Monitorování stavu rozsáhlých sítí

Status monitoring of Wide Networks

Bc. Jindřich Matúšů

Diplomová práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2007/2008

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jindřich MATÚŠŮ**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Monitorování stavu rozsáhlých sítí**

Zásady pro vypracování:

1. **Vytvořte systém pro monitorování stavu rozsáhlých sítí s využitím údajů, které o síti mohou být uloženy v databázi.**
2. **Výsledný systém bude integrací existujících monitorovacích systémů, např. Nagios, Smokeping, Calstats, Cacti aj.**
3. **Zaměřte se na systémy, které dokáží informace o stavu síťových prvků získávat pomocí standardních protokolů – SNMP popř. SSH u Linuxu/Mikrotiku.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ZANDL, Patrick. Bezdrátové sítě WiFI: Praktický průvodce. 1. vyd. Brno : Computer Press, 2003. 190s ISBN 80-7226-632-2**
2. **Nagios [online]. 17.1.2008.2004, 17.1.1008 [cit. 2008-01-17]. Dostupný z WWW : http://nagios.org .**
3. **Cacti [online]. 2004 [cit. 2008-01-17]. Dostupný z WWW: http://cacti.net .**
4. **Mistrovství v Linuxu – Příkazový řádek, shell, programování; Mark G. Sobell; Computer Press, 2007;880 stran černobílých; ISBN: 987-80-251-1726-2**

Vedoucí diplomové práce: **Ing. Tomáš Dulík**
Ústav aplikované informatiky

Datum zadání diplomové práce: **20. února 2008**

Termín odevzdání diplomové práce: **19. května 2008**

Ve Zlíně dne 20. února 2008

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Tato diplomová práce se zabývá návrhem a implementací kompletního monitoringu pro rozsáhlé sítě, jakou je slfree.net, s využitím nejznámějších Open-Source nástrojů. Teoretická část je zaměřena na popis struktury sítě, protokolu SNMP a nejznámějších nástrojů pro monitoring. V praktické části je konkrétním způsobem implementován vybraný systém Cacti do komunitní sítě slfree.net. Na této síti jsou ukázány hlavní možnosti a funkce monitoringu.

Klíčová slova: monitoring, počítačová síť, Open-Source , protokol SNMP, Cacti, Nagios, Mikrotik RouterOS, opeační systém Debian Etch, plugin, SQL databáze ,PHP

ABSTRACT

This graduation thesis deals with design and implementation of full monitoring of wide networks like slfree.net with assimilation of best-known Open-Source software tools. Theoretical part describes network architecture, protocol SNMP and best-known monitoring methods. Practical part implements selected Cacti system into community network slfree.net. There are demonstrated main monitoring functions and facilities.

Keywords: monitoring, computer network, Open-Source, SNMP protocol, Cacti, Nagios, Mikrotik RouterOS, Debian Etch operating system, plugin, SQL database, PHP

Chtěl bych poděkovat vedoucímu diplomové práce panu Tomáši Dulíkovi za cenné připomínky a čas, který mě věnoval při konzultacích nad problémy řešení této diplomové práce a rovněž patří dík i Zdeňkovi Nejedlému za připomínky při testování systému.

Prohlašuji, že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

OBSAH

ÚVOD

Současná neustále rostoucí velikost a složitost lokálních počítačových sítí přináší i rostoucí požadavky na nepřetržitý dohled nad jejich správnou činností který je nezbytným předpokladem jejich dobré výkonnosti, bezpečnosti a spolehlivosti.

Co nelze měřit a sledovat, to nelze ani dobře a efektivně řídit. Monitoring sítě slouží k nepřetržitému sledování stavu a dostupnosti síťových prvků, serverů a jejich služeb, umožňuje sledování velkého množství parametrů sítě U rozsáhlých sítí je jediným efektivním prostředkem schopným průběžně dodávat provozní informace ze zařízení konsolidované do jednoho či více centralizovaných míst dle velikosti monitorované sítě.

Síťová a zařízení poskytují velký objem informací. Tyto informace je prakticky nemožné vyhodnotit bez výkonných a účinných nástrojů. Kvalitní grafické rozhraní umožní rychlou a přehlednou definici monitorovacích pravidel pro různé typy hardware a sníží pravděpodobnost chybné konfigurace. Možnost zaslat zprávy při výpadku některého ze sledovaných prvků či služeb administrátorům dle definovaných pravidel přináší zlepšení ve funkčnosti takové sítě.

Nasazení monitoringu je proces, který obnáší stanovení si požadavků co je důležité monitorovat, o čem je potřeba mít informace, které služby mají kritickou povahu a které neohrožují vlastní chod sítě. Požadované výsledky monitoringu je nutné často skládat z naměřených hodnot získaných naprosto odlišnými typy měření, například pomocí SNMP protokolu, sběrem a vyhodnocováním aplikačních logů zařízení či měřením na bázi toků dat.

Oblast monitoringu je podle mého názoru specifická tím, že zde neexistují definitivní, všeobjímající řešení typu all-in-one, která by vyhověla v prostředí libovolné infrastruktury. Každá síť a poskytované služby jsou z tohoto hlediska unikátním dílem.

V této práci se chci zaměřit na výběr vhodného Open-Source systému pro monitoring a implementaci do rozsáhlé komunitní sítě slfree.net Tento systém bude schopen poskytnout statistická data pro následnou analýzu činnosti sítě a jejich aktivních prvků, provoz sítě sledovat, upozorňovat na výpadky a poruchové stavy. Funkce tohoto systému bude možno rozšiřovat o další nové vlastnosti pomocí přídavných modulů. Konkrétní výsledky této práce si čtenáři mohou prohlédnout na stánkách komunitní sítě slfree.net v sekci Monitoring.

I. TEORETICKÁ ČÁST

1 AKTIVNÍ A PASIVNÍ MONITOROVÁNÍ

Většinu monitorovacích metod lze rozdělit mezi aktivní a pasivní. Při aktivním monitorování posíláme do sítě testovací pakety, které opět přijímáme v jiném místě sítě. Tímto způsobem můžeme měřit například zpoždění při průchodu sítí, ztrátovost nebo dosažitelnou propustnost.

Nevýhodou aktivního monitorování je přidaná zátěž do sítě, zejména při měření propustnosti intenzivním datovým tokem, možné ovlivnění provozu uživatelů a to, že

měříme charakteristiky našich testovacích paketů, nikoliv charakteristiky provozu uživatelů, které mohou být velmi odlišné. Je například obtížné měřit aktivně ztrátovost paketu v síti, protože ta velmi závisí na objemu a dynamice provozu, které jsou u skutečného provozu uživatelů velmi odlišné od testovacích paketů, které si můžeme dovolit do sítě posílat.[7]

Při pasivním monitorování neposíláme do sítě testovací pakety, ale vyhodnocujeme časové a objemové charakteristiky uživatelského provozu. Pasivní monitorování neovlivňuje uživatelský provoz a muže sledovat charakteristiky, které jsou aktivním monitorováním

nezjistitelné. Například jaký je objem a dynamika volné kapacity v síti, které aplikace

uživatelů mají největší nároky na kapacitu sítě nebo zda v síti dochází k bezpečnostním

útokům. Aktivní monitorování si lze tedy představit jako testovací sondu poslanou

jednorázově nebo opakovaně do sítě, zatímco pasivní monitorování je zpravidla trvale běžící pozorovatel dění na síti.

Kromě čistě aktivního nebo pasivního monitorování jsou i metody využívající kombinace

obou přístupů (vhodné například pro měření ztrátovosti), metody zpracovávající data získaná z komponentů síťové infrastruktury, např. pomocí SNMP nebo protokolu Netflow, a měření sledující stav koncové stanice (např. pomocí rozhraní PAPI). [7]

V této práci se soustředím na možnosti pasivního monitorování v komunitní sítí slfree.net.

1.1 Komunitní síť slfree.net

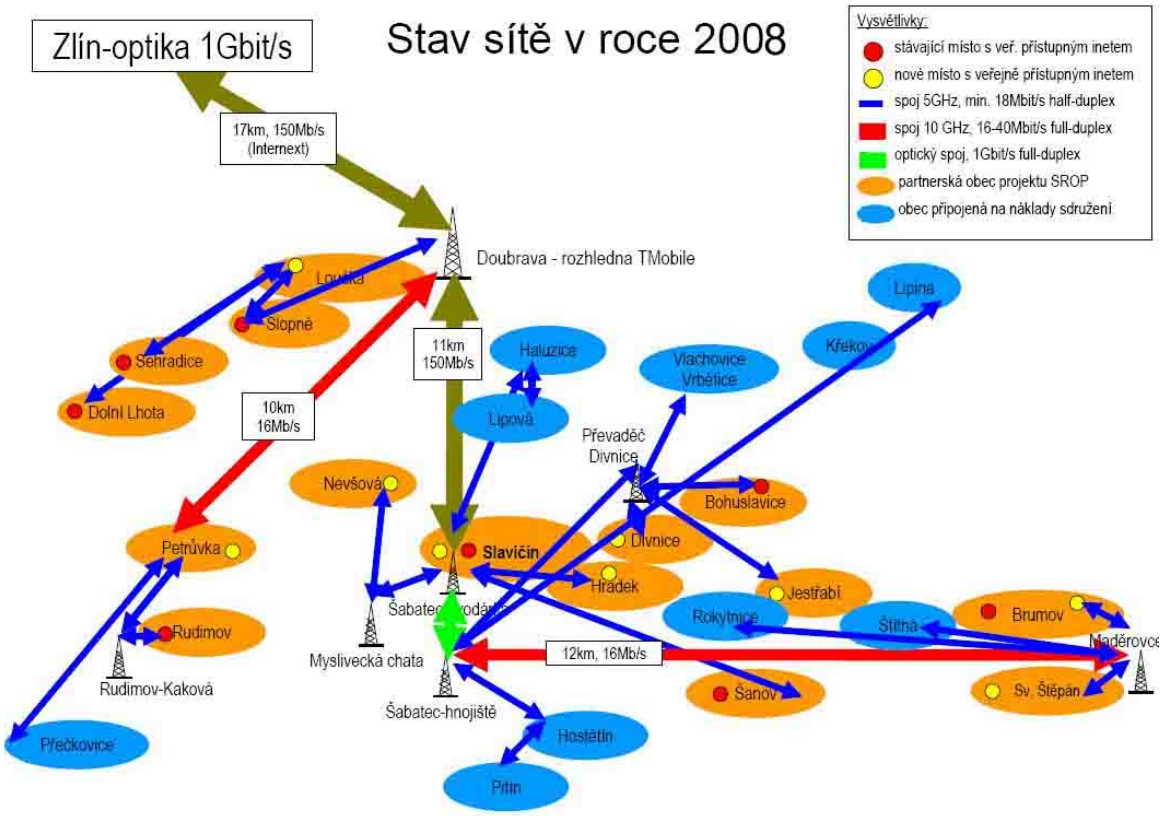
Komunitní síť slfree.net je součástí projektu „Vysokorychlostní internet pro Slavičínský region“. V červnu 2005 byla vyhlášena výzva grantového programu SROP, který byl dotován EU a Ministerstvem pro místní rozvoj, na předkládání projektů pro rozvoj informačních a komunikačních technologií v regionech, na což okamžitě reagovalo Občanské sdružení UnArt vytvořením žádosti o podporu projektu "Vysokorychlostní internet pro veřejnost a neziskové organizace ve Slavičíně". Regionální rada regionu soudržnosti NUTS II Střední Morava schválila projekt O.s. UnArt k financování programu SROP.

Ode dne chválení projektu začalo budování základní síťové infrastruktury potřebné pro získání internetové konektivity a připojení dalších a lokalit z prostředků stávajících členů O.s UnArt. Postupně k dnešnímu dni byla zprovozněna síťová infrastruktura vybudováním bezdrátových bodů v obcích Slopné, Loučka, Sehradice, Dolní Lhota, Nevšová, Petrůvka, Rudimov, Přečkovice, Haluzice, Lipová, Hrádek, Divnice, Bohuslavice. Vlachovice, Vrbětice, Lipina, Křekov, Pitín, Hostětín, Šanov, Rokytnice, Jestřabí, Štítná, Brumov, Svatý Štěpán a městě Slavičín a připojení těchto bodů jako celku do vysokorychlostní komunitní sítě slfree.net. Síť v jednotlivých obcích je budována převážně na systému vzájemně propojených bezdrátových přístupových bodů standardu 802.11a/b/g.

Ve městě Slavičín je síť kombinována technologií optika-ethernet-bezdrát.

O síť se stará 35 dobrovolných správců, kteří spravují jednotlivé přístupové body. Dále komunitní síť slfree.net zaměstnává jednoho technika na plný pracovní úvazek, který řeší problémy na hlavních páteřních spojích, routerech a převaděčích.

1.2 Topologie sítě



Obr.1. *Mapa sítě*

Na uvedeném schématu je znázorněna aktuální mapa sítě k lednu 2008. Síť neustále prochází vývojem, expanduje do dalších obcí, vznikají nové přístupové body v místech narůstajícího vytížení.

Zde si všimněme několika hlavních bodů:

1.2.1.1 Doubrava – Rozhledna TMobile

Jedná se o místo s centrálním routerem založeným na operačním systému Debian Etch 4.0, který routuje hlavní segmenty sítě :

- Směr k ISP ve Zlíně na Jižních Svazích, budova II. Segmentu, spoj Ceragon 150Mbps v pásmu 30GHz
- Směr Petrůvka, spoj Alcoma v pásmu 10GHz o rychlosti 16Mbps
- Směr Loučka spoj v pásmu 5Ghz o rychlosti 18Mbps
- Směr Slavičín - vodárna, spoj Ceragon 150Mbps v pásmu 30GHz

1.2.1.2 převaděč Slavičín – vodárna

Zde se nachází linuxové servery a sekundární router, tvořen dvěma propojenými routerboardy, který routuje směry:

- Optická síť Řadové domy ve středu Slavičína
- Optický spoj pro převaděč Šabatec – hnojiště
- přístupové body v částech Slavičína – Lukšín, Vlára, Městský úřad, AP Štefaník, Sídliště Mír, AP Hrádek Agrinea
- směr obce Šanov lyžařský vlek, Nevšová

1.2.1.3 převaděč Slavičín - hnojiště

Je propojen optickým spojem o rychlosti 1 Gbps s převaděčem Slavičín - Vodárna. Obsahuje dva routerboardy , které routují následující segmenty sítě:

- směr Haluzice, Křekov, Lipina, převaděč Divnice hřbitov, Lipová, Haluzice
- AP ve Slavičíně Agrol, Vlára, Vlára U Lesa, Výpusta
- směr převaděč Maděrovce
- směr Pitín, Hostětín, Přečkovice

1.2.1.4 převaděč Divnice hřbitov

Obsahuje routerboard zajišťující routování směrů:

- Divnice a Army park
- Vlachovice, Vrbětice, Bohuslavice a Jestřabí

1.2.1.5 převaděč Maděrovce

Je tvořen dvěma routerboardy, routuje směry k obcím:

- Brumov AP obecní úřad,Sněhurka,Družba, Dům dětí a Dům kultury
- Štítná, Svatý Štěpán, Rokytnice

1.2.2 Používané technologie a hardware

Jak již bylo řečeno, v jednotlivých obcích jsou vybudovány bezdrátové přístupové body v pásmu 2,4 a nověji v pásmu 5 GHz. Ve Slavičíně se používá kombinace sítě bezdrát-optika-ethernet.

Optická část sítě je tvořena spojem mezi převaděči Šabatec vodárna a Šabatec hnojiště, dále pak spojem Šabatec vodárna – Slavičín centrum. V centru Slavičína je spoj ukončen optickým switchem v nejbližším řadovém domě ve směru od Šabatce. Dále jsou odsud jednotlivé vchody řadových domů propojeny multividovým optickým kabelem a ukončeny celkem čtyřmi ethernetovými switchi s optickými převodníky.

