných hodnot se tento rozdíl bude snižovat.

Tabulka 10: Srovnání statistických hodnot rychlostí stahování

Statistická veličina	*Ruční měření [KB/s]*	*Automatické sledování [KB/s]*	*Rozdíl*
Střední hodnota	151,48	160,67	5,72%
Směr. odchylka	37,56	44,30	15,21%
Minimum	98,7	88,7	-11,25%
Maximum	256	237,2	-7,95%

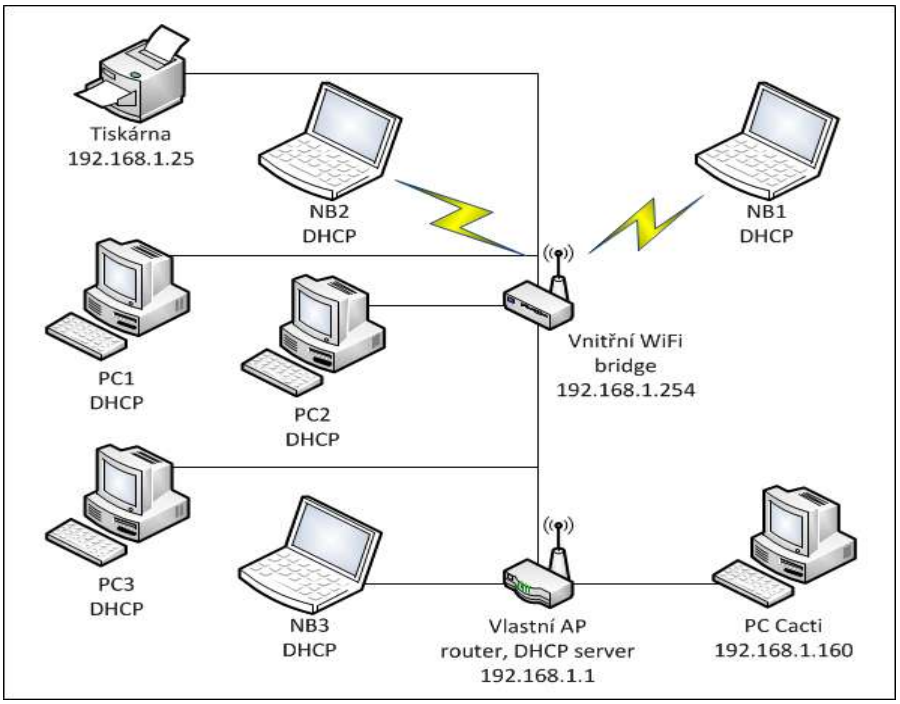
Zdroj: Vlastní zpracování

4.2. Monitorování sítě

Monitorování sítě sestává jednak ze sledování rychlosti odezvy zařízení na ping, tak z monitoringu, který slouží k rychlé identifikaci výpadku a určení místa poruchy. Snadno lze ověřit, zda vznikl problém na vlastním zařízení, nebo na zařízení poskytovatele připojení.

4.2.1. Identifikace poruchy

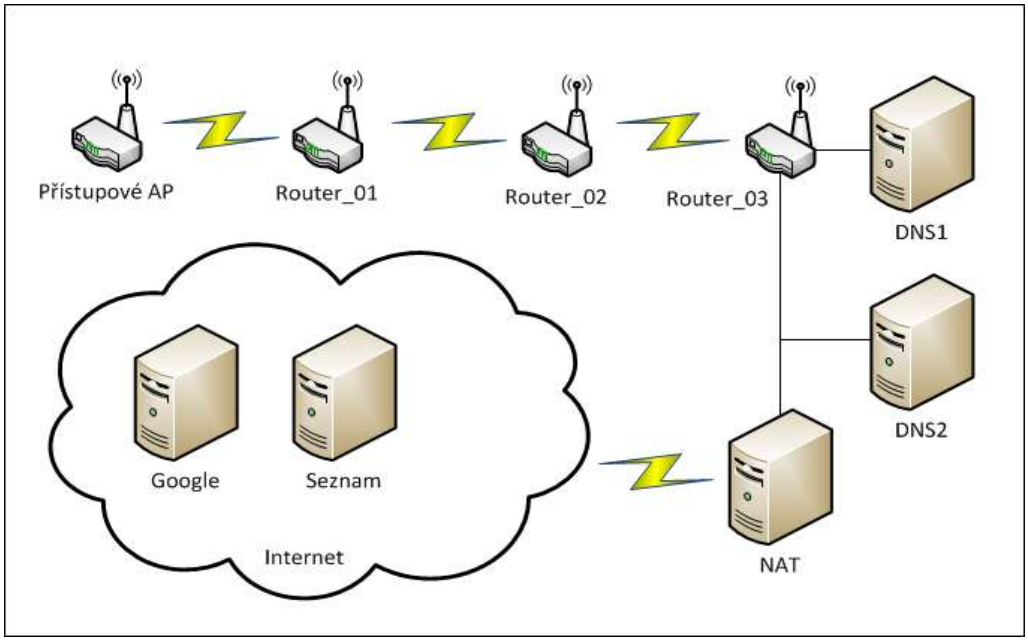
Pro snadné určení místa poruchy je nutné nejdříve uvést schéma monitorované sítě. Na obrázku číslo 25 je vidět vnitřní sít, ve které se nachází Vlastni_AP a počítač s nainstalovaným monitorovacím systémem Cacti.