1.2.2.1 Hardware

Bezdrátové přístupové body se skládají ze zařízení Routerboard RB 333, 500, 533, 600. Jedná se o kompaktní miniPC s CPU o frekvenci 233-433Mhz, 64-512MB RAM a CompactFlash kartou 64-512MB. Takovýto hardware je schopen zajistit dostatečnou konektivitu pro přístupový bod s počtem 40ti účastníků.

Převaděče, vzhledem k vyššímu požadavku na výkon při routování, jsou vybaveny převážně Routerboardy VIA EPIA s CPU o frekvencích 600 nebo 800 Mhz, poskytující dostatečný výkon pro routing více přístupových bodů.

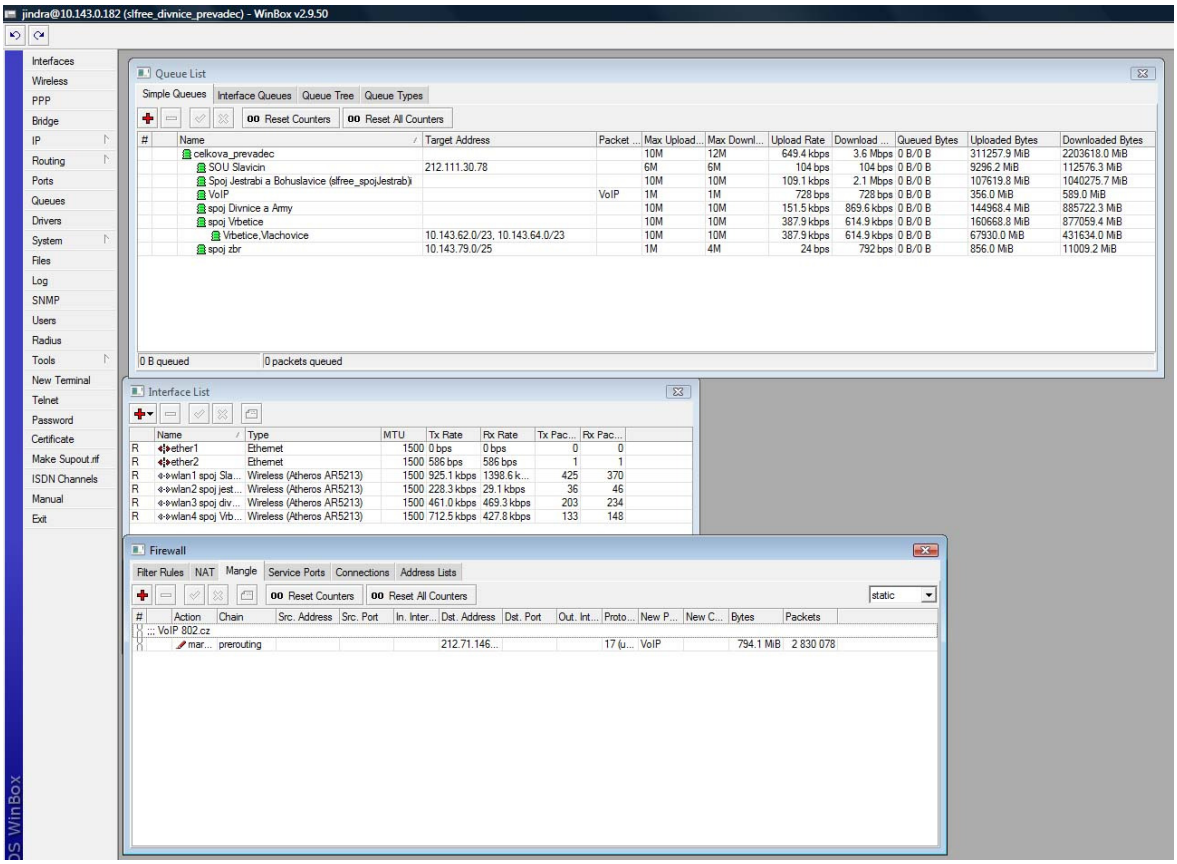
Optická část sítě se skládá ze dvou spojů s optickými kabely Siemens 8MBF50L55 tvořenými 8-mi vláknovým multividovým kabelem.

1.2.2.2 Software

Na většině přístupových bodů a routerů jsou zařízení s operačním systémem Mikrotik RouterOS v. 2.9 - 3.7. Jedná se o routerový operační systém založený na operačním

systému Linux, poskytující bohaté možnosti pro správu určité místní skupiny uživatelů, který možno konfigurovat a spravovat následujícími způsoby:

- Lokálně - připojením přes sériové rozhraní RS232 a telnet klientem spuštěným na počítači, odkud provádíme konfiguraci.
- Vzdáleně - přes webové rozhraní. Do libovolného internetového prohlížeče zadáme jeho IP adresu.
- Vzdáleně - použitím grafické konfigurační aplikace WinBox .
- Vzdáleně - přes šifrovaný protokol ssh.



Obr.2. *Winbox pro operační systém Mikrotik RouterOS*

Kromě klientských zařízení uživatelů sítě všechny aktivní prvky podporují SNMP protokol minimálně ve verzi 1.

2 MONITOROVACÍ NÁSTROJE

Pro monitoring sítě budeme převážně využívat protokol SNMP, který je ideálním prostředkem k získávání dat z jednotlivých přístupových bodů, převaděčů, linuxových hlavních routerů a optických switchů.

2.1 protokol SNMP

Simple Network Management Protocol začal vznikat v roce 1988 jako reakce na potřebu efektivní platformy pro správy počítačových sítí. V roce 1990 byl institucí IAB (Internet Acitivities Board) potvrzen jako standard sítě internet. První specifikace protokolu vznikla v roce 1989 a stanovovala vlastnosti SNMP verze 1.

Protokol SNMP se brzy po svém zavedení stal nejrozšířenější metodou pro řízení a sledování počítačových sítí. První verze tohoto protokolu SNMPv1 je definována v RFC 1157. Nepsaným standardem mezi výrobci zařízení je dnes ovšem jeho novější verze SNMPv2 vzniklá v roce 1993 a upravená v roce 1996. Z důvodu nedostatečné bezpečnosti obou předchozích verzí vznikla na počátku roku 1998 ještě novější verze, a to SNMPv3, která přidává mimo jiné i možnost šifrovaného přístupu ke spravovaným zařízením.

Při vzniku protokolu SNMP bylo cílem vytvořit pro správce sítí univerzální centralizovaný nástroj pro sledování funkce, kontrolu stavu a vzdálené řízení sítí. Z takového řídicího uzlu pak může správce číst a nastavovat jednotlivé parametry všech síťových zařízení.

Programové vybavení, které je k takové činnosti potřeba, se nazývá SNMP manažer. Ten komunikuje po síti se SNMP agenty v jednotlivých síťových zařízeních. Všechny potřebné informace jsou uloženy v přesně strukturovaných tabulkách MIB (Management Information Base). Standardní je dnes verze MIB, označovaná jako MIB-II, která je definována v RFC 1213. [5]

Identifikace každého objektu MIB je tvořena jednotlivými Object Idetifier řetězci (OID).

OID řetězec je tvořen posloupností čísel oddělených tečkou.Tato hodnota vznikne tak, že se vezme OID nadřazeného prvku a doplní se tečka a aktuální číslo. Celá tato stromová struktura je uložena v MIB databázi. MIB je tedy datová hierarchická stromová struktura,

která odpovídá danému konkrétnímu zařízení a je objektově orientována jako sada SNMP objektů, relací a operací na a mezi objekty.

Každý SNMP objekt zařízení musí mít jedinečné jméno, aby se dalo na něj odkazovat při SNMP operacích. Protože jedno zařízení může obsahovat objekty, definované nezávisle několika různými výrobci, schéma pro pojmenování těchto objektů muselo být navrženo tak, aby nemohlo dojít k záměně. Nějaký centrální registr všech možných objektů by byl nekonečně veliký, byla proto zvolena koncepce hierarchického stromu SNMP Global Naming Tree. Každé zařízení s podporou SNMP má svůj strom uložen ve vlastní MIB datové struktuře. Tyto datové struktury jsou volně ke stažení na stránkách výrobců síťového zařízení.

```
[admin@BBR] queue simple> print oid
Flags: X - disabled, I - invalid, D - dynamic
 0     name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.1686
       bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.1686
       bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.1686
       packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.1686
       packets-out=.1.3.6.1.4.1.14988.1.1.2.1.1.11.1686

 1 X   name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.1687
       bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.1687
       bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.1687
       packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.1687
       packets-out=.1.3.6.1.4.1.14988.1.1.2.1.1.11.1687

 2     name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.1688
       bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.1688
       bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.1688
       packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.1688
       packets-out=.1.3.6.1.4.1.14988.1.1.2.1.1.11.1688

 3     name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.1689
       bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.1689
       bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.1689
       packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.1689
```

Obr.3. *Příklad OID pro Queues v OS Mikrotiku*

Na obrázku můžeme vidět OID čísla objektů Simple Queue Mikrotiku. Mikrotik specifikuje pro každý queue následující formát OID:

.1.3.6.1.4.1.14988.1.1.2.1.1.**X.Y**

kde **X** specifikuje

2 pojmenování queue (pokud není zadáno, je shodné s target IP adresou)

3 target IP adresa

4 target IP maska

5 destination IP adresa

6 destination IP maska

8 přijaté bajty

9 odeslané bajty

10 přijaté pakety

11 odeslané pakety

V rámci monitoringu by nás zajímaly hodnoty příchozích a odchozích bajtů, tedy 8 a 9 u konkrétní queue.

V OS Mikrotik můžeme zjišťovat OID u objektů: /interface, /interface wavelan, /interface wireless, /interface wireless registration-table, /queue simple, /queue tree, /system identity, /system resources. Můžeme taktéž využít software, které umožňuje číst MIB strukturu zařízení a generovat námi definované SNMP dotazy, například MIB Browser 1.03.

Tab.1. Příklad SNMPv.1 paketu

verze	community string	operace	ID dotazu	error status	error ID	OID	hodnota
1	public	GET(0)	8	no error (0)	0	1.3.6.1.4.1.311.1.1.3.1.1.1	NULL

V protokolu SNMP je definováno celkem 6 základních operací pro komunikaci mezi manažerem a agenty v jednotlivých sledovaných zařízeních:

- Get - dovoluje manažerovi zjistit hodnotu vybraného objektu od SNMP agenta

- GetNext - dovoluje manažerovi získat hodnotu dalšího objektu ve stromové struktuře MIB
- GetBulk - (jen SNMPv2) tato operace byla přidána, aby se eliminovala potřeba zadávat velkého množství žádostí GetNext pro přenos větších objemů SNMP dat.
- Set - dovoluje manažerovi nastavit hodnotu vybraného objektu v agentu (přístup je řízen heslem tzv. community string)
- Trap - používáno na asynchronní informování manažera o významných událostech
- Inform - (jen SNMPv2) dovoluje výměnu Trap informací mezi několika manažery

SNMP protokol používá pro komunikaci UDP, díky čemuž je velmi rychlá, ale může dojít ke ztrátě (nedoručení) zasílané informace. Od verze 2 je implementována kontrola doručení, takže ke ztrátě by nemělo dojít. Standardně se používá port 161 a 162. Manažer, který posílá dotaz, zvolí dynamický port, z kterého posílá dotaz na port 161. Agent odpovídá z portu 161 na dynamický port klienta. V praxi je pro každý dotaz použit jiný dynamický port.

V této práci budeme pracovat převážně s definovanými šablonami SNMP dotazů, které jsou volně ke stažení pro zařízení s OS Mikrotik.

2.2 Nejpoužívanější open-source nástroje

Na internetu lze najít poměrně velké množství volně dostupných Open Source monitorovacích nástrojů vyvíjených pod licenci GNU/GPL,l liších se v poskytovaných možnostech monitoringu.

2.2.1 Nagios

Systém Nagios je robustní monitorovací nástroj, který je možno využít pro dohled aktivních síťových prostředků a služeb jimi poskytovaných. V případě výpadku některé z monitorovaných služeb umí systém poslat varování správcům systému či provést jiné definované akce, například restartovat problémovou službu nebo zařízení. Systém umožňuje monitorovat velké množství různých typů zařízení.

Nagios má spoustu možností a to z něj dělá velmi silný monitorovací nástroj. Některé z jeho významnějších rysů a charakteristik:

- monitorování síťových služeb SMTP, POP3, HTTP, NNTP, PING, atd.
- monitorování hostitelských zdrojů jako např. vytíženost procesoru, využití disku a pamětí, běžící procesy, logovací soubory atd.
- monitorování činitelů vnějšího prostředí jako je například teplota, tlak
- použití pluginů, které umožňuje uživatelům snadno vyvinout své vlastní kontrolní skripty a mechanizmy
- schopnost definovat síťovou hostitelskou hierarchii, dovolující odhalení a rozpoznání rozdílu mezi zařízením (službou), které je vypnuté a které nedostupné
- možnost poslat zprávu o stavu sítě, zařízení přes email, pager nebo na další uživatelem definované zařízení
- možnost rozesílání upozornění různým kontaktním skupinám
- vnější příkazové rozhraní, které dovoluje za provozu uzpůsobovat monitorování a chování celého systému
- uchování stavu zařízení a služeb i po restartu
- schopnost vizualizace problémů přes www rozhraní
- sledování aktuálních síťových stavů prostřednictvím webového rozhraní, zobrazení historií událostí, logovacích souborů atd.
- jednoduché autorizační schéma, které umožňuje definovat to, co který uživatel přes webové rozhraní uvidí a co ne

- možnost navázání stavu na nějakou akci, například při výpadku DHCP serveru restart démona či celého serveru

2.2.1.1 Systémové požadavky

Pro běh Nagiosu jsou nezbytné následující komponenty:

- dostatečně výkonné PC s operačním systémem Linux s kernelem 2.4 a vyšší
- Web server Apache s podporou CGI skriptů
- MySQL databázový program

2.2.1.2 Architektura

Hlavní částí Nagiosu je démon *nagios*, který nemá žádnou schopnost ani neobsahuje žádné funkce pro samotný monitoring. Je nezbytné doinstalovat zásuvné moduly zajišťující monitorovací a testovací funkce. Zásuvné moduly jsou nezbytně nutné pro monitoring sítě.

Základní pluginy Nagiosu jsou *check_fping*, *check_game, check_hpjd, check_ldap, check_mysql, check_radius, check_snmp*.

Démon *nagios* po spuštění načte z vlastního konfiguračního souboru nagios.cfg a konfiguračních souborů pluginů nastavení a začne provádět definované monitorovací činnosti. Informace o výsledcích činností ukládá do dočasných souborů a ty následně ukládá do MySQL databáze. Pro zobrazení informací o stavu slouží webové rozhraní, které je realizováno několika CGI skripty. Tyto CGI skripty přistupují do databáze MySQL se stavy a hodnotami jednotlivých sledovaných zařízení a zobrazují jej jako HTML stránky.[2]

2.2.1.3 Výhody a nevýhody Nagiosu

+ mohutný nástroj pro komplexní monitoring rozsáhlých sítí s možnostmi zasílání upozornění při definovaných událostech na e-mail, mobilní telefon, pager
+ velké množství zásuvných modulů rozšiřující funkce programu

+ poměrně velká podpora nejznámějších výrobců hardware
- složitá konfigurace
- webové rozhraní slouží pouze k zobrazování výsledků. Konfiguraci je nutno provádět v jednotlivých .cfg souborech editací a úpravou
- při chybě v kterémkoli konfiguračním souboru nelze systém spustit, nutno hledat příčinu v logu
- webové stránky slouží jen k vizualizaci

Systém je ideálním prostředkem k monitoringu rozsáhlé sítě. Poskytuje spoustu funkcí usnadňující dohled sítě.

Vzhledem k velké náročnosti konfigurace a časté potřebě drobných úprav monitoringu, jsem nezvolil tento systém pro nasazení v komunitní síti slfree.net. Nagios je vhodným pro sítě se zkušenými administrátory linuxového operačního systému. Jakákoli chyba, například v syntaxi kteréhokoliv konfiguračního souboru, má za následek pád a nefunkčnost celého systému, nikoliv jen těch služeb, jež daný plugin poskytuje.

2.2.2 Cacti

Cacti je vynikající open-source nástroj pro monitorování zařízení v síti s výstupem v podobě pěkných a přehledných grafů. Je velice univerzální, takže nám dovoluje širokou volnost při vytváření monitorování, ale existuje okolo něj silná komunita uživatelů, kteří vytváří různé šablony a přídavné moduly, takže běžné použití je jednoduché. Je komplexním monitorovacím systémem tvořeným v PHP, který ke své činnosti využívá RRD-Tool. Round Robin Database Tool je softwarový Open Source nástroj sloužící k měření, ukládání a zobrazování strukturovaných dat ve formě grafického výstupu.

Cacti umožňuje spravovat uživatele, kterým lze takto zpřístupnit jen důležité grafy a informace. Od základů byl navržen pro monitorování stovek zařízení. K samotné práci využívá převážně SNMP protokolu, je však možné vyrobit si vlastní skripty a skrze ně předávat Cacti informace. Za zmínku stojí možnost monitorovat dostupnost pingem, číst libovolné informace přes SNMP jako vytížení zařízení, datový tok, stav tiskáren, routerů, serverů, měřit teplotu a další uživatelsky definovatelné položky. Dalším použitím je

monitorování, zda jsou daná zařízení ONLINE-OFFLINE a sledování dostupnosti služeb. Systém můžeme nasadit do rozsáhlého prostředí, protože zvládá sledovat stovky až tisíce hodnot.[3]

Ke své činnosti v operačním systému Linux je nutno mít nainstalovány komponenty Apache2 web server, MySQLv. 3.x a PHPv.4.3.x.

Obr.4. *Grafické webové prostředí*

Cacti také dává možnost upravit vzhled grafů a například i jejich automatický export na vzdálený server.

2.2.2.1 Princip činnosti

Operace systému v Cacti mohou být rozděleny do tří částí – získání, uložení a vizualizace dat.

Pro získávání dat slouží Poller, který je potřeba naplánovat k pravidelnému spouštění. Poller pomocí prostředků PHP nebo pomocí pluginů získává data. Primárně se získávají

data pomocí SNMP, ale je možno využít i různé typy skriptů. Některá data se ukládají do SQL databáze, ale hlavní data jsou uložena pomocí RRDToolu do velmi kompaktních souborů o stálé velikosti. K zobrazení pomocí grafů slouží opět RRDTool s bohatou nabídkou možností.

V praxi potřebujeme vždy nejprve zadat zařízení, kterého se budou akce týkat, pomocí Devices. Následně vytvořit zdroj dat Data Source. Ten se vytváří automaticky pomocí šablony. Z datového zdroje se vytvoří graf v Graph Managementu pomocí šablony grafu, který přidáme se do stromové struktury pro zobrazení v Graph Trees.

Základní vizualizace spočívá v tvorbě grafů pomocí šablon Graph Templates, které jsou automaticky zřetězeny s datovými šablonami, jenž vytvářejí zdroje dat. Pomocí přídavného pluginu Weathermap lze tvořit mapy sítě, na kterých lze sledovat aktuální vytížení spojů, vytížení aktivních prvků ve formě již definovaných grafů.

Cacti je plně grafiky orientovaný monitorovací nástroj, kompletní administraci a ovládání lze provádět v přehledném grafickém rozhraní. Silnou stránkou Cacti je nejen existence řady šablon, ale také existence řady rozšíření primární funkčnosti pomocí pluginů. Samotná správa a nastavení je jednoduchou záležitostí i pro méně zdatné správce jednotlivých přístupových bodů komunitní sítě slftree.net, proto jsem jej zvolil jako hlavní monitorovací nástroj.

2.2.2.2 Nejznámější rozšiřující pluginy a jejich popis

Kolem open-source projektu Cacti je soustředěna silná komunita uživatelů, kteří neustále vyvíjejí další pluginy se zajímavými funkcemi.

Mezi nejznámější patří:

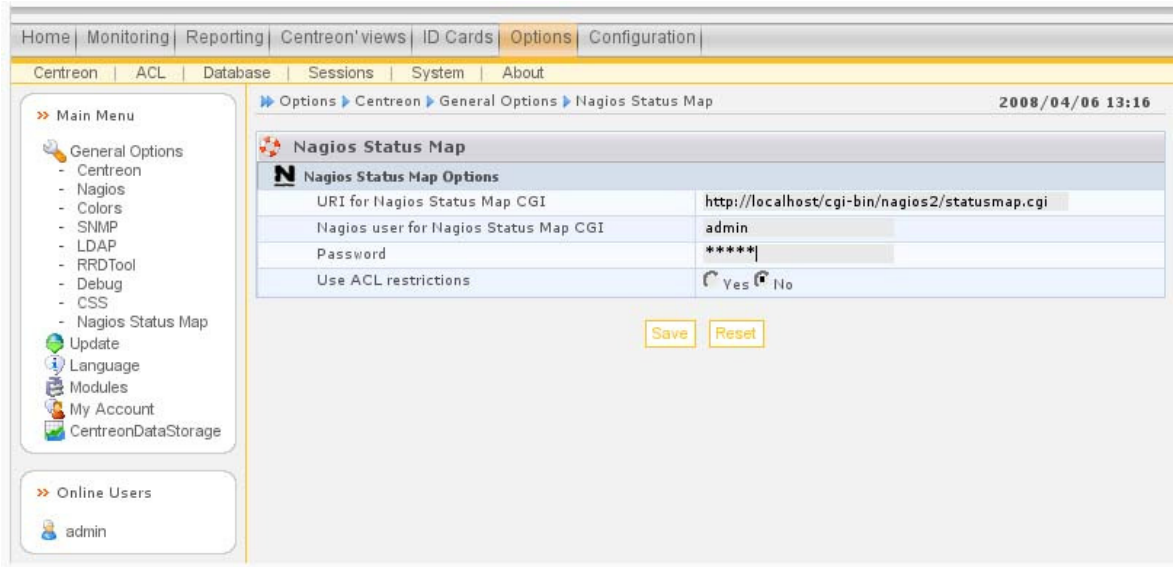
- **BackUP** - Přidává možnost archivace uložených dat a nastavení Cacti, možno archivovat i na vzdálený server.
- **Reports** - Umožňuje zasílat grafy v definovaných časech e-mailem.
- **Discovery** - Plugin automaticky vyhledává v síti aktivní prvky s podporou SNMP, která ještě nejsou monitorována.

- **Syslog** - Přidáva možnost ukládat logy ze zařízeních v databázi a vytvářet alerty podle dat z logů prvků sítě.
- **Thold** - Hlídá definované prahové hodnoty na prvcích sítě.
- **Uptime** - Sleduje stav zařízení, umožňuje provádět přes protokol SSH restart zařízení čislužeb na základě splnění nějaké definované podmínky
- **Manage** - Umožňuje provádět vzdálenou správu zařízení, serverů, služeb atd., hlídá jejich stav a provádí plánované definované akce na zařízeních.
- **NCP** - Nagios Plugin for Cacti. Umožňuje propojení s monitoringem Nagios a využívat jeho dat a funkcí.
- **Weathermap -** Umožňuje tvořit grafické mapy sítě.

2.2.3 Centreon

Centreon je modulárním monitorovacím softwarem, který ke své činnosti používá Nagios2. Obsahuje plně grafické rozhraní, ve kterém je možno provádět kompletní konfiguraci a správu monitoringu. Veškeré nastavení a získaná data se ukládají do databáze MySQL, a do konfiguračních souborů Nagiosu.

Centreon obsahuje množství přídavných modulů, dokáže pracovat s protokolem SNMP síťových prvků, zobrazovat grafy, mapu sítě ve 2D i 3D. Též poskytuje možnost při definovaných stavech síťových zařízení zasílat upozornění formou emailu, SMS.



Obr.5. *Centreon*

Systém je fronted aplikací k Nagiosu.

2.2.4 Zabbix

Je multiplatformní software na monitorování aplikací, sítí a jejich aktivních prvků. Projekt poskytuje flexibilitu a jednoduchou administraci prostřednictvím webového rozhraní. Umožňuje zobrazovat přehledné výsledky monitorovaní ve formě grafů, zasílat upozornění a užívatelsky definované přehledy, je zde přidána podpora pro PostgreSQL.

Pro Zabbix nejsou vyvíjeny žádné pluginy, tento monitorovací systém je uzavřeným systémem pro vývojáře pluginů, obsahuje pouze základní funkce monitoringu jako jsou podpora SNMP protokolu, vizualizace v podobě map, upozorňování na stav zařízení ONLINE-OFFLINE.

Je vhodným nástrojem pro malé sítě.

II. PRAKTICKÁ ČÁST

3 CACTI A ROZSÁHLÁ KOMUNITNÍ SÍŤ SLFREE.NET

V praktické části této práce se budu věnovat vlastní implementaci monitorovacího systému do komunitní sítě slfree.net. Cacti splňuje důležité 3 základní požadavky:

- otevřený, uživatelsky přívětivý systém s množstvím rozšiřujících pluginů
- malá náročnost na systémové prostředky
- jednoduchá administrace pro správce sítě

Od monitoringu očekávám dlouhodobou archivaci shromažďovaných dat z instalovaných síťových prvků, možnost tvorby výstupů v podobě grafů statistik provozu i za uplynulá časová období, upozorňování na poruchy nebo na stavy blízké poruchovým stavům. Analýzou provozu spojů, klientských zařízení budeme moci odhalit časově nestálé problémy, které běžnou kontrolou provozu sítě nelze téměř odhalit, například problematiku tzv. skrytých uzlů v bezdrátové síti.

Problém skrytého uzlu je způsoben faktem, že návrh fyzických protokolů 802.11a/b/g byl veden hlavním předpokládaným způsobem využití - bezdrátovým připojením uživatelů uvnitř budov na vzdálenost maximálně desítek metrů, jako doplněk k metalické síťové kabeláži. Typický příklad je připojení desítek notebooků účastníků konference v sále, kde by připojení pomocí kabelů bylo neekonomické, nepraktické a velmi těžko realizovatelné. Rozdíl mezi konferenčním sálem a wifi sítí s externími anténami (na střechách) je ten, že wifi karty všech uživatelů v sále vzhledem k malé vzdálenosti a všesměrovým anténám vzájemně slyší své vysílání. Mohou tak reagovat na stav, kdy před vysíláním vlastních dat zjistí, že kanál je momentálně obsazen vysíláním jiného uživatele. Situace je ale naprosto odlišná v případě externích antén: důvodem je jejich větší směrovost a také členitý venkovní terén s mnoha překážkami (stromy, domy, …), kvůli čemuž se část klientů vzájemně neslyší. Uživatelům, jejichž vysílání je před ostatními uživateli skryto díky překážkám nebo díky velké směrovosti jejich antény, se říká „skryté uzly“. Omezení efektu skrytých uzlů je možné pouze dodržování minimálních vzdáleností uživatelů od přístupového bodu do 100m a použitím máloziskových antén s větším úhlem vyzařování, které zajistí, že se většina uživatelů bude vzájemně slyšet. [9]

Síť slfree.net je z velké části tvořena bezdrátovými přístupovými body, je zde tedy velká pravděpodobnost výskytu skrytých uzlů.

Nastavením monitorování statistik síťového provozu takového klienta nám pomůže odhalit, zda se jedná o skrytý uzel nebo zda-li je problém s připojením jiného rázu.

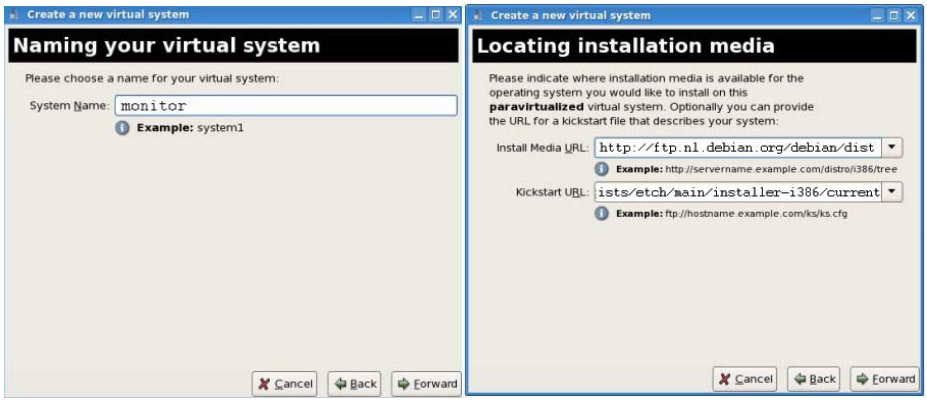
3.1 Instalace a konfigurace serveru

Pro Cacti budeme potřebovat linuxový server s webovým serverem Apache2, MySQL a PHP, dále vyčlenit veřejnou IP adresu 212.111.4.116 z ze seznamu rozsahu slfree.net a nastavit v DNS záznamy pro tuto adresu na *monitor.slfree.net.*

3.1.1 Instalace serveru

Síť slfree.net má pro monitoring k dispozici v technologickém domku v místní části Slavičína – Šabatce fyzický server Zeus s hardwarovou konfigurací Intel Pentiun 4 2.8 Ghz, 2GB RAM DDR2, 2x500GB v RAID1 poli. Operačním systém je linux Debian Etch s instalovaným XEN virtual PC. Na tento virtuální počítač nainstalujeme operační systém Debian Etch .

Na fyzickém serveru Zeus spustíme XEN, pomocí průvodce vytvoříme virtuální stroj. Zadáme webovou cestu s instalačními soubory Debianu, název počítače *monitor* a IP adresu 212.111.4.116.



Obr.6. *Průvodce vytvořením virtuálního stroje v XENu*

V průběhu instalace zvolíme k nainstalování komponenty Apache2, MySQL databázi. Po nainstalování základu operačního systému doinstalujeme z bashe příkazem apt-get install {název_balíku} nezbytné balíky:

- ssh - openssh-server pro vzdálený přístup protokolem ssh
- phpmyadmin - webové rozhraní pro správu MySQL databází
- mc - souborový manažer Midnight Commander

3.1.2 Konfigurace serveru

Konfigurace serveru zahrnuje především správné nastavení PHP a PhpMyAdminu pro přístup k SQL databázi. Konfigurace PhpMyAdminu se provádí editací a úpravou souboru `/etc/phpmyadmin/config.inic.php`. Otevřeme konfigurační soubor a nastavíme následující parametry:

název počítače, kde běží MySQL

```
$cfgServers[1]['host'] = 'localhost'
```

autentifikační metodu pro přístup k MysSQL cookie

```
//$cfg['Servers'][$i]['auth_type'] = 'cookie'
```

způsob připojení k MySQL

```
$cfgServers[1]['connect_type'] = 'tcp'
```

Upravíme konfiguraci PHP pro použití Cacti editací souboru `/etc/php.ini`. Přidáme zde cestu rozšiřujících direktiv pro PHP `extension_dir = /etc/php.d` .

V souboru `/etc/php.d/mysql.ini` aktivujeme rozšíření pro protokol SNMP přidáním řádku `extension=snmp.so` .

Posledním krokem v konfiguraci serveru před samotnou instalací Cacti bude vytvoření hesla pro root uživatele MySQL databáze pomocí příkazu `mysqladmin --user=root password našeheslo`. Aktivaci hesla provedeme příkazem `mysqladmin --user=root --password reload` .
Tím je náš server připraven pro instalaci Cacti.

3.2 Instalace Cacti

Nyní můžeme instalovat monitorovací nástroj Cacti. Pod root uživatelem příkazem `apt-get install cacti` stáhneme a nainstalujeme ze zrcadla Debianu instalační balík obsahující mimo samotného Cacti balíky Perlu, RRDTool a knihovny. V průběhu instalace budeme dotazováni na hesla k MySQL databázi a PHP. Dále se nás instalační skript dotáže, který z detekovaných webových serverů chceme automaticky nakonfigurovat pro Cacti. Zde zvolíme Apache2, jenž je součástí distribuce Debianu Etch. Instalační skript zapíše uživatelskou konfiguraci Apache pro Cacti v souboru `/etc/apache2/httpd.conf`.