Obrázek 25: Schéma vnitřní sítě

Zdroj: Vlastní zpracování

Na obrázku číslo 26 je vidět zjednodušené schéma vnější monitorované sítě.



Obrázek 26: Zjednodušené schéma vnější monitorované sítě

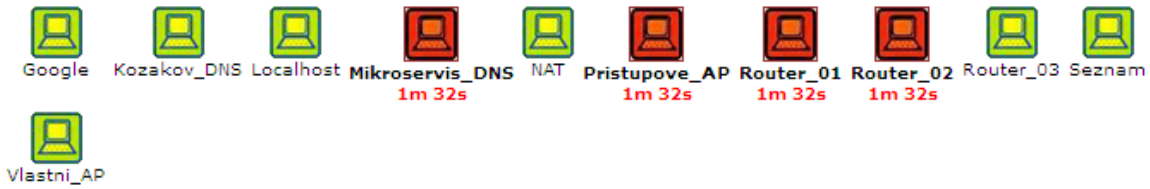
Zdroj: Vlastní zpracování

Na obrázku číslo 27 je vidět sérii tří snímků, které představují vznik poruchy na DNS serverech a postupné obnovení jejich činnosti.

Obrázek 27: Identifikace výpadků

Zdroj: Vlastní zpracování

Systém Cacti umožňuje zaslání mailu v případě výpadku, což je ovšem poněkud komplikované v případě, že je sledováno připojení k internetu, tedy vnější síť. Při jejím výpadku těžko prostřednictvím nefunkční sítě odešleme mail. V případě simulované poruchy, pomocí krátkodobého vypnutí vlastního AP, dojde postupně ke ztrátě spojení s ostatními vnějšími body. Příklad na obrázku 28.



Obrázek 28: Simulace poruchy spojení

Zdroj: Vlastní zpracování

V tomto případě záleží na délce vypnutí vlastního AP, kolik nefunkčních bodů bude detekováno. Příklad seznamu mailových zpráv odeslaných systémem ukazuje obrázek číslo 29.

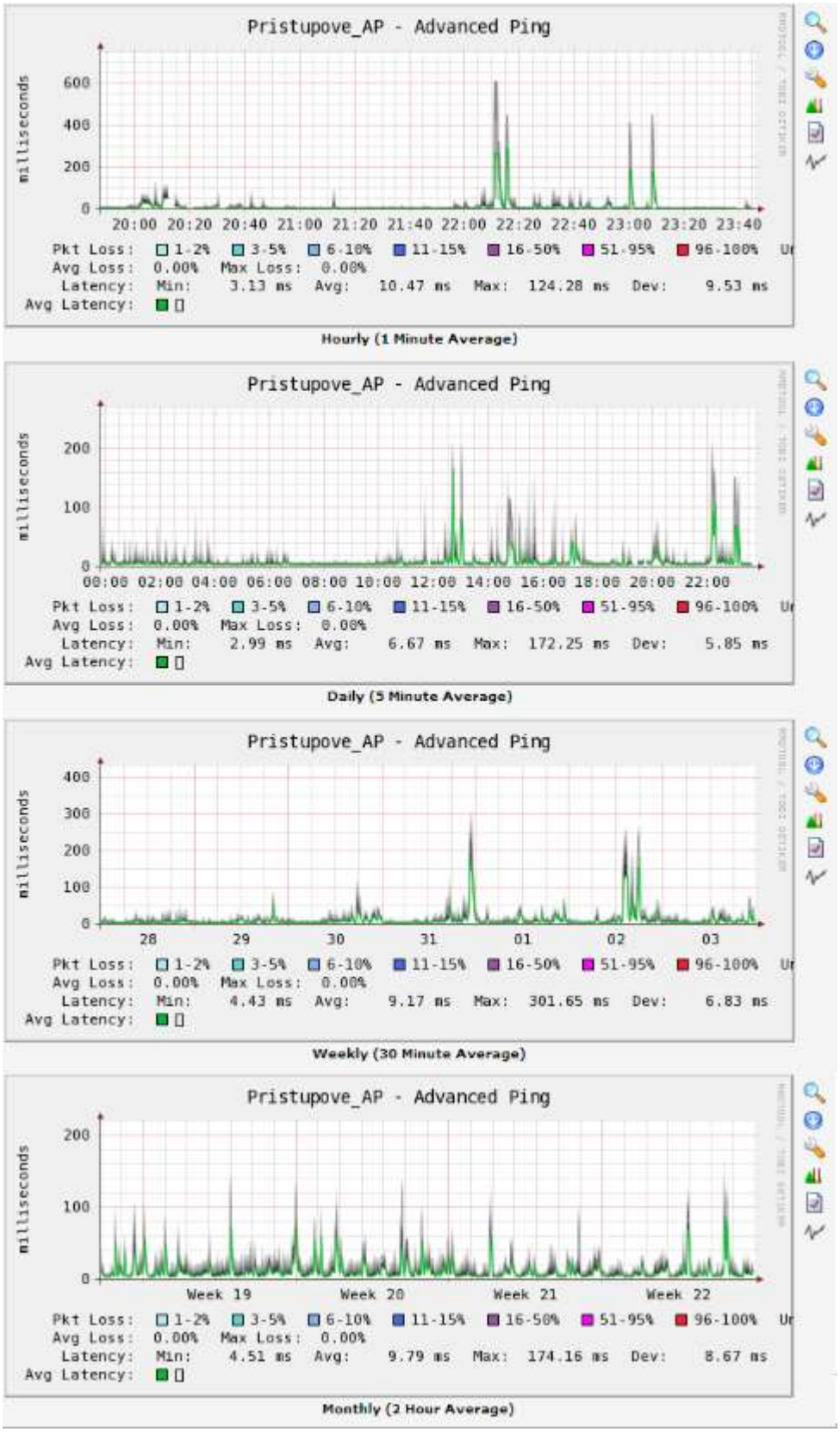
Obrázek 29: Soupis předmětů zpráv odeslaných systémem Cacti