Provedeme konfiguraci pro první spuštění, skládající se z následujících kroků:

1. Vytvoříme v MySQL defaultní databázi Cacti příkazem `mysql cacti < cacti.sql`
2. Nastavíme oprávnění pro uživatele Cacti v MySQL.

   Příkazem `mysql --user=root mysql` se připojíme k MySQL jako uživatel root. Příkazy `GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY 'našeheslo';` a `flush privileges;` nastavíme oprávnění na databázi Cacti.
3. Upřesníme v souboru `cacti/include/config.php` uživatele, heslo a databázi pro Cacti uživatele

   ```
   $database_default = "cacti";
   $database_hostname = "localhost";
   $database_username = "cactiuser";
   $database_password = "našeheslo";
   ```
4. Nastavíme patřičné oprávnění na adresáře Cacti pro generování grafů a logů příkazem `chown -R cactiuser rra/log/ .`
5. Alokujeme dostatečné množství paměti pro běh Cacti. Cacti je sadou PHP skriptů, pro něž tedy vyčleníme 128MB paměti nastavením v řádku konfiguračního souboru `/etc/php.ini`

   ```
   memory_limit=128m
   ```

3.2.1 Instalace pluginů Architecture, Discovery, Thold a Weathermap

Cacti v základní instalaci poskytuje statistiky v podobě grafů a monitoring stavů ONLINE-OFFLINE jednotlivých aktivních prvků sítě. Pro opravdu komplexní monitoring sítě je nezbytné instalovat další pluginy, které rozšiřují možnosti Cacti. Pro instalaci pluginů Cacti vyžaduje mít instalován nejdříve základní plugin Architecture. Prostředí Cacti je dostatečně uživatelsky příjemně navrženo pro integraci jiných pluginů s malým množstvím nezbytně nutných modifikací systému pro jejich použití.

3.2.1.1 Plugin Architecture,

Integruje do Cacti standardní architekturu, která nám dovoluje vytvořit a integrovat další rozšiřující moduly bez potřeby modifikovat naši stávající instalaci Cacti.

Ze stránek projektu Cacti stáhneme plugin Architecture a rozbalíme jej do adresáře `cacti-plugin-arch`. V tomto adresáři spustíme z bashe příkazy `patch -p1 -N --dry-run < cacti-plugin-arch.diff` a `patch -p1 -N < cacti-plugin-arch.diff`. Tím dojde ke konfiguraci databáze Cacti pro plugin Architecture.

Nyní upravíme konfiguraci pro Cacti editací konfiguračního souboru `/usr/share/cacti/site/include/global.php`.

Zde upravíme řádky pro cesty, uživatele, heslo a port

```
$config['url_path'] = "/cacti/";
#$database_default = "cacti";
#$database_hostname = "localhost";
#$database_username = "cacti";
#$database_password = "cacti_my";
#$database_port = "3306";
require('/etc/cacti/debian.php');
#include($config["library_path"] . "/adodb/adodb.inc.php");
include("/usr/share/php/adodb/adodb.inc.php");
```

Příkazem z bashe `cat pa.sql | mysql -u root -p cacti` naimportujeme do databáze MySQL plugin Architecture. Tím je instalace a konfigurace pluginu kompletní.

3.2.1.2 Plugin Thold Discovery a Weathermap

Thold poskytuje možnost nastavovat a sledovat prahové hodnoty sledovaných prvků v síti. Při překročení defininovaných hodnot je Cacti schopno poslat upozorňující e-mail s grafickým zobrazením porušení stanovených podmínek.

Discovery plugin prochází celou síť i se subnety a detekuje na nalezených aktivních prvcích podporu SNMP protokolu. Nalezené zařízení je možno v záložce Discovery přidat do seznamu Hostů.

Weathermap přináší do Cacti možnost kreslit a zobrazovat mapy sítě s aktivními prvky. Na mapách lze sledovat aktuální stav sítě, tj. vytížení jednotlivých spojů, přístupových bodů, serverů a dalších síťových prvků. Data pro zobrazení provozu jsou zobrazována ve formě přehledných grafů.

Instalace a základní konfigurace uvedených pluginů je velmi snadná. Provedeme ji najednou stažením souborů `thold-0.3.9.zip`, `php-weathermap-0.95b.zip` a `discovery-0.8.4.tar.gz` ze stránek projektu Cacti, rozbalíme do adresáře s pluginy `/var/www/cacti/plugins/`.

Upravíme konfigurační soubor Cacti `/usr/share/cacti/site/include/global.php` přidáním řádků

```
$plugins = array();
$plugins[] = 'thold';
$plugins[] = 'discovery';
$plugins[] = 'weathermap';
```

Nastavíme pro plugin Weathermap PHP editor map. V konfiguračním souboru editoru `/usr/share/cacti/site/plugins/editor-config.php` upravíme cesty

```
$cacti_base = "/usr/share/cacti/site";
$cacti_url = "http://monitor.slfree.net/cacti/";
```

Přidáme oprávnění web serveru do adresářů s konfigurací a výstupy Weathermapu příkazem z bashe

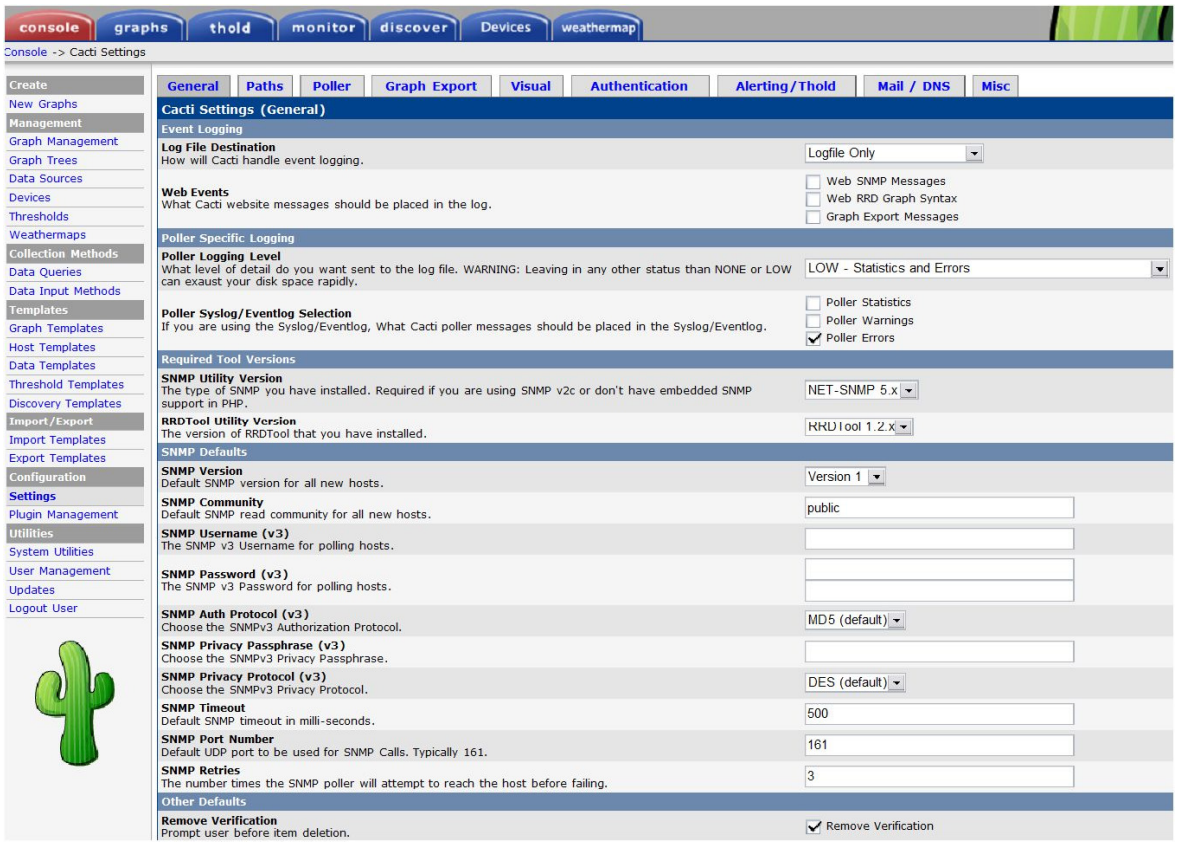
```
chown www-data.www-data configs -R
chown www-data.www-data output -R
```

Vytvoříme databázi pro Discovery. V adresáři s pluginy spustíme z bashe import databáze do MySQL příkazem `mysql cacti < discover.sql`.

Tím jsme provedli instalaci a základní konfiguraci nutnou pro spuštění Cacti a jeho pluginů. Dílčí konfigurace a samotné nastavování monitoringu budeme provádět z grafického rozhraní Cacti.

3.3 Konfigurace Cacti v grafickém rozhraní

Zadáním adresy monitor.slfree.net/cacti/ do webového prohlížeče se přihlásíme do Cacti, kde budeme provádět podrobnou a kompletní konfiguraci pro monitoring komunitní sítě slfree.net.



Obr.7. *Grafické administrační rozhraní Cacti*

Pro první přihlášení použijeme jako uživatelské jméno admin a heslo necháme prázdné. Z bezpečnostního nastavení budeme následně vyzváni ke změně hesla.

Vlastní grafické rozhraní se skládá ze záložek Graph a Devices samotného Cacti, záložek Thold a Monitor jenž jsou součástí pluginu Thold, záložky Discovery pluginu a záložky pluginu Weathermap.

Tyto záložky zobrazující výstupy z uvedených pluginů.

3.3.1 Základní konfigurace monitoru Cacti

Základní nastavením systému provedeme v konfiguraci `Configuration/Settings` a to v jednotlivých záložkách nastavením patřičných parametrů.

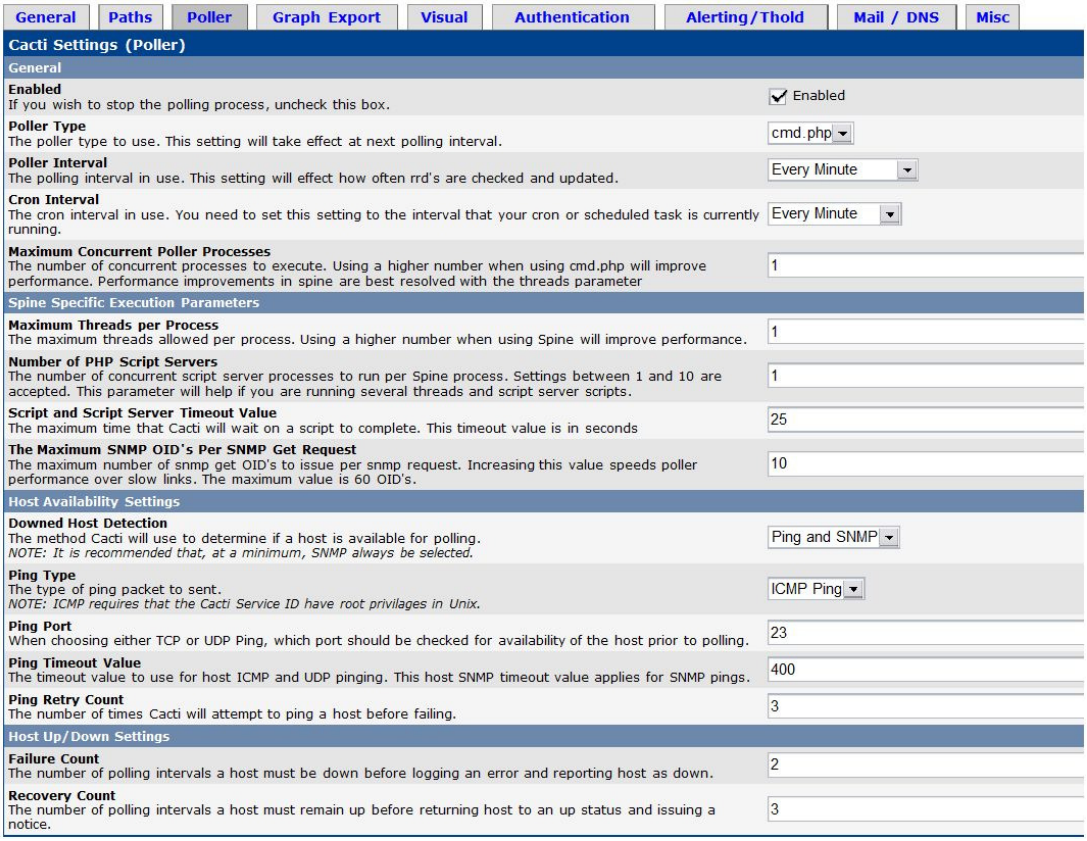
3.3.1.1 General

Zde se nachází obecné nastavení Cacti. Nastavíme logování `Log only`, velikost logu omezíme zvolením Poller Logging levelu na `Low-statistics and Errors`. Zaznamenávat do logu budeme i samotné chyby Polleru, zatrhneme proto pole Poller errors.

V Required Tool Version zvolíme NET-SNMP 5.x a RRDTool utility version 1.2.x. Jedná se o nástroje nutné pro běh, které obsahovala instalace Cacti.

SNMP Defaults vybereme verzi protokolu SNMPv1 používanou v síti převážnou většinou routerů. Používat budeme community string PUBLIC, který je taktéž nastaven v jednotlivých routerech a serverech. Ostatní nastavení ponecháme na defaultních hodnotách.

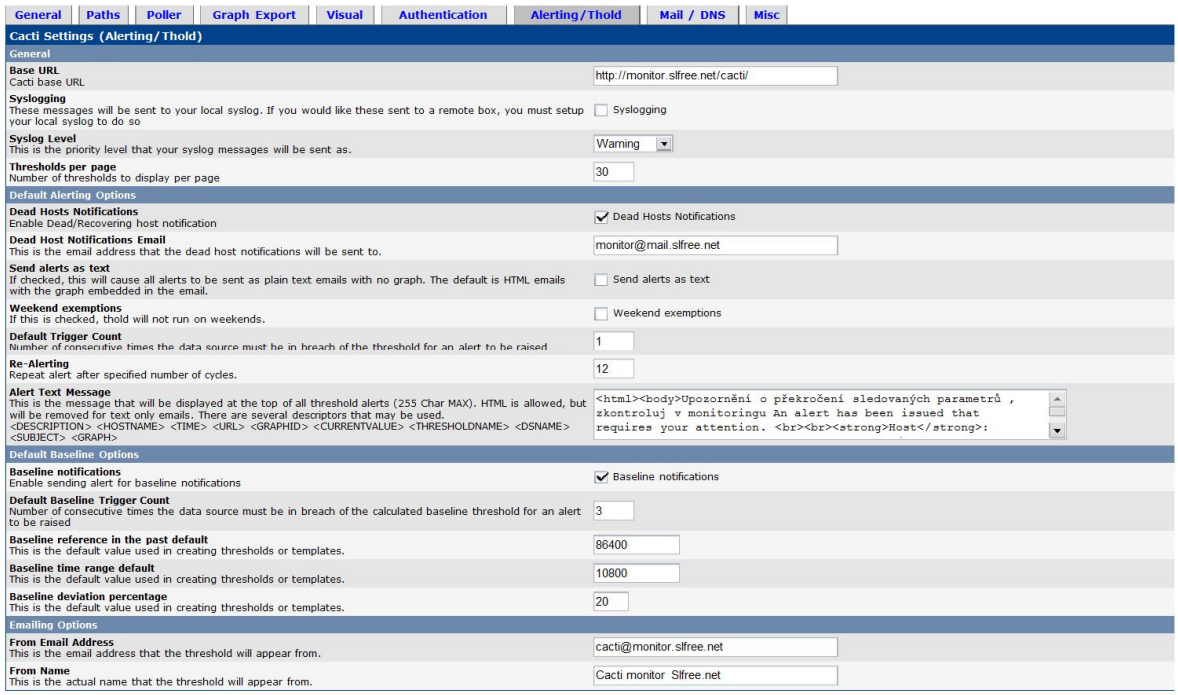
3.3.1.2 Poller



Obr.8. *Grafické administrační rozhraní Cacti - Poller*

Poller je modul zajišťující spouštění dotazových skriptů na zařízení definovaná v monitoringu. Cacti obsahuje PHP Poller `cmd.php` a `spine`, který je naprogramován v jazyce C. Spouští defaultně každých minutu sadu skriptů načítající ze zařízení pomocí RRDToolu SNMP informace o sledovaných prvcích. Poller zvolíme `cmd.php`. Spouštění Polleru zajištuje v linuxu modul Cron , nastavíme jej taktéž na 1 minutu.