Zdroj: Vlastní zpracování

Problém s odesláním mailu v případě nefunkčnosti sítě lze obejít zasláním notifikace pomocí SMS za použití mobilního telefonu připojeného k monitorovacímu PC. V takovém případě je ovšem nutná instalace software ovládajícího mobilní telefon. Celý postup v tomto případě je popsán na stránce: http://makesomecode.com/2011/07/19/setting-up-sms-with-cactiez-and-gnokii/ .

4.2.2. Měření odezvy na ping

Sledování rychlosti odezvy na ping odhalilo, že klient Vlastni_AP nemá problém s počtem připojených klientů, kterých obvykle bývá pět až šest. Přestože kvalita připojení na Pristupove_AP není špatná, spojení by pravděpodobně zlepšila směrová anténa, pokud lze předpokládat, že ne veškerá zpoždění má na svědomí přetížení přípojného bodu Pristupove_AP. Průběh charakteristik při průchodu paketů distribučním systémem poskytovatele připojení je obdobný napříč celou infrastrukturou. Mírně odlišné charakteristiky poskytují odezvy Internetových serverů www.seznam.cz a www.google.cz. Náhled na typické charakteristiky ukazuje příklad výstupu bodu Pristupove_AP na obrázku číslo 30. Porovnání automatického měření odezvy s ručním bylo prováděno vždy na stejném serveru. Průměrná doba odezvy na sledovaném vzorku vykazovala rozdíl 7,09%.



Obrázek 30: ICMP odezvy přístupového accesspointu

Zdroj: Vlastní zpracování

ZÁVĚR

Výsledkem této práce je plně funkční monitorovací systém pro sledování parametrů připojení na Internet. Systém je velmi snadno rozšiřitelný a pouhým přidáním nových bodů sledování umožňuje sledovat například všechna domácí PC a další zařízení. Vlastní implementace je vytvořena na bazarovém PC s nainstalovaným operačním systémem Linux. Protože samotné využití volně šiřitelného software nezaručí dodržení minimálních pořizovacích nákladů, které v takovémto případě představují v převážné míře mzdové náklady odborného technika provádějícího instalaci a nastavení, je využita specializovaná distribuce OS Linux CactiEZ. Náklady na provoz jsou představovány spotřebou elektrické energie, příkon činí přibližně 50 W. Vlastní monitorování je prováděno systémem Cacti, softwarem pro monitoring infrastruktury zapojené v počítačové síti. Tento je doplněn pluginem pro sledování odezvy serverů a vlastním skriptem umožňujícím měřit rychlost stahování dat z Internetu. Systém byl využit pro sledování připojení k Internetu a následnému vyhodnocení naměřených parametrů. Tímto byly splněny základní požadavky na zadanou práci. Přestože systém je využit pro sledování domácího připojení k Internetu, nic nebrání jeho nasazení v menší firmě a v případě použití výkonnějšího hardware i pro sledování rozsáhlejších sítí. Jelikož protokol SNMP je součástí všech dnes běžně používaných operačních systémů, umožňuje kromě připojení k Internetu sledovat celou infrastrukturu vnitřní sítě.

POUŽITÁ LITERATURA

[1] BADGER, MICHAEL. *Zenoss Core 3.x Network and System Monitoring*. Birmingham, UK: Packt Publishing, 2011, 312 s. ISBN 978-1-849511-58-2

[2] Cacti : *View topic - CactiEZ 0.6 yum troubles:*. [online]. 05.04. 2011. [cit. 2012-05-29]. Dostupné z: <http://forums.cacti.net/viewtopic.php?f=2&t=46833>

[3] ČSÚ: *Statistická ročenka České republiky 2011 - 21. Informační a komunikační technologie.* [online]. 23.11. 2011. [cit. 2012-05-29]. Dostupné z: <http://www.czso.cz/csu/2011edicniplan.nsf/t/35001C7F25/$File/0001112116.xls>

[4] DOSTÁLEK, LIBOR; KABELOVÁ, ALENA. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5. aktualizované vydání Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.

[5] HALL, ERIC A. *Internet core protocols*: *the definitive guide*. Cambridge, Mass.: O'Reilly, 2000, xx, 449 s. ISBN 15-659-2572-6.

[6] HARTPENCE, BRUCE. *Packet guide to core network protocols*. Sebastopol, Calif.: O'Reilly Media, 2011, 137 s. ISBN 14-493-0653-5.

[7] KAPLER, TOMÁŠ. *Internet pro všechny: Jak se připojit: kabelový Internet.* [online]. 7. 3. 2005. [cit. 2012-06-14]. Dostupné z: <http://www.internetprovsechny.cz/jak-se-pripojit-kabelovy-internet/>

[8] KYSELA, JIŘÍ. Internet pro všechny: Mobilní Internet v České republice – kompletní přehled. [online]. 1. 3. 2010. [cit. 2012-06-14]. Dostupné z: <http://www.internetprovsechny.cz/mobilni-internet-v-ceske-republice-kompletni-prehled/>

[9] KRETCHMAR, JAMES M; DOSTÁLEK, LIBOR. *Administrace a diagnostika sítí*: *pomocí OpenSource utilit a nástrojů*. 1. vyd. Brno: Computer Press, 2004, 216 s. ISBN 80-251-0345-5.

[10] KUNDU, DINANGKUR; LAVLU, IBRAHIM. *Cacti 0.8 Network Monitoring: monitor your network with ease!*. Birmingham, UK: Packt Publishing, 2009, 116 s. ISBN 978-1-847195-96-8.

[11] Nagios: *Nagios Overview*. [online]. [cit. 2012-06-14]. Dostupné z: <http://www.nagios.org/about/overview/>

[12] OLUPS, RIHARD. *Zabbix 1.8 network monitoring*: *monitor your network's hardware, servers, and Web performance effectively and efficiently*. Birmingham, U.K.: Packt Pub., 2010, vii, 410 p. ISBN 978-1-847197-68-9.

[13] SHINDER, DEBRA LITTLEJOHN. *Počítačové sítě*: *nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí*. Praha: SoftPress, 2003, 752 s. ISBN 80-864-9755-0.

[14] SCHRODER, CARLA. *Linux*: *kuchařka administrátora sítě*. Vyd. 1. Brno: Computer Press, 2009, 596 s. ISBN 978-80-251-2407-9.