3.3.1.3 Alerting/Thold



Obr.9. *Nastavení pluginu Thold*

Záložka Alerting/Thold slouží pro nastavení upozorňování pluginu Thold. Nastavíme zde jednak informace, které budou uváděny v upozorňovacím mailu, a také parametry základního monitoringu. *Base URL* nastavíme adresu `http://monitor.slfree.net/cacti/`. Z ní budou vycházet veškeré odkazy zasílané v upozorňovacích mailech.

U všech zařízení budeme chtít oznamovat stav nedostupnosti, zvolíme možnost Dead Host Notification a zadáme adresu `monitor@mail.slfree.net`, ze které budou emaily odesílány.

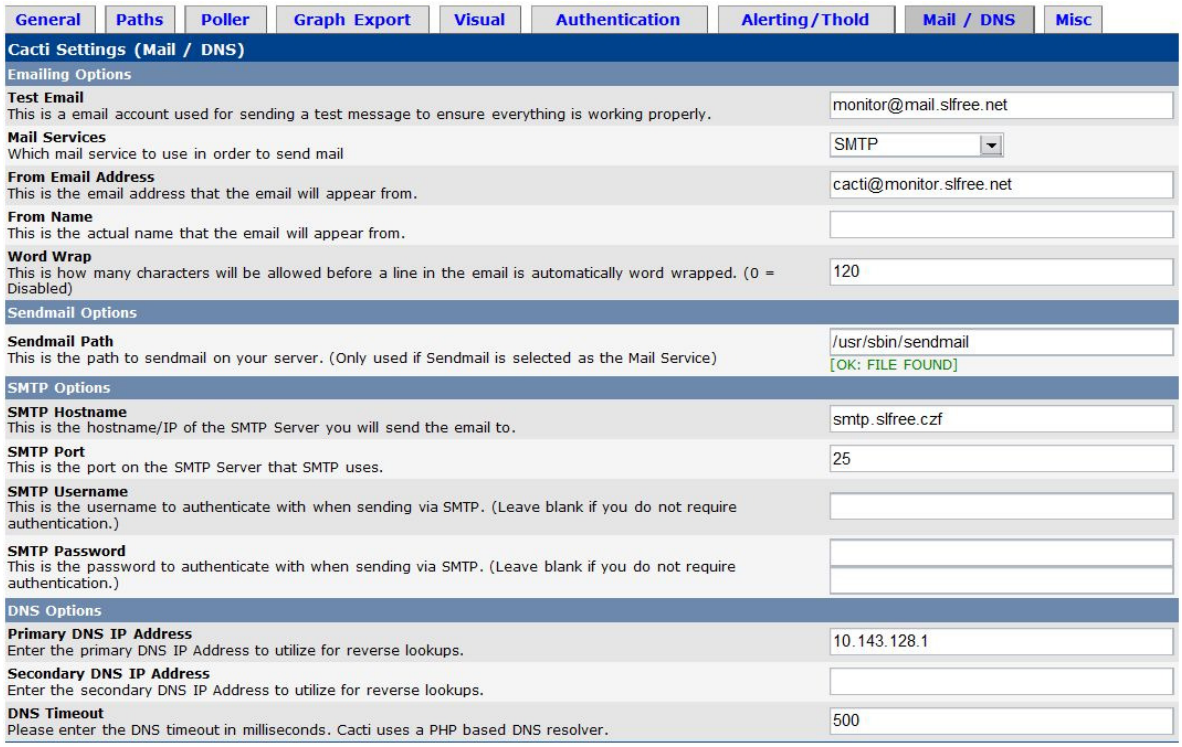
Default Baseline Options slouží pro obecné nastavení chování spouštění alertů u všech zařízení. Toto nastavení využívají šablony Thresholdu jako defaultní. *Default Baseline Trigger count* udává počet porušení sledovaných prahových hodnot u nějakého zařízení. Nastavením hodnoty 3 určíme, že má být zasláno či notifikováno upozornění na nějaký stav až po třech po sobě jdoucích zjištěných porušení hlídaných provozních hodnot zařízení či služby.

Baseline reference in the past default nastavíme na hodnotu 86400 (1 den), což je hodnota ve vteřinách, určující celkovou denní časovou periodu sledování definovaného zařízení.

Baseline time range default nastavíme na hodnotu 10800. Určuje dobu ve vteřinách, která slouží k zpětnému porovnávání získaných hodnot.

Baseline deviation percentage určuje toleranci v procentech u sledovaných hodnot. Nastavíme na hodnotu 20, tím omezíme případné prudké výkyvy.

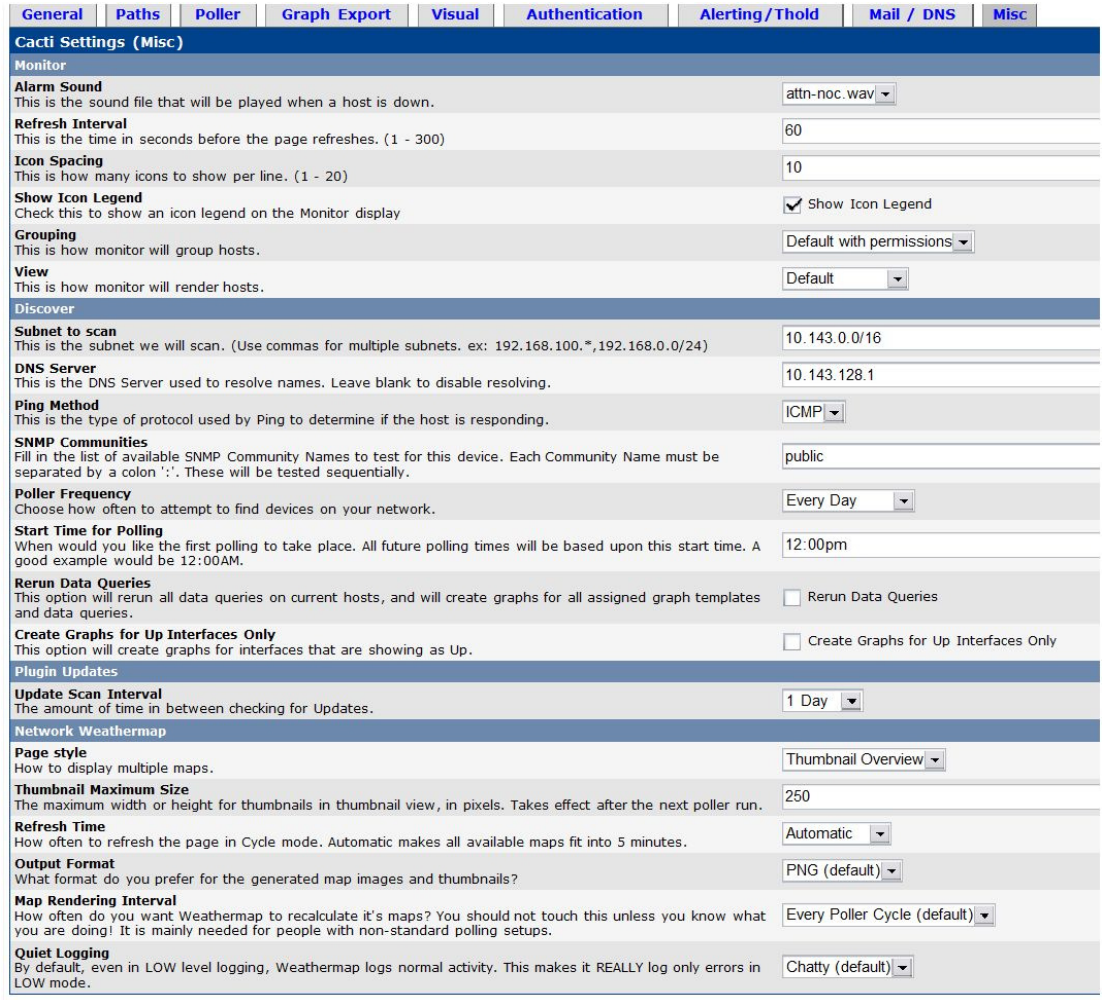
3.3.1.4 Mail/DNS



Obr.10. *Nastavení pluginu Thold –Mail/DNS*

Zde zadáme mailový server komunitní sítě slfree.net, jeho port a server DNS. Zvolíme mailovou službu pro testovací e-maily `SMTP`.

3.3.1.5 Ostatní nastavení - Misc



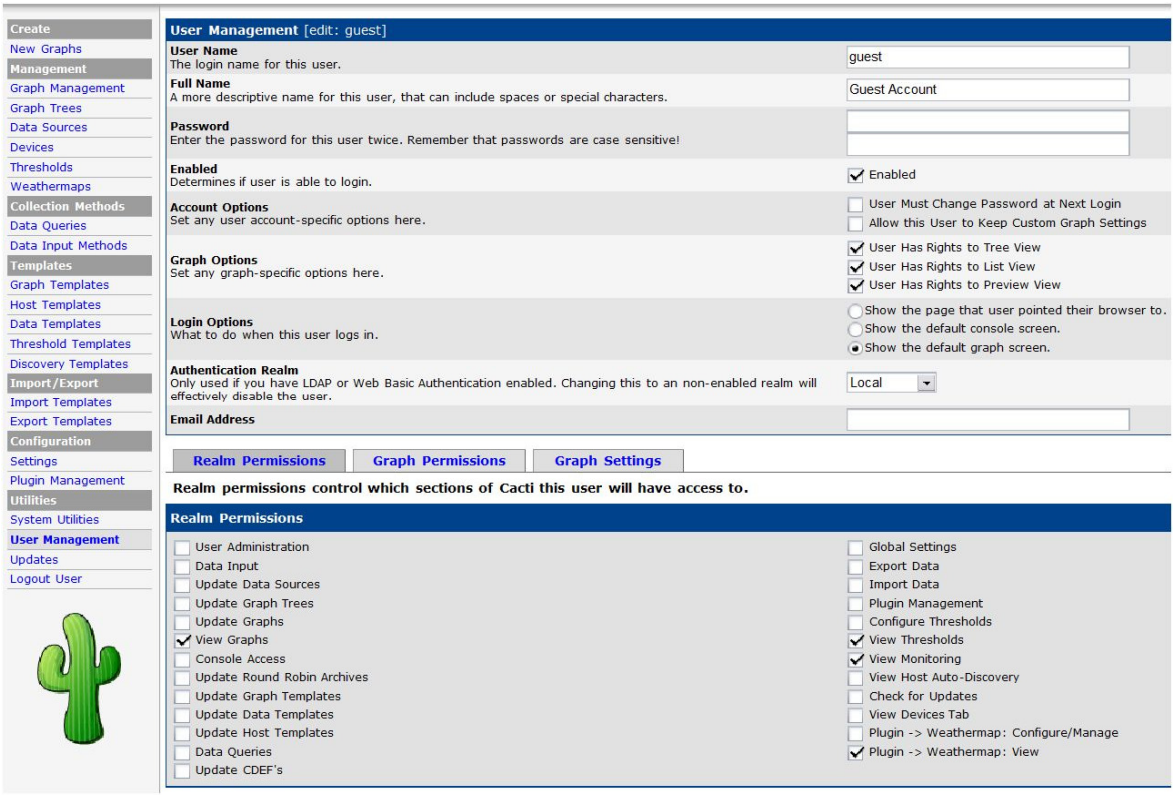
Obr.11. *Ostatní nastavení*

Tato záložka slouží především k nastavení pluginu Discover. *Subnet to scan 10.143.0.0/16* určuje celý adresní rozsah slfree.net k vyhledávání zařízení podporující SNMP protokol. Opět nastavíme *SMNP community* na `public`, dobu spouštění prohledávání na `Every Day`.

Záložky Paths, Graph export,Visual Authentication ponecháme v defaultním nastavení.

3.3.2 Správa uživatelů – User Management

Cacti poskytuje jednoduchou a přehlednou správu uživatelů, přistupujícím k systému. Při přístupu ke grafickým statistikám Cacti pomocí internetové adresy monitor.slfree.net/cacti/graph_view.php je použit účet uživatele host.



Obr.12. *Účet hosta*

Pro správnou funkci přehledů statistik monitoru je potřeba u účtu hosta nastavit oprávnění jen na ty části systému, které slouží k zobrazování výstupů Cacti a jeho pluginů. Povolíme tedy pouze položky *View Graphs, View Thresholds, View Monitoring a Plugin -> Weathermap View.*

V záložce *Graph Permisions* povolíme uživateli host volbou `Allow` prohlížení všech vytvořených grafů a jejich zobrazení ve stromových strukturách. Stromovou strukturu sítě slfree.net budeme později vytvářet v kapitole Monitoringu.

Ve Správě uživatelů lze vytvářet libovolné uživatele a přiřazovat jim rozličné oprávnění. Pro účely zasílání zpráv musíme vytvořit správcovské uživatele, kteří budou informování

formou e-mailu o výpadcích či jiných definovaných stavech na zvolených zařízeních. U každého správcovského účtu proto vyplníme platný e-mail a to na kartě správce v položce *Email address.*

Nyní je Cacti nastaveno a připraveno pro vkládání uživatelských dat sítě slfree.net.

4 MONITORING

Monitoring sítě v Cacti a obecně ve všech monitorovacích systémech se dá obecně shrnout do následujících bodů:

- Vložení údajů o monitorovaných prvcích
- Nastavení prahových hodnot pro detekci poruchových stavů
- Sledování provozu sítě a analýza poruchových stavů

Vložení zařízení a jejich parametrů probíhá pomocí uživatelsky definovaných šablon Host Template, která obsahuje šablony Thresold Template, Data Templates, Graph Template, dále metody získávání dat pomocí skriptů Data Queries a Data Input Methods . Získávání, zpracování a zobrazení dat pro monitoring probíhá skrze tyto šablony.

Šablona Thresold Template slouží k nastavování prahových hodnot a notifikaci při jejich porušení.

Šablona Data Queries obsahuje dotazy SMNP, pomocí kterých jsou získáván data ze zařízení v pravidelných časových intervalech. Tato data jsou dále zpracovávána šablonou Data Templates, kde je možno editovat nastavení všech možných dotazů šablony Data Queries.

Šablona Graph Template obsahuje dílčí šablony sloužící k sestavování grafů a statistik ze získaných a zpracovaných dat pomocí šablon Data Queries a Data Templates.

4.1 Vložení údajů o monitorovaných prvcích sítě

V Cacti se vkládá každé jednotlivé monitorované zařízení do celkového seznamu zařízení Devices prostřednictvím připravených datových nebo Host šablon vytvořených pro nejčastěji používaná zařízení, operační systémy a služby. Lze importovat nové datové šablony pro zařízení jiných výrobců nebo vytvářet své vlastní. To je případ pro linuxové routery s operačním systémem Mikrotik RouterOS 2.9.x-3.7 používané v komunitní síti slfree.net. Nejdříve tedy importujeme Host šablonu Mikrotiku. Importem vzniknou zároveň

šablony pro grafy Graph Template, dotazy Data Querie, data Data Template a upozorňování (alerty) Threshold Template.

4.1.1 Import šablon pro zařízení s OS Mikrotik

Import šablony se skládá ze dvou kroků, a to nakopírováním jednotlivých skriptů do adresáře Cacti, a následně pomocí Importu v grafickém rozhraní nahráním dílčí šablony do skupiny šablon s označením Mikrotik Templates.

Importovat budeme šablonu Mikrotik Host Template obsahující šablonu Data Queries se SMPT dotazy pro:

- Mikrotik Wireless Interfaces
- Mikrotik Queue Simple
- Mikrotik Queue Tree
- Mikrotik Wireless Client
- Host CPU
- Host Disk
- Host Memory
- Host Uptime

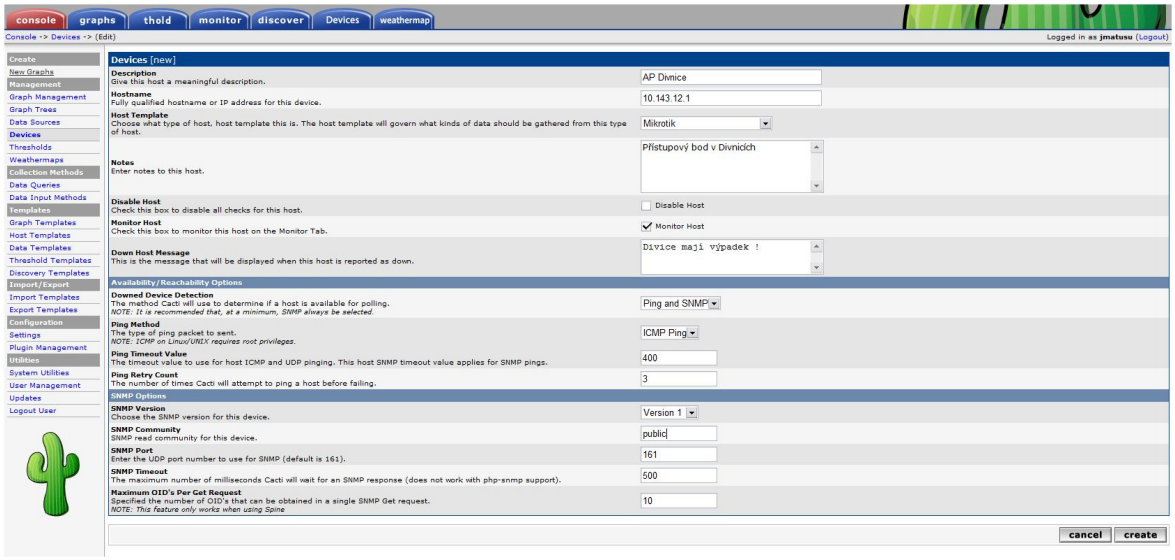
Šablony Mikrotiku Data Templates obsahují názvy systémových prostředků Mikrotiku, MIB tabulku včetně všech OID čísel.

Postup importu šablony Mikrotik Host Template:

1. stáhneme ze stánek projektu Cacti soubor se šablonami Mikrotiku `cacti_mikrotik_template.zip`
2. rozbalíme a nakopírujeme soubory do adresáře `/var/www/cacti/resource/`
3. v grafickém rozhraní Cacti přes volbu Import zadáme cestu s hlavní šablonou `var\www\cacti\resource\cacti_host_template_mikrotik.xml` a provedeme import

Tím jsme vytvořili novou šablonu Mikrotik v Host Templates, která je připravena k použití.

4.1.2 Vložení zařízení – Devices



Obr.13. *Device AP Divnice*

Každé zařízení Host nebo rozhraní je nutno zadávat pomocí Devices. V této sekci zvolíme *Add* , následně ve formuláři zařízení uvedeme název AP Divnice, *Hostname* jeho IP adresu 10.143.12.1, vybereme pro zařízení s OS Mikrotik šablonu *Host Template* `Mikrotik`, ve volbě pro dostupnost `PING and SNMP`. Ve volbách pro SNMP zvolíme verzi protokolu v.1 a community string `public`.

Tím jsme vytvořili zařízení AP Divnice v seznamu Devices. Pro toto zařízení vytvoříme dotazy Data Queries , datové zdroje Data Sources a jejich grafy.

Volbou šablony *Host Template Mikrotik* u AP Divnice jsme k tomuto zařízení asociovali šablony grafů:

- IP routes, PPP Active

- Queue - Simple traffic,
- System - CPU Load, Memory Usage, System–Uptime
- Wireless - Data Rates, Wireless Signal Strengh

a šablony datových dotazů:

- Queue Simple, Queue Tree
- Wireless - Registration Table, Client
- SMNP - Interface Statistics

Z roletového menu lze přidat další typy šablon a dotazů.

Nyní pro toto AP vytvoříme Datové zdroje a jejich grafy jenž nám poskytuje šablona Mikrotik Template. V seznamu zařízení Devices otevřeme AP Divnice, zvolíme položku Create Graphs for this Host.

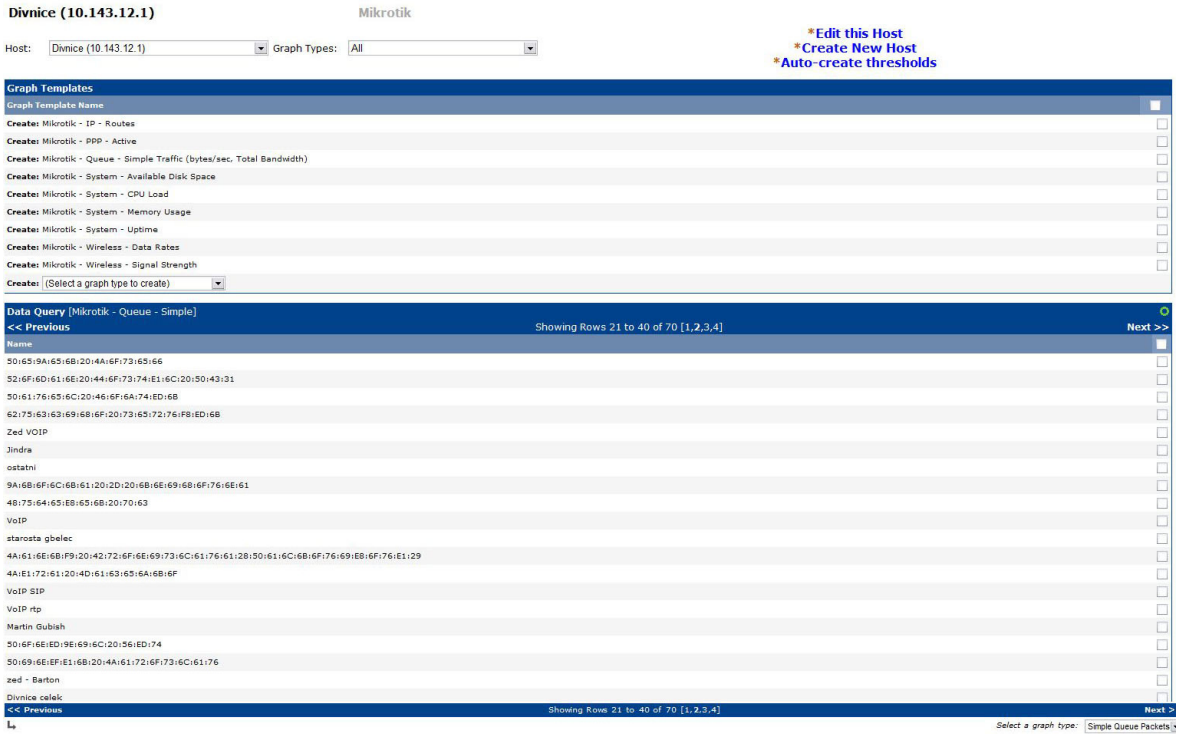
Data Query obsahuje prostředky k monitoringu, které jsme zvolil volbou šablony Mikrotik Queue Simple, Wireless-Client, Wireless-Registration Table a SNMP Interface Statistics při tvorbě zařízení AP Divnice. Nyní zvolíme z nabízených Data Sources a Data Queries požadované zdroje a volbou Create vytvoříme grafy (Obr. 13 a 14).

4.1.2.1 Šablona Mikrotik Simple Queue

Simple Queue označuje v OS Mikrotik strukturu HTB. V případě AP Divnice je zde vytvořena hlavní rodičovská třída *Divnice celek*. Rodič *Divnice celek* obsahuje jednotlivé potomky, což jsou jednotlivý klienti (jejich síťové zařízení) na přístupovém bodu s vyhrazenými částmi přenosového pásma. Součet dílčích pásem všech potomků je roven přenosovému pásmu jejich rodiče. Tím je zaručeno spravedlivé přidělování rychlosti všem klientům i při maximálním vytížení přístupového bodu.

Ze tabulky Simple Queues přístupového bodu AP Divnice (Obr.14) zvolíme pro tvorbu datových zdrojů a veřejných grafů rodiče *Divnice celek* a potomka *ostatni.* Z rolovacího

menu můžeme vybrat typ dat. Na výběr máme *Simple Queue Traffic* nebo *Simple Queue Packets.*



Obr.14. *Datové zdroje zařízení AP Divnice*

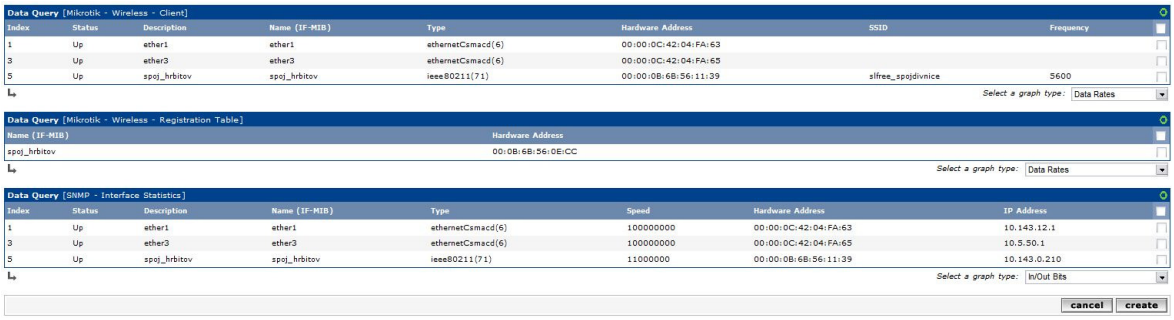
4.1.2.2 Šablona Mikrotik- Wireless Client, Wireless Registration Table

Wireless Client obsahuje seznam fyzických síťových rozhraní instalována v routerboardu AP Divnice. Rozhraní zde tvoří bezdrátová miniPCI kara Atheros CM9 sloužící jako síťové rozhraní spoje *spoj_hrbitov* a interní ethernetové rozhraní *ether1*.Obě rozhraní zvolíme pro vytvoření grafů a zdrojů dat. Z roletového menu můžeme volit *Data Rates, Signal Strengh* nebo *Frequency 802.11 a,b,g*.

Wireless Registration Tables obsahuje seznam zařízení v tabulce povolených bezdrátových klientů a spojů. V případě AP Divnice bohužel neobsahuje žádná klientská zařízení, protože AP Divnice slouží pouze jako přístupový bod s jedním bezdrátovým přijímacím/vysílacím rozhraním. Připojení klientů k tomuto AP je řešeno dvěma

samostatnými bezdrátovými body v obci. Tyto body jsou metalickým vedením připojeny k rozhraní *ether1*. Vybereme tedy k tvorbě grafu datových zdrojů jediné bezdrátové zařízení a to *spoj_hrbitov*.

Ovšem u ostatních přístupových bodů, které budeme taktéž vkládat do Cacti, *Wireless Registration Tables* obsahují seznam registrovaných klientských zařízení. V tomto seznamu lze najít informace o síle signálu připojeného klientského zařízení, jeho aktuální přenosovou rychlost a datový tok.



Obr.15. *Datové zdroje zařízení AP Divnice*

Tím jsme vytvořili zařízení v Devices AP Divnice, jeho příslušné datové zdroje v Data Sources a grafy datových zdrojů.

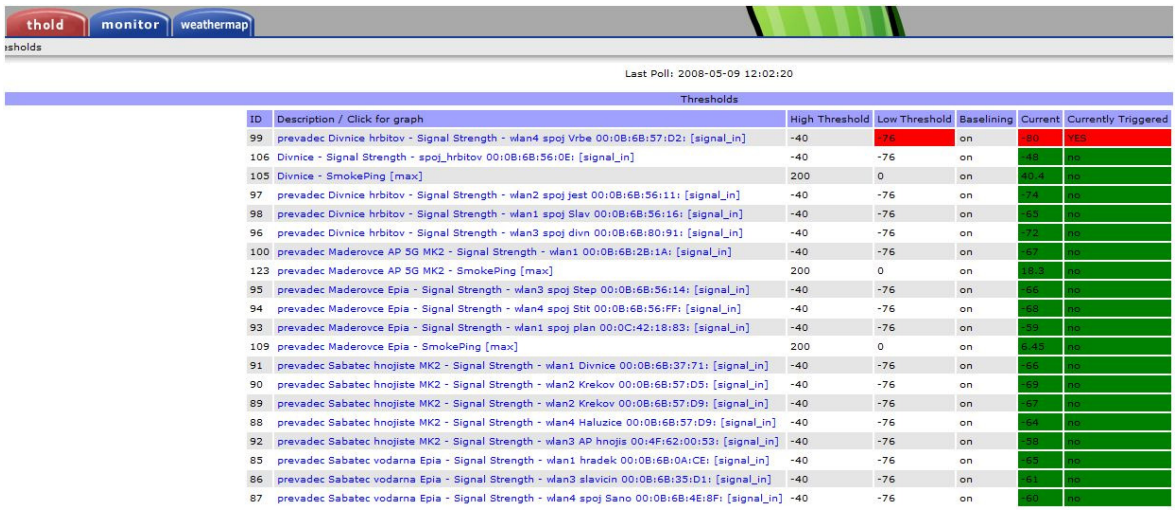
Uvedený postup tvorby Hosta zopakujeme pro všechna zařízení v síti slfree.net podle následující tabulky.

Tab. 1. IP adresy zařízení s OS Mikrotik používaných v síti slfree.net

Hostname	Description	Hostname	Description
10.143.54.1	bohuslavice	10.143.80.1	Slavicin radnice
10.143.60.1	Brumov-Centrum	10.143.6.1	Slavicin Sabatec
10.143.99.1	brumov družba	10.143.51.1	Slavicin Stefanik
10.143.68.1	brumov kulturak	10.143.23.1	Slavicin Valenta
10.143.69.1	brumov Snehurka	10.143.10.1	Slavicin Vlara
10.143.59.1	Bylnice DD	10.143.86.1	Slavicin Vlara U lesa
10.143.91.1	Divnice Army park	10.143.1.1	Slavicin Vypusta
10.143.38.1	Dolni Lhota	10.143.100.1	Slavicin optika
10.143.40.1	Haluzice	10.143.33.1	Slopne komin
10.143.94.1	Hostetin sloup	10.143.32.1	Slopne sokolovna
10.143.16.1	Hradek bytovka	10.143.72.1	Stitna
10.143.52.1	Jestrabi	10.143.96.1	Stitna Zahumeni
10.143.74.1	Krekov	10.143.56.1	Sv. Stepan
10.143.78.1	Lipina	10.143.57.1	Sv. Stepan Mostatni
10.143.88.1	Lipova	10.143.64.1	Vlachovice bytovka
10.143.43.1	Loucka DD	10.143.62.1	Vrbetice
10.143.128.13	prevadec Maderovce Epia	10.143.65.1	Vrbetice dedina
10.143.92.1	Sanov hasicarna	10.143.0.18	Nevsova bytovky
10.143.93.1	Sanov škola	10.143.18.193	Nevsova ctvrte
10.143.45.1	Sanov vlek	10.143.19.129	Nevsova Horni konec
10.143.34.1	Sehradice	10.143.0.17	Nevsova Myslivecka chata
10.143.35.1	Sehradice komin	10.143.19.1	Nevsova stara škola
10.143.17.1	Slavicin Agrinea	10.143.48.1	Petruvka Maca
10.143.85.1	Slavicin Agrol	10.143.47.1	Petruvka Urad
10.143.84.1	Slavicin hnojiste	10.143.48.255	Petruvka prevadec Rudimov
10.143.82.1	Slavicin Luksin	10.143.114.1	Pitin škola
10.143.8.1	Slavicin Mir	10.143.115.1	Pitin sloup
10.143.4.1	Slavicin Mladoticka Unart	10.143.66.1	Preckovice
10.143.111.1	Slavicin Mladoticka 5GHz	10.143.0.209	prevadec Divnice
10.143.25.1	Slavicin panelaky3	10.143.128.14	prevadec Hnojiste 5GHz
10.143.112.1	Slavicin panelaky 482-484	10.143.0.3	prevades Sabatec Epia

4.2 Plugin Thold

Plugin Thold, jak již bylo zmíněno, dovoluje nastavit u jednotlivých rozhraní prahové hodnoty, tzv. Thresholdy, při jejichž překročení budeme informování jednak vizuálně v záložce Thold a Monitor a taky zasláním e-mailu.