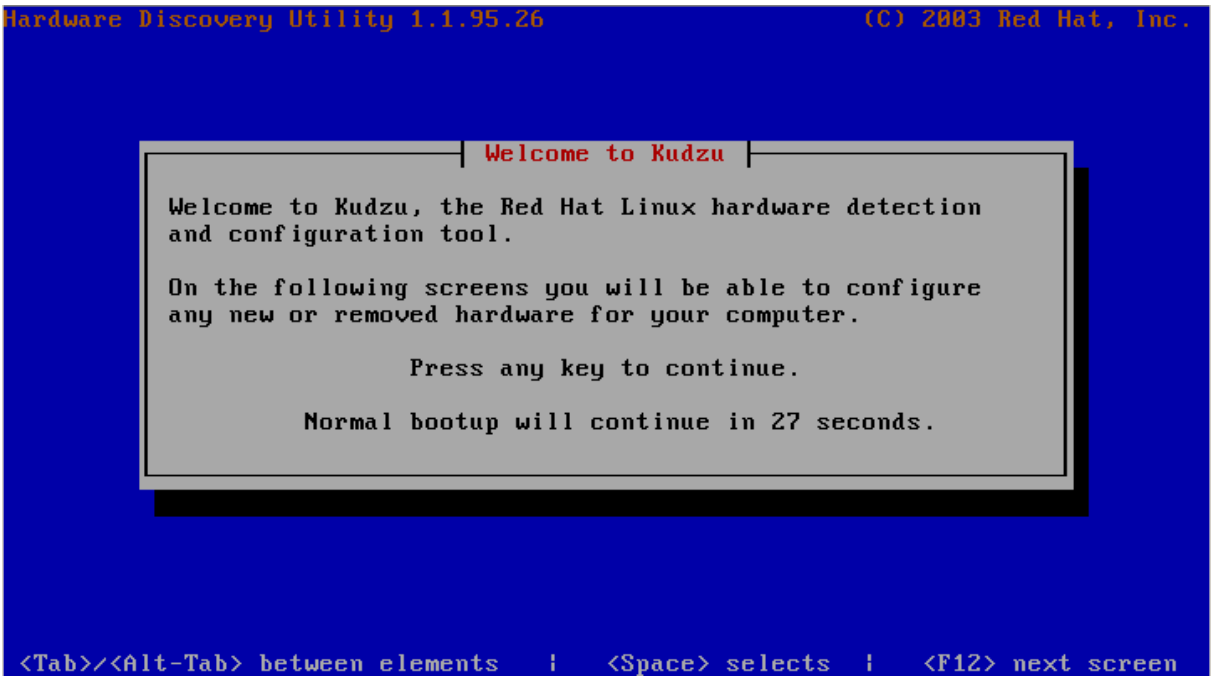
[15] URBAN, THOMAS. Cacti 0.8: beginner's guide : learn Cacti and design a robust network operations center. Birmingham, UK: Packt Publishing, 2011, 327 s. ISBN 978-184-9513-920.

[16] ZANDL, PATRICK. *Bezdrátové sítě WiFi*: *praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s. ISBN 80-722-6632-2.

SEZNAM PŘÍLOH

PŘÍLOHA A. INSTALACE MONITOROVACÍHO PC Z IMAGE DISKU

Pro instalaci monitorovacího PC lze využít image jeho disku vytvořenou pomocí nástroje Clonezilla, případně použít již hotovou instalaci do VirtualBoxu. Obě jsou součástí DVD přílohy této bakalářské práce. Clonezillu lze nalézt na stránce http://clonezilla.org/. Po obnovení image na PC, případně do virtuálního PC, dojde při prvním startu k nové konfiguraci ovladačů hardware. Při spuštění nástroje Kudzu je nutné stisknout libovolné tlačítko pro pokračování rekonfigurace, jak ukazuje obrázek číslo 31.



Obrázek 31: Spuštění Kudzu

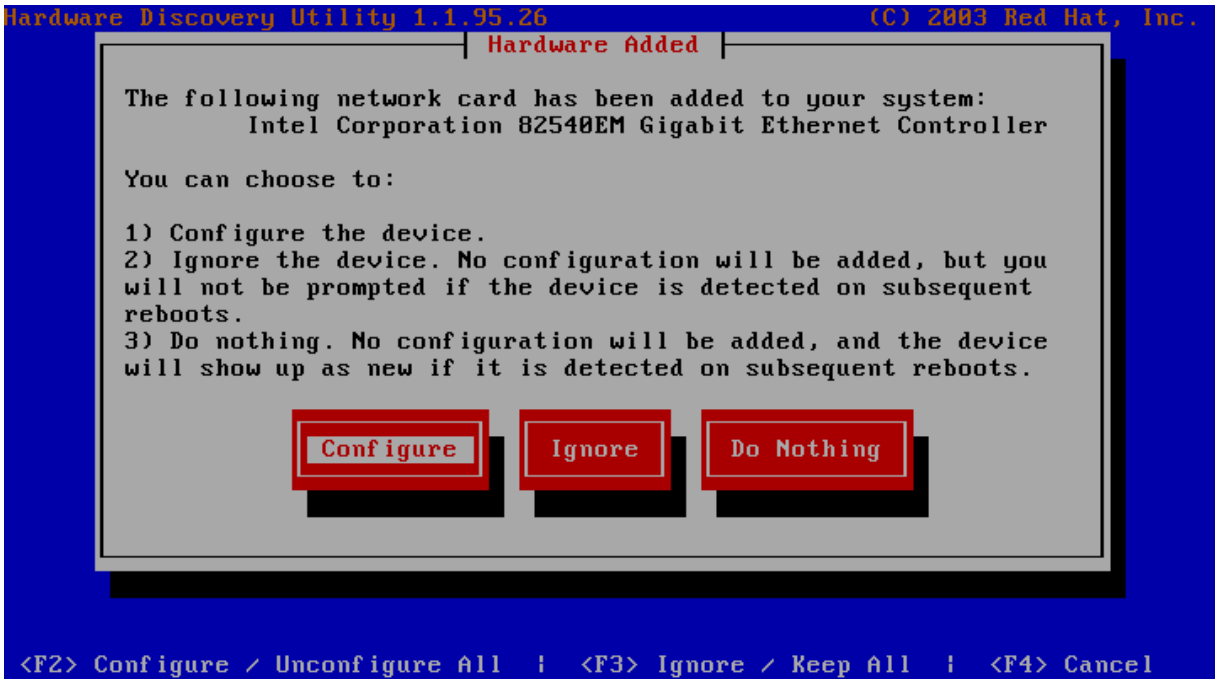
Zdroj: Vlastní zpracování

Následně potvrdíme odebrání konfigurace neexistujícího hardware, dle obrázku číslo 32.

Obrázek 32: Odebrání neexistujícího hardware

Zdroj: Vlastní zpracování

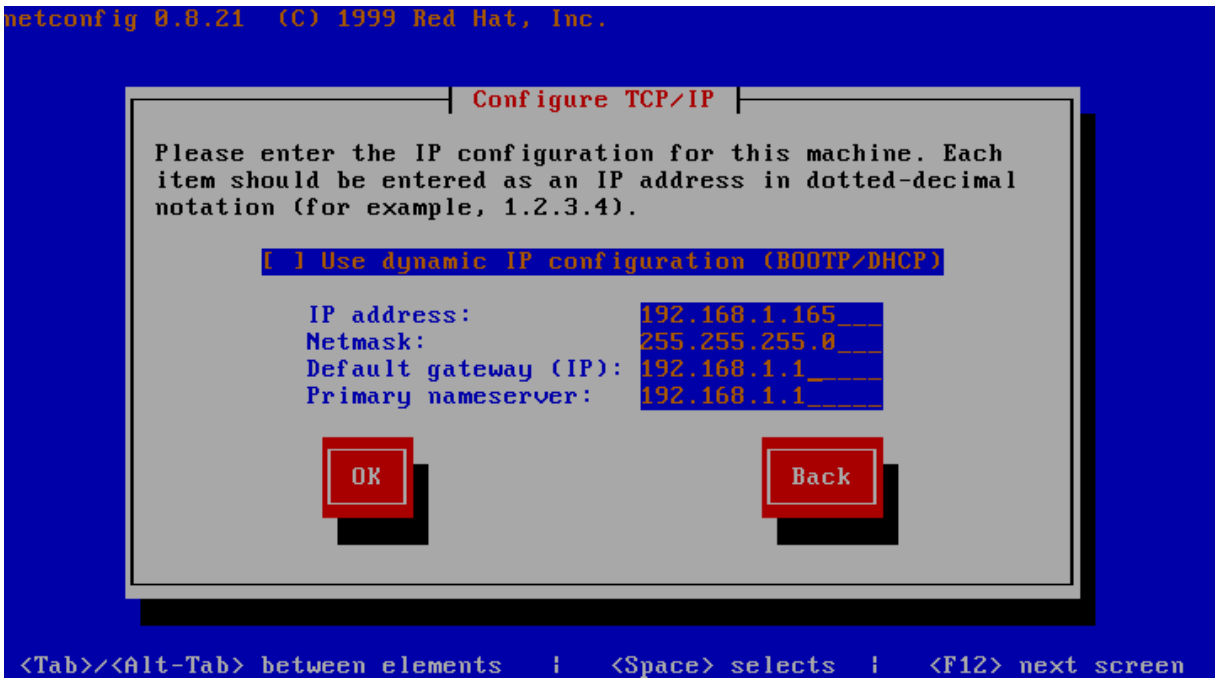
Odebírání neexistujícího hardware proběhne ještě několikrát, dle počtu změn oproti původnímu PC. Poté následuje konfigurace nového hardware dle obrázku 33.



Obrázek 33: Přidání nového hardware

Zdroj: Vlastní zpracování

Potvrzením tlačítka Configure dojde k automatické konfiguraci bez dalšího dotazu, pouze v případě síťové karty je požadováno její nastavení, příklad na obrázku číslo 34.



Obrázek 34: Nastavení síťové karty

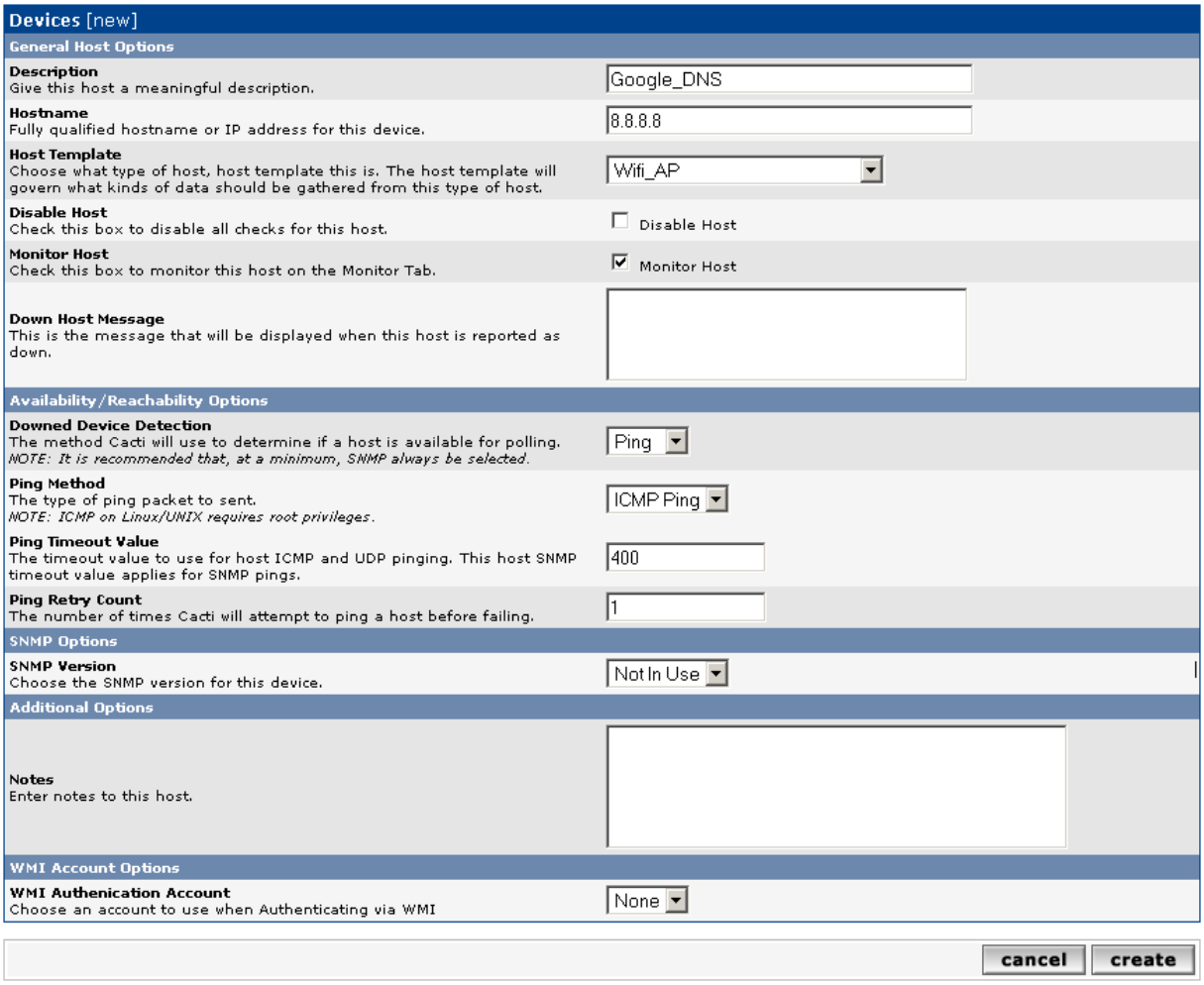
Zdroj: Vlastní zpracování

Po startu systému využívajícího image připraveného virtuálního PC v systému VirtualBox, je nutné nastavit IP adresu ručně nástrojem netconfig (sudo netconfig) na požadovanou hodnotu opět dle obrázku číslo 34. Heslo uživatele root je nastaveno na „upce2012“, heslo uživatele „admin“ pro Cacti je nastaveno na „upce2012“ Přihlášení do systému Cacti se provádí z webového prohlížeče, otevřením adresy použité v konfiguraci. Změnu konfigurace monitorovaných bodů, lze provést na záložce Console, volba Devices, dle obrázku 35.

Obrázek 35: Monitorovaná zařízení v Cacti

Zdroj: Vlastní zpracování

Monitoring jiného bodu lze spustit změnou konfigurace stávajícího bodu, bohužel však ani po vynulování statistik nedojde k úplnému odstranění jejich zobrazení v grafu, za tímto účelem je výhodnější vytvořit zařízení znovu dle zařízení již v systému vložených. Obrázek číslo 36 přibližuje vytvoření nového zařízení Google_DNS, zařízení je vloženo dle vzoru, vybraná šablona „Wifi_AP“ zajistí předvolení šablony grafu „Advanced Ping v1.3“, pro vytvoření stiskneme „Create“

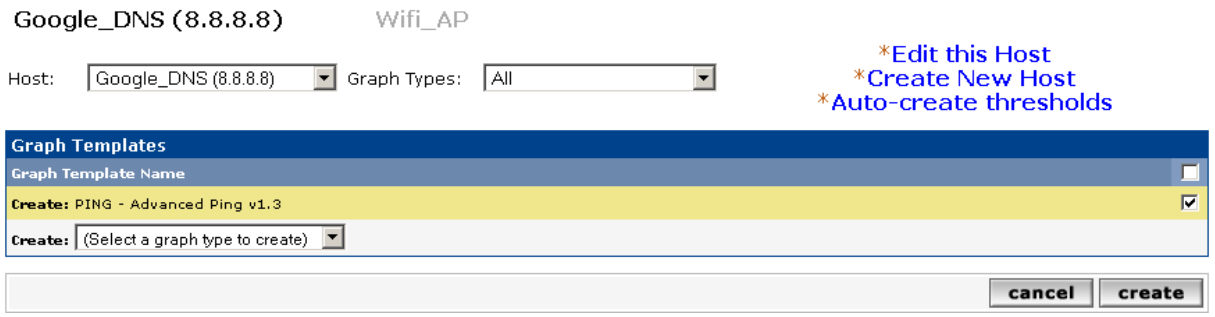


Obrázek 36: Vložení nového zařízení Google_DNS

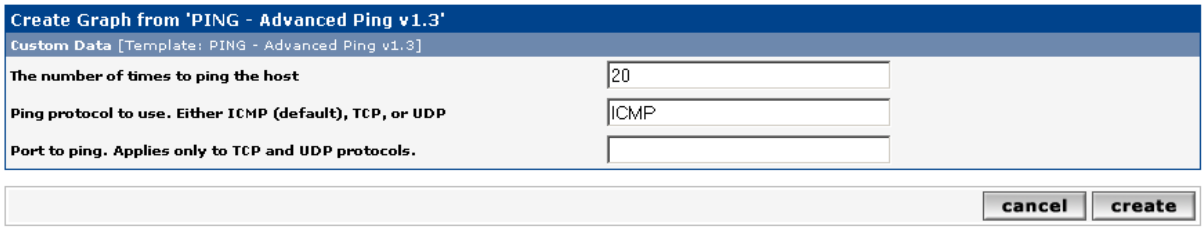
Zdroj: Vlastní zpracování

Následující série obrázků označená číslem 37, detailně přibližuje vytvoření grafu pro toto zařízení

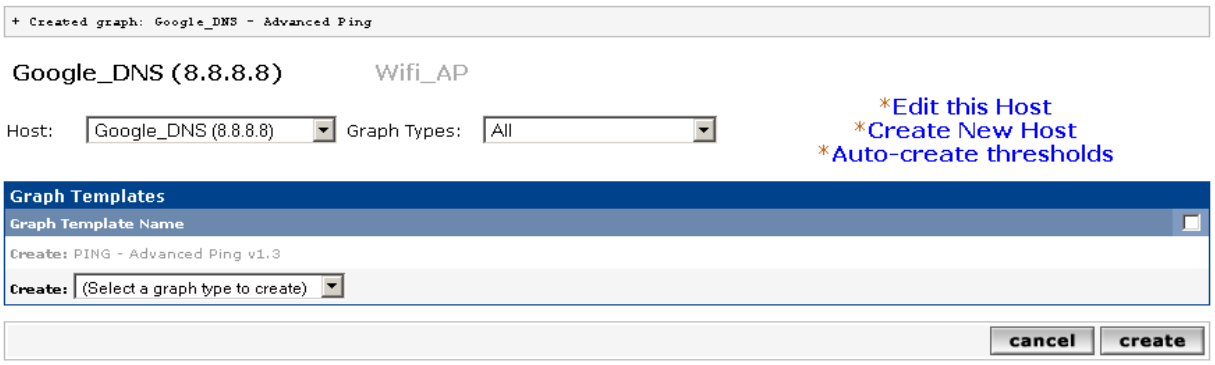
Zvolíme „Create Graph for this Host“



Zaškrtneme políčko u PING – Advanced Ping v1.3 a klikneme na „Create“



Stiskneme „Create“



Takto vypadá výsledek

V detailu zařízení (volba Devices a Google_DNS) je vidět že zařízení již je vykreslováno

Obrázek 37: Spuštění vykreslování grafického výstupu

Zdroj: Vlastní zpracování

PŘÍLOHA B. OBSAH PŘILOŽENÉHO DVD

- /VirtualBox – image připravené pro spuštění ve VirtualBox
- /Clonezilla – image disku vytvořené pomocí Clonezilla
- /txt - text práce