ID	Description / Click for graph	High Threshold	Low Threshold	Baselining	Current	Currently Triggered
99	prevadec Divnice hrbitov - Signal Strength - wlan4 spoj Vrbe 00:0B:6B:57:D2: [signal_in]	-40	-76	on	-80	YES
106	Divnice - Signal Strength - spoj_hrbitov 00:0B:6B:56:0E: [signal_in]	-40	-76	on	-48	no
105	Divnice - SmokePing [max]	200	0	on	40.4	no
97	prevadec Divnice hrbitov - Signal Strength - wlan2 spoj jest 00:0B:6B:56:11: [signal_in]	-40	-76	on	-74	no
98	prevadec Divnice hrbitov - Signal Strength - wlan1 spoj Slav 00:0B:6B:56:16: [signal_in]	-40	-76	on	-65	no
96	prevadec Divnice hrbitov - Signal Strength - wlan3 spoj divn 00:0B:6B:80:91: [signal_in]	-40	-76	on	-72	no
100	prevadec Maderovce AP 5G MK2 - Signal Strength - wlan1 00:0B:6B:2B:1A: [signal_in]	-40	-76	on	-67	no
123	prevadec Maderovce AP 5G MK2 - SmokePing [max]	200	0	on	18.3	no
95	prevadec Maderovce Epia - Signal Strength - wlan3 spoj Step 00:0B:6B:56:14: [signal_in]	-40	-76	on	-66	no
94	prevadec Maderovce Epia - Signal Strength - wlan4 spoj Stit 00:0B:6B:56:FF: [signal_in]	-40	-76	on	-68	no
93	prevadec Maderovce Epia - Signal Strength - wlan1 spoj plan 00:0C:42:18:83: [signal_in]	-40	-76	on	-59	no
109	prevadec Maderovce Epia - SmokePing [max]	200	0	on	6.45	no
91	prevadec Sabatec hnojiste MK2 - Signal Strength - wlan1 Divnice 00:0B:6B:37:71: [signal_in]	-40	-76	on	-66	no
90	prevadec Sabatec hnojiste MK2 - Signal Strength - wlan2 Krekov 00:0B:6B:57:D5: [signal_in]	-40	-76	on	-69	no
89	prevadec Sabatec hnojiste MK2 - Signal Strength - wlan2 Krekov 00:0B:6B:57:D9: [signal_in]	-40	-76	on	-67	no
88	prevadec Sabatec hnojiste MK2 - Signal Strength - wlan4 Haluzice 00:0B:6B:57:D9: [signal_in]	-40	-76	on	-64	no
92	prevadec Sabatec hnojiste MK2 - Signal Strength - wlan3 AP hnojis 00:4F:62:00:53: [signal_in]	-40	-76	on	-58	no
85	prevadec Sabatec vodarna Epia - Signal Strength - wlan1 hradek 00:0B:6B:0A:CE: [signal_in]	-40	-76	on	-65	no
86	prevadec Sabatec vodarna Epia - Signal Strength - wlan3 slavicin 00:0B:6B:35:D1: [signal_in]	-40	-76	on	-61	no
87	prevadec Sabatec vodarna Epia - Signal Strength - wlan4 spoj Sano 00:0B:6B:4E:8F: [signal_in]	-40	-76	on	-60	no

Obr.16. *Záložka Thold*

Upozornění pomocí Thresholdů bude automaticky zasílano těm uživatelům, kteří mají nastaven ve svém profilu e-mail a povolenou volbu *Email Notification*.

Při zadávání Hostů jsme volili u každého možnost *Monitor Host*. Toto nastavení znamená, že v záložce Monitor vidíme tato zařízení a jejich aktuální stav.

Obr.17. *Záložka Monitor*

Přidržením kurzoru myši na kterémkoliv zařízení se zobrazí základní informace jako IP adresa, průměrný ping a poslední výpadek a dostupnost zařízení. Thresholdy budeme převážně nastavovat jen u páteřních routerů a problémových zařízení, jejichž stav chceme hlídat. U páteřních routerů budeme hlídat sílu signálu jednotlivých bezdrátových rozhraních, pokud klesne hodnota pod námi definovanou minimální úroveň -75dBm, budeme na tento stav upozorněni. Vzhledem k tomu, že ve wifi pásmech je počet kanálů omezen, můžeme předpokládat, že spoj je zarušen například špatně nastaveným spojem cizího zařízení.

4.2.1 Vytvoření a nastavení Thresholdů Hosta

Provedeme nastavení Thresholdů síly signálu a ztrátovosti PING paketů na rozhraních u zařízení převaděče Divnice hřbitov. Nejprve je nutno určit, jaké Thresholdy chceme použít z již existujících šablon v *Thresold Templates*. Zkontrolujeme, zda *Threshold Templates* obsahují šablony *Mikrotik-WirelessRegTable Signal Strengh* a *Unix- SmokePingLike* a přidáme pokud chybí. Otevřeme v seznamu zařízení Device *prevadec Divnice hrbitov*. Na kartě zařízení vidíme seznam asociovaných grafů a datových dotazů *Data Querie* ze šablony Host Template Mikrotik. Přidáme zde šablonu pro graf pingu *SmokePingLike*. Odkazem *Create graph for this* Host vytvoříme této šabloně graf. Zvolíme *Auto create-*

Thresholds. Tím se vytvoří Thresholdy podle šablony Mikrotik *Threshold Template* a SmoothLikePing *Threshold Template ,* které se nám objeví v záložce Thold.

Převaděč Divnice hřbitov obsahuje 1 hlavní spoj pro směr Slavičín a celkem 3 spoje na další přístupové body. Bude nutno upravit parametry vytvořených Thresholdů tak, aby každý jednotlivý Thresold spoje měl nastaven rozsah hlídaného signálu v mezích funkčnosti s ohledem na jeho konstrukční parametry. Tyto meze můžeme vyčíst například z jednotlivých grafů úrovní signálů převaděče Divnice.

Nastavíme v sekci Thresholds pro spoje *wlan1_spojSlavicin*, *wlan2_spojJestrabi* a *wlan3_spojDivnice* hodnoty High Threshold na -40dBm a Low Threshold na -71dBm. Spoj *wlan4_spojVrbetice* nastavíme v krajních mezích funkce spoje a to -40 a -78dBm, protože se jedná spoj na nejdelší vzdálenost se zastíněnou Frenelesovou zónou.

Podobně nastavíme Thresholdy pro ostatní páteřní routery - převaděč Maděrovce a převaděč Šabatec.

Můžeme hlídat hodnoty pingů, přenesených dat jednotlivých členských tříd v HTB na kterýchkoliv zařízení, úroveň signálu klientských zařízení a mnoho dalšího.

4.2.2 Tvorba nových vlastních šablon Host, Data a Graph Template

Jak již bylo řečeno, můžeme tvořit své vlastní šablony pomocí skriptů v jazyce Perl, PHP nebo bashi. Další možností je integrovat dotazy ze stávajících šablon do šablony nové, která bude obsahovat dotazy z několika šablon pro různá zařízení. To se může například hodit, pokud potřebujeme monitorovat u jednoho klientského zařízení jeho provoz v závislosti na provozu jiného zařízení – třeba centrálního routeru.

Můžeme tvořit své vlastní datové šablony k jiným zařízením, pokud známe OID čísla jejich objektů. Každou šablonu tvoří dvojice programový kód v Perlu, bashi nebo PHP s příponou .pl, .sh nebo .php a skript v jazyku XML. Pokud zvládáme uváděné programovací jazyky není problém tvořit své vlastní šablony. Pro naše potřeby monitoringu

budeme používat naiportované šablony, které poskytují vše potřebné pro tvorbu potřebných dotazů, statistik a grafů.

4.2.2.1 Tvorba nových šablon pomocí Importu

Importujeme vždy dvojici skript+kód XML. Programový kód .xml zobrazuje skriptem naměřená a uložená data.

Skript obsahuje příkazy pro získávání měřených dat a kód XML metodiku zpracovávání získaných dat, tj. ukládání do MySQL databáze, výpočetní metody, formu zobrazení v grafech apod.

Provedeme import šablony Graph Template SmothPingLike, která přináší do monitoringu informaci o ztrátovosti paketů Ping Latency. Ze stránek projektu Cacti stáhneme zdrojové kódy šablony s příponami .pl a .xml. Skript v Perlu nakopírujeme do adresáře se skripty */var/www/cacti/skripts/*. Kód .xml pomocí Importu načteme a uložíme.

Nyní se nám v seznamu šablon Graph Template objevila tato nová šablona pod názvem SmothPinkLike v.1.0.

Skript v jazyce Perl:

```
#!/usr/bin/perl
$host = $ARGV[0];
$ping = `/bin/ping -c 10 -n -q $host`;
my ($loss) = ($ping =~ /(\d+)%/g);
my ($one,$rtt) = ($ping =~ /(\d+\.\d+)\//g);
if ($rtt eq ”) {
$rtt = 0;
$loss = 100;
}
print “rtt:$rtt loss:$loss”;
```

4.2.2.2 Tvorba nových šablon integrací stávajících

Další možností jak tvořit vlastní šablony je integrovat stávající šablony s dotazy do nových vlastních šablon. Tato volba je výhodnější pro méně zdatné programátory, kteří chtějí používat jen některá zdrojová data či dotazy a mít je zahrnuta do nové samostatné šablony.

Příklad tvorby a použití šablony Hosta pouze s daty *Ping* a *Simple Queue Traffic* integrací:

V *Host Template* vložíme novou šablonu volbou *ADD.* Do názvu uvedeme *Ping a Traffic Kaluska Josef* a potvrdíme volbou *Create.*. Z asociovaných grafů přidáme *Mikrotik- Simple Queue Traffic, SmothPingLike* a z datových dotazů zvolíme *Mikrotik Queue Simple.*

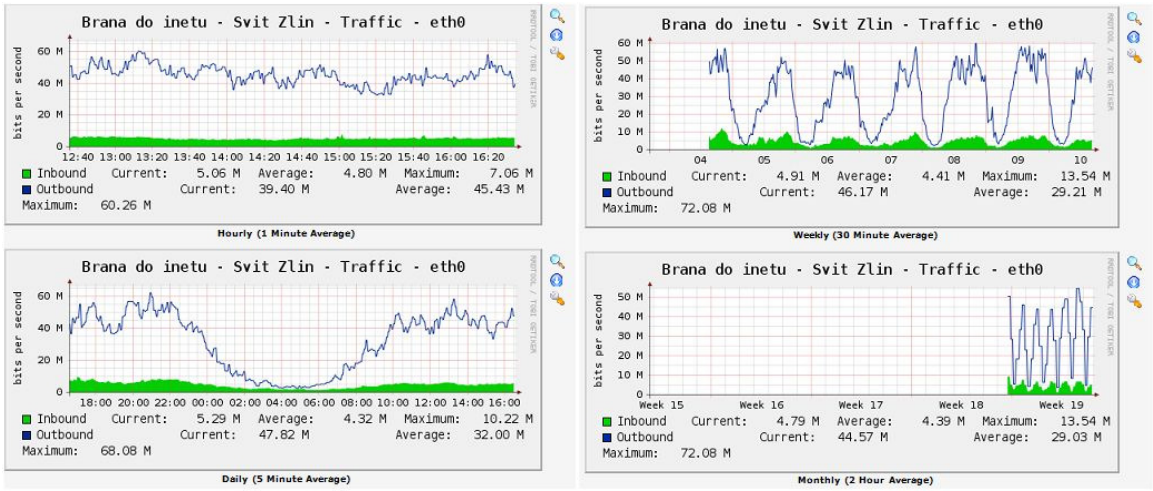
Přejdeme do seznamu zařízení *Devices* kde zvolíme nové. Vybereme šablonu s názvem *Ping a Traffic Kaluska Josef ,* jako ip adresu zadáme *10.143.10.1,* což je adresa přístupového bodu na který je klient připojen. Vytvoříme grafy pouze *SmothPingLike* a *Data Queue Simple – Kaluska Josef.*

Tím jsme definovali zařízení (konkrétního klienta) *v Devices,* u kterého bude zobrazován jen ping a celkový datový tok.

5 VIZUALIZACE

Vizualizace v Cacti se obecně se skládá z grafického přehledu jednotlivých datových zdrojů a z vizualizace provozu sítě ve formě provozních map, zachycující aktuální vytížení sítě. Tyto mapy v Cacti je nutno kreslit ručně, narozdíl od jiných systémů, například Zabbixu, kde je možnost je generovat automaticky podle vložených zařízení a SNMP dat.

V grafech je možno sledovat statistiky provozu i za uplynulá období.



Obr.18. *Grafy*

5.1 Graph Management

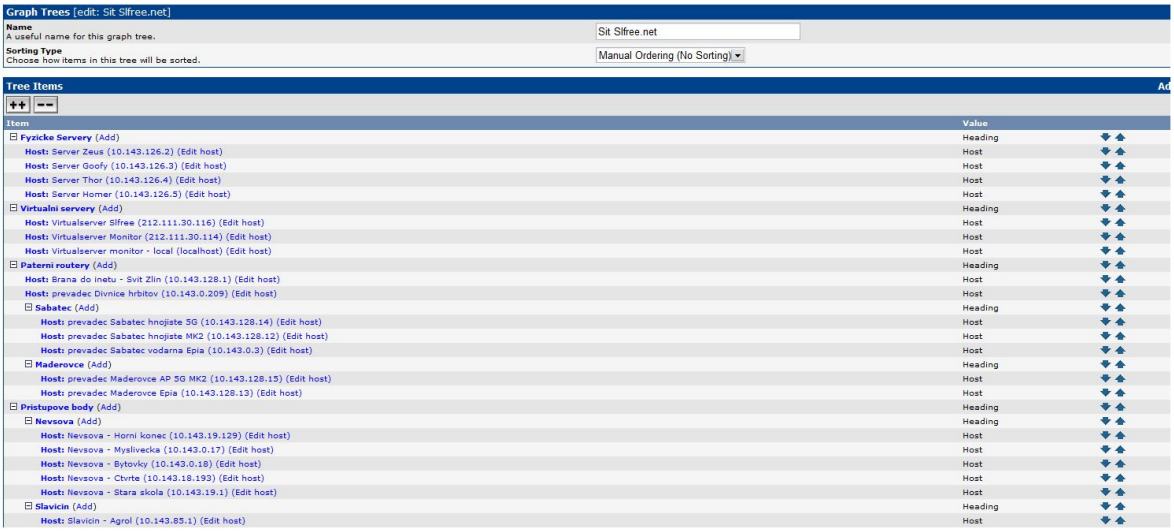
V této části systému Cacti se provádí konfigurace všech grafů jednotlivých datových zdrojů. Obsahuje seznam asociovaných grafů k datovým zdrojům *Data Sources.* Jednotlivým grafům můžeme upravovat vzhled a zdroje dat, transponovat hodnoty do nových rozsahů či tvořit grafy nové.

Například zde můžeme vytvořit graf datového toku nějakého zařízení, jenž bude obsahovat standardní křivky *bytes-in* a *bytes-out* a navíc novou křivku úrovně signálu *signal strengh.*

5.2 Graph Tree

Cacti dovoluje pro přehlednost vizualizace statistik tvořit stromové struktury grafů zařízení či jednotlivých dotazů *Data Queries,* které jsou zobrazovány v záložce Graphs.

Pro komunitní síť vytvoříme stromovou strukturu s hlavními větvemi Fyzické servery, Virtuální servery, Páteřní routery, Přístupové body. K těmto větvím přidáme jejich odpovídající členy typu HOST. Host obsahuje grafy vázané ke všem datovým zdrojům daného hosta.



Obr.19. *Část stromu slfree.net*

5.3 Weathermap

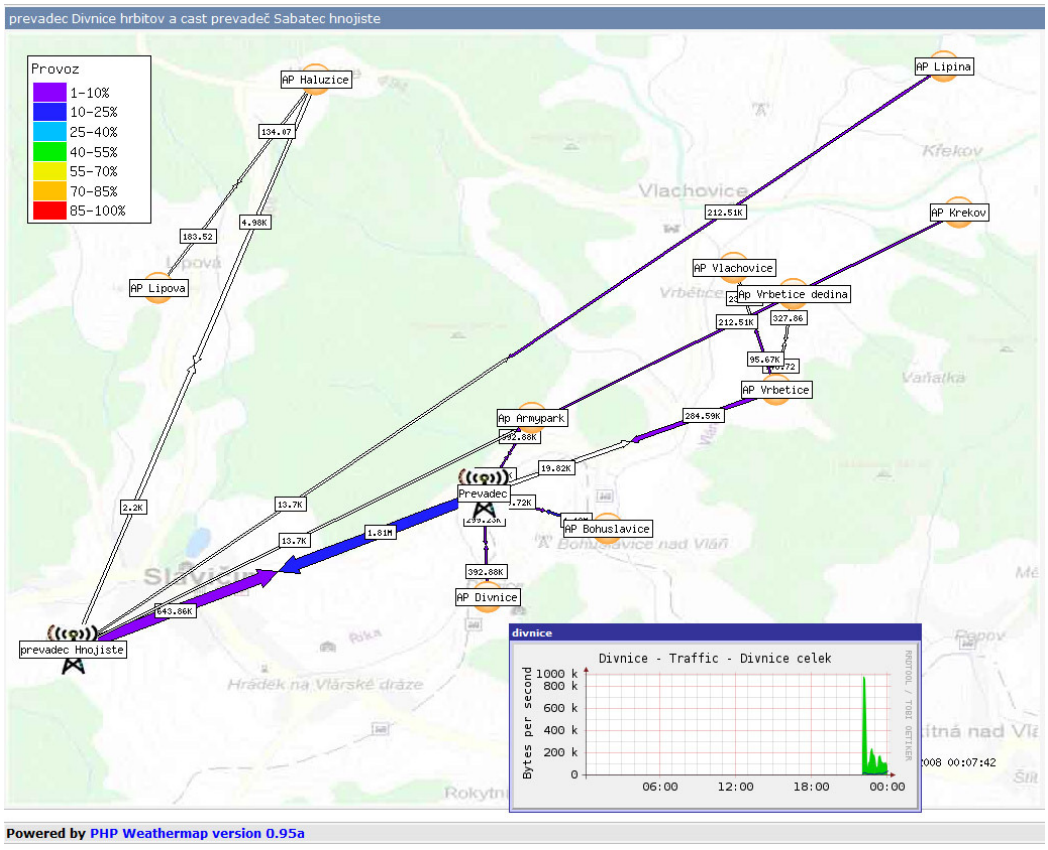
Plugin Weathermap rozšiřuje možnosti Cacti o tvorbu a zobrazování struktury sítě ve formě grafických map. Tyto mapy používají datových zdrojů Cacti k vizualizaci vytížení spojů mezi jednotlivými routery či přístupovými body, aktuální vytížení provozu formou grafů.

Můžeme tvořit mapy přístupné všem návštěvníkům internetových stránek monitoringu nebo mapy které budou sloužit pouze některým uživatelům či skupině.

Vzhledem k rozsáhlosti sítě budeme tvořit mapy dílčích částí. Aktuální mapa celkové sítě slfree.net se všemi aktivními prvky by byla značně rozsáhlá a její načtení a zobrazování provozu by bylo při přístupu z Internetu zdlouhavé.

Pro ukázku schopností pluginu Weathermap vytvoříme mapu části sítě, sestávající se z přístupového bodu převaděč Divnice a přístupových bodů, které jsou na něj napojeny.

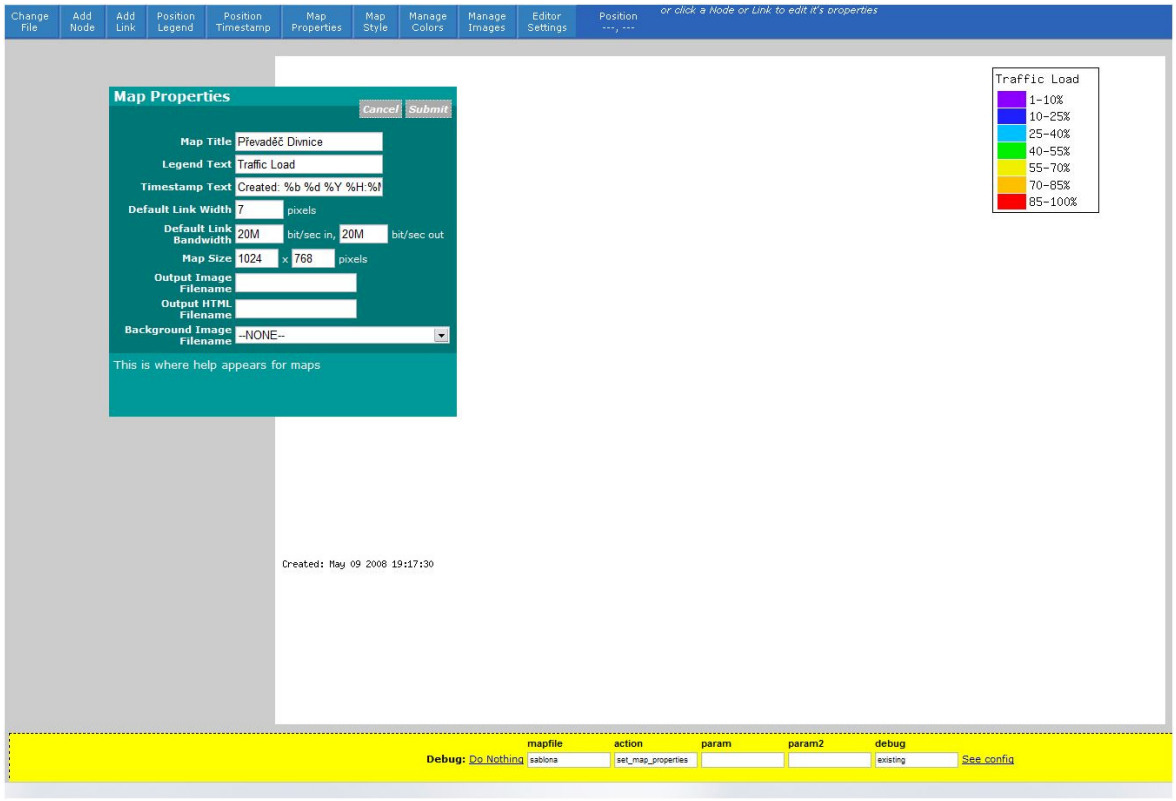
.



Obr.20. *Mapa pluginu Weathermap*

Z administrátorského přístupu otevřeme položku *Weathermaps*. Zde se nachází ukázková mapa *sample* a šablona *template*. Vložíme novou mapu odkazem *Add,* vybereme šablonu *template*, přejmenujeme ji na *prevadec Divnice.* Ve sloupci *Accessible by* je defaultně uveden učet *admin,* abychom tuto mapu zpřístupnili všem uživatelům, vybereme i účet *guest.*

Zvolíme mapu *prevadec Divnice*. Následně se otevře jednoduchý grafický editor.



Obr.21. *Grafický editor map pluginu Weathermap*

Tento editor z nakreslené mapy vygeneruje programový kód v adresáři výstupů */var/www/cacti/plugins/output/*, který může sloužit jako šablona pro tvorbu dalších map podobného typu.

Definujeme základní parametry mapy:

- v *Map Properties* zvolíme velikost mapy 1024x768 pixelů, defaultní rychlost spojů mezi převaděčem Divnice a jednotlivými přístupovými body 20Mbit/s
- *v Map styles* popisy vytížení linek jednotkách bit/sekunda, které budou uváděny u jednotlivých spojů

Vložení zařízení provedeme tlačítkem Add node. U každého zařízení je možnost zadání vlastní pozice pomocí souřadnic X a Y, názvu zařízení, ikonu, a zvolit datový zdroj, jehož grafické zobrazení bude po najetí kurzoru myši aktivováno. Můžeme vybírat z rolovacího seznamu, který obsahuje seznam všech datových zdrojů *Data Source.*

Vložením datového spoje provedeme tlačítkem *Add node* a následnou volbou dvou zařízení, která jsou spolu fyzicky propojena. V parametrech takto vytvořeného spoje taktéž

vybereme odpovídající datový zdroj. Jako zdroj dat mezi dvěma zařízeními bychom měli používat údaje ze zdrojů síťových rozhraní *Mikrotik Wireless-Registration Table.*

Po vložení všech zařízení, spojů a jejich nastavení se vrátíme na seznam map a tlačítkem *Recalculate map NOW* spustíme generování programového kódu mapy. Generátor v průběhu kompilace zobrazuje se kterými moduly pracuje a s jakým výsledkem. Nalezené chyby během kompilace jsou zobrazeny v celkovém logu. Nejčastěji se můžeme setkat s chybami přístupu k objektům mapy, což je způsobeno chybným oprávněním zpravidla u námi vložených nových souborů ikon a obrázků.

ZÁVĚR

Mezi hlavní úkoly monitorování počítačových sítí patří schopnost dlouhodobě poskytovat provozovateli sítě a náročným uživatelům se specifickými požadavky informace o operačním stavu sítě, o výkonnostních charakteristikách a o možných provozních a bezpečnostních problémech.

V této diplomové práci jsem implementací Open Source monitorovacího nástroje Cacti do komunitní sítě slfree.net vytvořil systém, který podává důležité informace o provozu svým členům v podobě statistik jejich přenosů. Tento systém poskytuje uživatelům aktuální informace o vytížení přístupového bodu, na který jsou napojeni a to i s možností zobrazení uložených dat. Z těchto grafických informací si mohou běžní uživatelé sami zjistit příčiny svých možných problémů, například s rychlostí svého připojení, množství stažených dat za určité období a další důležité informace.
Pro správce přístupových bodů komunitní sítě slfree.net systém nabízí funkce upozornění na výpadky zařízení nebo služeb sítě, na stavy signalizující překročení sledovaných parametrů. Umožňuje přidávat nové funkce do stávajících funkci monitoringu pomocí přídavných modulů, což přináší možnost pro zdatné programátory tvořit a následně importovat své vlastní skripty s požadovanými monitorovacími funkcemi.

Při použití existujícího rozšiřujícího modulu Manage systém Cacti umožňuje spravovat aktivní prvky sítě, prostřednictvím sady definovaných skriptů, které jsou na zařízení spuštěny, můžeme restartovat nefunkční služby či rozhraní a mnoho dalšího. Integrací rozšiřujícího modulu NCP přidáme možnost propojení monitoringu Cacti s jiným Open-Source monitorovacím systémem Nagios, jehož dat a funkcí je možno taktéž využívat.

Věřím, že výsledky této diplomové práce výrazně usnadní správu a dohled nad sítí slfree.net všem jejím správcům a poskytnou zajímavé informace všem členům.

Informace a postupy obsažené v této práci mohou být nápomocné při implementaci Open-Source monitorovacích systémů i do ostatních sítí.

ZÁVĚR V ANGLIČTINĚ

One of the main objectives of computer network monitoring is the ability to offer to the network administrators and exacting users the information about operational network status, performance, and possible operational and security problems.

In this graduation thesis, I have created a system by implementing Open Source Cacti monitoring tool into the community network slfree.net. The system offers important information to its members about operating in the form of statistics of their traffics. This system provides actual information about Access Point capacity utilization for connected users, namely with saved data visualization. By using this type of information, common users can discover the cause of their troubles such as decrease in speed connection, mount of downloaded data during a time period, and other important information.

The system will alert Slfree community network administrators about possible device or network service failures. It will also provide an alert in case of failure of any of the monitored parameters. The system makes it possible to add new functions into the existing monitoring functions by adding new modules, which offers to efficient programmers to create and to import their own scripts with required monitoring functions.

By using existing extending module, system Cacti offers managing active networks elements by using a set of defined scripts running on the network equipment. There is also a possibility to restart non-functioning services or interfaces and many other features. In conjunction with the integration of extending module NCP, we can increase interconnection Cacti monitoring with the other Open Source monitoring system Nagios, which functions can be also used.

I believe that results of this graduation thesis will make the administration of slfree.net network easier for its administrators and will offer interesting information for all members of Slfree.net. I also believe that the information and procedures included in this graduation thesis can be useful in course of implementation of Open-Source Monitoring Systems into the other computer networks.

SEZNAM POUŽITÉ LITERATURY

[1] ZANDL, Patrick. Bezdrátové sítě WiFi : Praktický průvodce. 1. vyd. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

[2] Nagios [online]. 17.1.2008. 2004 , 17.1.2008 [cit. 2008-01-17]. Dostupný z WWW: < http://www.nagios.org >.

[3] Cacti [online]. 2004 [cit. 2008-01-17].Dostupný z WWW: < http://www.cacti.net >.

[4] Mistrovství v Linuxu - Příkazový řádek, shell, programování; Mark G. Sobell; Computer Press, 2007; 880 stran černobílých; ISBN: 978-80-251-1726-2

[5] ROTT, Milan. Správa a monitorování lokálních počítačových sítí . Computerworld : Archiv tištěného Computerworldu [online]. 1999 [cit. 2008-05-13]. Dostupný z WWW: <http://archiv.cw.cz/cwarchiv.nsf/clanky/321B1D5406D95F13C12569B00055B852?OpenDocument>.

[6] O.s. UnArt. SLFREE.NET [online]. 2006 [cit. 2008-05-13]. Dostupný z WWW: <http://www.slfree.net/>.

[7] UBIK, Swen. Trendy v monitorování vysokorychlostních počítačových sítí. Sdělovací Technika [online]. 2006 [cit. 2008-04-13]. Dostupný z WWW: <http://www.ist-lobster.org/publications/articles/sdel_tech.pdf>. ISSN 0036-9942.

[8] Mikrotik Latvia. Reference Manual [online]. Document revision 3.40. 2008 [cit. 2008-04-10]. Dostupný z WWW: <http://www.mikrotik.com/testdocs/ros/2.9/>.

[9] KLIMENT, Michal. Co je to skrytý uzel (hidden node)? [online]. Neděle, 01 říjen 2006 [cit. 2008-05-01]. Dostupný z WWW: <http://www.slfree.net/technicke-otazky-a-odpovedi/co-je-to-skryty-uzel-hidden-node>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AP	Access point
CPU	Central Processing Unit
HTB	Hierachical Token Bucket
HTTP	Hypertext Transfer Protocol
IAB	Internet Architecture Board
ISP	Internet service provider
MIB	Management Information Base
NCP	Nagios Plugin for Cacti
NNTP	Network News Transfer Protocol
NUTS II	Nomenclature Unit of Territorial Statistic
O.s.	Občanské sdružení
OID	Object Indentifier
PAPI	Performance Application Programming Interface
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SROP	Společný regionální operační program
UnArt	United Art
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK