Monitorování zátěže páteřního spoje lokální počítačové sítě na budově U5

LAN Backbone Load Monitoring the U5 Building Computer Network.

Bc. Peter Böhm

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Peter BÖHM**
Osobní číslo:	**A10465**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Téma práce:	**Monitorování zátěže páteřního spoje lokální počítačové sítě na budově U5**

Zásady pro vypracování:

1. **Proveďte literární rešerši na dané téma.**
2. **Analyzujte protokoly a služby využívané v monitorovacích systémech.**
3. **Průzkumem trhu analyzujte možná řešení.**
4. **Vybrané řešení aplikujte na přípojce budovy U5.**
5. **Popište další možnosti dohledových systémů.**
6. **Proveďte analýzu výsledků monitorování.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DONDICH, Taylor. Network monitoring with Nagios. Sebastopol, CA: OReilly, 2006. ISBN 978-059-6528-195.**
2. **KRETCHMAR, James M. Administrace a diagnostika sítí: pomocí OpenSource utilit a nástrojů. 1. vyd. Brno: Computer Press, 2004, 216 s. ISBN 80-251-0345-5.**
3. **BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.**
4. **MCQUERRY, Steve, David JANSEN a Dave HUCABY. Cisco LAN switching configuration handbook. 2nd ed. Indianapolis, IN: Cisco Press, c2009, 333 s. Cisco Press networking technology series. ISBN 15-870-5610-0.**
5. **MATÚŠŮ, Jindřich. Monitorování stavu rozsáhlých sítí. Zlín, 2008. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Tomáš Dulík.**

Vedoucí diplomové práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **28. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práca je zameraná na monitorovacie systémy počítačových sietí a následnú realizáciu jedného vhodného riešenia pre monitorovanie dátového toku. Úvodné kapitoly teoretickej časti sú venované problematike monitorovania počítačových sieti, dôvodom na monitorovanie a možným nástrojom a technológiám, ktoré sa dajú na monitorovanie využívať. Ďalšia časť približuje tri monitorovacie systémy, ktoré boli následne porovnané. Na základe výsledkov som vybral vhodné riešenie pre implementáciu na hlavný server na budove U5.

V praktickej časti je popísaný postup inštalácie a konfigurácia nástroja PRTG Network Monitor od spoločnosti Paessler a analýza nameraných dát.

Klíčová slova: monitorovací systém, monitorovanie, počítačová sieť, SNMP, Nagios, Cacti, PRTG, analýza

ABSTRACT

The thesis focuses on monitoring systems of computer networks and the subsequent implementation of a suitable solution for the monitoring of the data flow. The opening chapters of the theoretical part are dedicated to the problematics of monitoring computer networks, reasons for monitoring and possible tools and technologies that can be used for monitoring. The next section focuses on the three monitoring systems, which were thoroughly analyzed. Based on the results of analysis, I selected the most suitable solution for implementation to the master server for building U5.

The practical part describes procedure of installation and configuration of the tool PRTG Network Monitor from Paessler and the analysis of collected data.

Keywords: monitoring system, monitoring, computer network, SNMP, Nagios, Cacti, PRTG, analysis

Poděkování:

Chcel by som poďakovať všetkým, ktorí mi akýmkoľvek spôsobom pomohli a podporovali ma pri spracovaní tejto diplomovej práce. Moje poďakovanie patrí najmä vedúcemu diplomovej práce, Ing. Korbelovi Ph.D. , za odbornú pomoc a cenné rady, ktoré mi poskytol.

Osobitné poďakovanie patrí mojim rodičom a mojim najbližším za ich podporu počas písania tejto práce.

Motto:

„Keď prechádzaš peklom, nezastavuj sa!“ Winston Churchill

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Medzi súčasné trendy moderných počítačových sietí patrí jednoznačne neutíchajúci vývoj počítačovej techniky a technológii, ako aj prudký nárast aplikácií typu klient-server. Aplikácie sa presúvajú z personálnych staníc na dedikované servery a tak vznikajú obrovské dátové úložiská. Vďaka týmto zmenám sa výrazne mení aj spôsob využívania siete - množstvo prenášaných informácií v rámci siete i mimo nej výrazne stúpa a vzniká veľké množstvo spojení. Architektúra a návrh sietí sa musí neustále prispôsobovať týmto požiadavkám. Vysoká dostupnosť a bezpečnosť siete tvoria spolu s včasným reportingom hlavné faktory pri správnom monitoringu siete a sieťového manažmentu. Ich porušenie má často krát za následok nemalé finančné straty pre danú spoločnosť. Práve preto je permanentné monitorovanie stavu siete, analýza týchto dát, riadenie a plánovanie rozvoja nevyhnuté.

Monitoring nám poskytuje informácie o súčasnom stave siete, aktivitách, využívaní jednotlivých zdrojov, bezpečnosti a o tom, či dostupnosť a efektivita služieb skutočne odpovedajú požiadavkám. Je nutné permanentne monitorovať stav jednotlivých serverov, dátových uložísk, aktívnych prvkov a dátových liniek. Administrátor musí mať možnosť monitorovať stavy a aktivity všetkých staníc, sledovať dátové toky v sieti a vyťaženosť jednotlivých liniek. K požiadavkám na monitorovanie zároveň pribudla aj potreba analyzovať a vyhodnocovať namerané dáta. Pred implementáciou monitorovacieho nástroja je dôležité si položiť otázku, čo všetko a akým spôsobom chceme monitorovať. Chceme monitorovať len stavy jednotlivých sieťových aktív alebo aj dostupnosť a reakčné doby služieb? Analýzu sieťovej prevádzky? Vyťaženosť liniek? Detekciu anomálneho chovania? Zber a analýzu bezpečnostných logov? Reporting?

Rôzne skupiny užívateľov samozrejme majú odlišné nároky na monitorovací systém. Základom je však monitorovací systém, ktorý bude schopný ponúknuť ucelené a prehľadné informácie o celkovom stave a vývoji siete, jej službách, aplikáciách a užívateľoch. Kvalitné monitorovanie je preto nevyhnutnou podmienkou úspešného chodu akejkoľvek dátovej siete.

V súčasnosti je na trhu veľké množstvo ako open-source, tak komerčných nástrojov. Dôležitými kritériami pre voľbu nástroja sú jednoznačne užívateľské požiadavky na monitoring, možnosť podpory a v neposlednom rade aj jeho cena a náklady na prevádzku.

I. TEORETICKÁ ČÁST

1 SIEŤOVÝ MANAŽMENT

1.1 Prečo monitorovať počítačovú sieť

Monitoring serverov, sieťových prvkov a ďalších sieťových zariadení je dnes nevyhnutnou súčasťou správneho a bezpečného spravovania siete. Pritom možností a monitorovaných oblastí je veľké množstvo. Pokiaľ poznáme odpovedajúce technológie a cieľ monitorovania, môžeme zhotoviť kvalitný monitorovací systém aj s minimálnymi nákladmi, ba dokonca zadarmo. V tejto kapitole budú priblížené možnosti monitorovania spolu s technológiami, ktoré sú k dispozícii. [1]

1.2 Analýza a monitorovanie siete

1.2.1 Čo monitoring dáva a aké technológie sú k dispozícii

Monitoring má mnoho podôb a je možné využiť radu technológii a protokolov. Celý monitorovací systém môže byť postavený na vlastných skriptoch či na bezplatných riešeniach, do ktorých sa investuje iba vlastný čas a znalosti. Možné je tiež využiť niektorý z rozsiahlej ponuky komerčných riešení, ktoré síce šetria čas, no sú finančne náročné a investícia do nich nemusí byt preto vždy najlepšie riešenie. Pre detailný prehľad o tom ako monitoring prebieha a či presne odpovedá potrebám, je lepšie sa nespoliehať na cudzie aplikácie, ale postaviť monitoring na vlastnoručne napísaných skriptoch alebo programoch. Je potreba však disponovať dobrými znalosťami skriptovania a programovania, takisto ako mať dobrú znalosť sieťových protokolov a príslušných technológii. Tvorba takéhoto riešenia je časovo pomerne náročná, avšak bude istota, že dané riešenie stopercentne odpovedá požiadavkám.

Produkty zdarma sú často dostatočne univerzálne so širokými možnosťami konfigurácie, aby dokázali pokryť čo najväčšie množstvo cieľov monitorovania. Vyžadujú však takisto hlbšie znalosti pre konfiguráciu a nastavovanie, pretože niektoré konfigurácie sú možné len s pomocou vlastných skriptov. Výhodou je komplexné prostredie, zahrňujúce napríklad konfiguráciu, dashboard, webové rozhranie či spracovanie grafov a na mieru sa nastavujú iba určité šablóny a prídavné pluginy a balíčky, pre získavanie dát. Oproti tomu sa komerčné produkty väčšinou nanštalujú na par kliknutí a celkové monitorovanie je k dispozícii behom pár minút. Stačí iba poznať a zadať adresy zariadení, ktoré majú byť monitorované a aké údaje z nich budú zaznamenávané. Väčšinou sú pred pripravené

šablóny pre jednotlivé oblasti monitorovania, ktoré výrazne uľahčujú prácu, no zároveň obmedzujú možnosti použitia. Samozrejme aj tieto riešenia je možné konfigurovať a rozširovať o vlastné skripty podľa uváženia, stráca sa tým však jednoduchosť celého systému. [1]

Niektoré monitorovacie systémy:
Zdarma - Nagios, Cacti, Zabbix
Platené - Zenoss, PacketTrap pt360, WhatsUp Gold, PRTG
Od veľkých firiem - Microsoft System Center Operations Manager, HP OpenView, IBM Tivoli Netcool, CiscoWorks LAN Management Solution

1.2.2 Čo chceme sledovať?

Skôr ako sa začne samotný monitoring plánovať, je treba si uvedomiť čo presne má byť monitorované a aké výstupy z monitoringu sú prioritné. Podľa toho je treba zvoliť aj použité technológie. I keď existujú rozsiahle systémy s radou komponent, tak nájsť monitorovací nástroj, ktorý obsahuje všetky možné oblasti monitorovania, ktoré je možné sledovať je prakticky nemožné a je nutné skombinovať viacero produktov. Monitoring sa dá vo všeobecnosti rozdeliť na dve skupiny. Jedna z možností je monitorovanie bezproblémového chodu siete, kde sa sleduje či nedošlo v danej siete k chybe. Teda že niečo prestalo fungovať alebo boli dosiahnuté kritické hodnoty, ktoré by mohli viest k chybe. Druhou možnosťou je získavanie aktuálnych (alebo tiež historických) informácií o určitom systému, napr. vyťaženie serveru, množstvo pripojených klientov alebo vyťaženie dátových liniek. Zozbierané dáta môžu byt následne vykreslené do grafov pre ľahký a rýchly prehľad o nameraných hodnotách. [1]

1.2.3 Oblasti pre monitoring

V počítačovej sieti je možné monitorovať takmer všetky parametre siete a jednotlivých zariadení . Zo všeobecného hľadiska môžeme monitoring rozdeliť na :

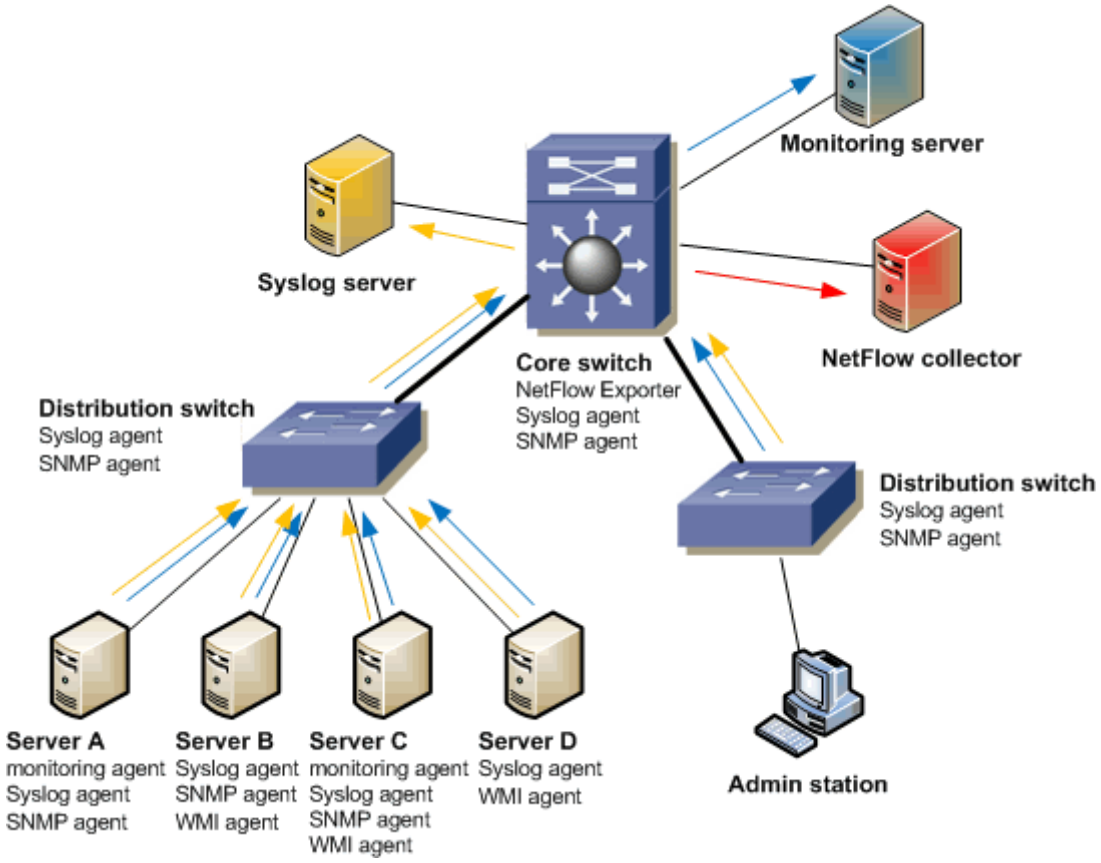
- monitoring serverov a ich služieb
- monitoring aktívnych sieťových prvkov
- monitoring sieťovej komunikácie

- monitoring bezpečnosti

Pomocou špecializovaných nástrojov je možné sa zamerať na viac špecifické oblasti, aj keď ide v podstate o hore uvedené monitorovanie. Sú to oblasti ako IP telefonovanie, bezdrôtové siete, FTP komunikácia alebo virtuálne prostredí. [1]

Oblasti, ktoré sa dajú monitorovať:

- dostupnosť serverov
- dostupnosť služieb/aplikácií
- latencia – reakční dobou
- udalosti na serveroch
- vyťaženosť zdrojov (CPU, pamäť, HDD)
- vyťaženosť liniek – meranie prenosu dát
- štatistika sieťovej komunikácie
- analýza neštandardného chovania v sieti
- informácie o portoch na switchoch
- monitoring WiFi či IP telefonovanie
- bezpečnostné incidenty



Obr. 1 Ukážka monitorovacieho systému

1.3 Technológie pre monitoring

Pokiaľ sa pouzije nejaký komplexný monitorovací systém pre dohľad serverov, tak ponúka väčšinou dve základné možnosti pre prístup k informáciám.

Monitorovanie s agentom

Na server je potrebne nainštalovať špeciálneho klienta daného dohľadového systému. K dispozícií musí byť teda agent pre daný operačný systém, možnosť ho na daný server inštalovať a pripadne doinštalovať ďalšie nutné aplikácie, ktoré však môžu spôsobovať nežiaduce problémy. Ak sa nevyskytnú žiadne problémy, z daného klienta sa dá získať dostatočne široké spektrum údajov. [1]

Monitorovanie bez agenta

Druhou možnosťou je monitorovanie bez agenta, kde sa testujú vlastné služby serveru alebo sa dáta získavajú pomocou určitých štandardných protokolov ako SNMP, WMI, IPMI.

Na monitorovanie jednotlivých oblasti sa dá využiť niekoľko technológií, či už samostatne alebo implementovane vo vnútri monitorovacieho systému. Záleží len na užívateľovi, pre ktorú technológiu sa rozhodne, keďže každá oblasť sa dá monitorovať niekoľkými technológiami . [1]

- dostupnosť serveru pomocou ping testu
- dostupnosť služby pomocou TCP spojenia alebo na aplikačnej úrovni
- udalosti zo serverov - Syslog
- získavanie údajov pomocou klienta
- získavanie údajov pomocou monitorovacích protokolov WMI, SNMP, IPMI
- sledovanie sieťových tokov - NetFlow
- analýza sieťových protokolov - network protocol analyzer
- bezpečnosť v sieti - IDS/IPS

1.3.1 Výstupy monitoringu – reporty a alerty

Aj perfektný monitoring, ktorý bude sledovať a zaznamenávať všetko v našej sieti, pokiaľ nebude mať prehľadné, dostupné a často aj inteligentné výstupy, tak celý monitoring stráca na význame. Preto je dôležité hneď od začiatku plánovať, aký výstup pre akú oblasť je najvhodnejší.

Z pohľadu typu dát je možné rozlíšiť dve základné oblasti. Môžu to byt buď udalosti, ktoré získané pomocou Syslogu, WMI či SNMP trapov zo serverov, switchov a ďalších zariadení alebo hodnoty, často číselné, ukazujúce okamžitý stav danej vlastnosti. Záleží už na potrebách užívateľa, či mu stačí vedieť okamžitý stav nebo potrebuje ukladať históriu, ako sa hodnoty menia v čase. Pre rôzne sledované údaje sa samozrejme hodí rôzna reprezentácia výstupu. Vyťaženosť liniek alebo procesoru je potreba poznať v určitom časovom období, preto vhodným zobrazením je graf. Naopak stavy portov switchov sa zaznamenávajú v aktuálnych hodnotách a najlepšou a najprehľadnejšou reprezentáciou je tabuľka. Dostupnosť serveru sa zas môže zobrazovať ako percentuálna hodnota. Pre globálny pohľad na sieť je výhodná grafická reprezentácia, kde je viditeľná schéma siete

alebo jej časti. Pri zistení problému sa daný prvok zvýrazní a po rozkliknutí poskytne detailné informácie o danom probléme.

Tieto reprezentácie sú jednoduché a vo väčšine situáciách veľmi užiteľné. Existujú však aj situácie, kedy ide o bezpečnostnú alebo havarijnú udalosť, a nie je k dispozícii dohľadový tým, ktorý neustále sleduje monitorovací systém. V takom momente je omnoho užitočnejšie odosielanie emailovej alebo SMS správy o tejto chybe zodpovedným osobám, aby boli čo možno v najkratšom možnom čase schopné reagovať na daný problém. [1]

1.3.2 Dostupnosť zariadení a služieb

Dokazovanie sa na dostupnosť zariadenia alebo služby je jednou zo základnej technológie pre monitoring. Asi prvou vecou, ktorá sa začína monitorovať, je dostupnosť serveru či aktívneho sieťového prvku. V malej sieti, kde je minimálny počet serverov a iných sieťových prvkov, sa nedostupnosť prejaví pomerne rýchlo, skôr okamžite. Vo väčšom prostredí sa však môžu začať hromadiť problémy nadväzujúcich služieb a môže trvať dlhšiu dobu, kým sa podarí niekomu zaregistrovať nedostupnosť nejakého prvku či sieťovej cesty, čo môže spôsobiť ochromenie funkcionality celej siete.

Bežne sa dostupnosť zariadení zisťuje pomocou jednoduchej metódy ICMP echo request/response, známejšej ako ping. Prípadne sa používa tzv. „SNMP ping“, čo je SNMP dotaz na bežné OID. Takto je možné zistiť, či je dané zariadenie dostupné, ak áno, môže sa merať jeho doba odozvy (latencia). Ďalším krokom monitoringu je dostupnosť aplikačnej služby, pretože pomocou pingu sa dá zistiť, či je funkčný webový server, ktorý využíva sieťový protokol TCP tak ako väčšina bežných sieťových služieb. Takže sa testuje, či sa podarí naviazať so serverom TCP spojenie na daný port. Ak spojenie prebehne bez problémov, znamená to, že daná služba beží v poriadku. Ďalšou možnosťou ako overiť dostupnosť sieťovej služby je aplikačný test. Ide o oveľa lepšie riešenie, keďže overujeme či sa daná služba chová tak ako má. [1]

1.3.3 Syslog – udalosti zo serverov

Syslog je štandard pre zasielanie správ z logov v sieti. Používa sa na zaznamenávanie logov z rôznych zariadení a ich aplikácií na jedno miesto, aby sme boli schopní na ne reagovať. Na klientovi je potrebné mať nainštalovanú aplikáciu, ktorá odosiela správy z logu pomocou Syslog. Následne je potreba vlastniť Syslog server, ktorá prijíma a spracováva tieto správy.

Syslog je veľmi užitočný, pretože do logu pribúdajú bežne stovky správ za minútu a pre desiatky zariadení nie je šanca tieto informácie prehľadávať. V Syslogu je možné vytvárať skripty, ktoré sú schopné analyzovať prichádzajúce správy a dokážu upozorniť na vyskytnuté problémy. Napríklad zo Security logu Windows sa dá vyčítať neplatné prihlasovacie pokusy a keď sa jedno konto pokúša neúspešne prihlásiť v danom časovom intervale viackrát, je možné zaslať e-mail správcovi s varovaním o možnom útoku na dané zariadenie. [1]

Druhou výhodou je možnosť uchovávať a archivovať veľkého množstva správ, t. j. dlhodobú históriu. Mnoho zariadení dokáže uložiť lokálne iba obmedzený počet logov. Okrem toho sú tieto logy k dispozícii, aj keď je server nedostupný. Teda ak dôjde k zlyhaniu servera alebo bol napadnutý útočníkom, nie je možné z jeho logu zistiť dôvody nefunkčnosti. V takomto prípade je možné na Syslogu nájsť správy ktoré viedli k tomu, že server si neplní svoju. Monitorovanie viac-menej nepozná hranice a záleží na kreativite a schopnostiach ľudí, ako si ho dokážu prispôsobiť pre vlastne potreby.

2 ZÁKLADNÉ INFORMÁCIE

2.1 Čo je to dohľadový systém

Nasadzovanie IT technológií vo všetkých oblastiach života spoločnosti už neprekvapí snáď nikoho. Spoločnosť je čoraz viac závislá na IT technológiách a tak narastá aj závislosť na spoľahlivej a bezpečnej prevádzke jednotlivých systémov tvoriacich informačný systém. S narastajúcim vplyvu IT technológií, narastajú aj náklady na ich prevádzku. Napríklad kolaps systému riadiaceho výrobu vo väčšine prípadov znamená aj výpadok v samotnej výrobe, čo spôsobuje nemalé ekonomické straty. Preto čoraz väčšiu úlohu v riadení IT hrajú systémy, ktoré robia ich prevádzku bezpečnejšou a efektívnejšou – systémy riadenia IT, IT manažment. IT manažment je pomerne komplikovanou záležitosťou zvlášť v podnikoch, kde je počet informačných subsystémov vysoký (banky, veľké výrobné korporácie, podniky a pod.). Súčasťou IT manažmentu je nie len vhodné SW a HW vybavenie, ale aj efektívny a spoľahlivý personálny a procesný manažment. Hlavnou časťou systému riadenia IT je pravdepodobne dohľadový systém. Jeho úlohou je zbierať údaje zo zariadení a subsystémov IT infraštruktúry, spracovávať ich a prezentovať spôsobom, aby bola obsluha schopná dostať sa k relevantným informáciám načas a v potrebnom rozsahu. Dohľadové systémy sú základom služieb monitoringu a správy systémov. Včasné informovanie o prípadných problémoch, ich prevencia a sledovanie kvality služby sú základom, na ktorom stavia proaktívne plánovanie systémových prostriedkov a priebežné zlepšovanie kvality služby.

Dohľadový systém sa dá takisto v jednoduchosti nazývať monitorovací systém, ktorého úlohou je monitorovať stav siete, aplikácií, záťaže servera, atď. Pod pojmom monitorovanie siete sa dá predstaviť aj systém umožňujúci správcovi siete kontrolovať sieť, služby alebo analyzovať a spravovať sieťovú infraštruktúru vzdialene z jediného miesta bez nutnosti osobného zásahu. Systémy môžu monitorovať a kontrolovať vybrané podsiete, zobraziť štatistiky siete ako aj hardvérový a softvérový zoznam a zoznam služieb spustených v počítači. Systém môže kontrolovať všetky aspekty siete LAN a WAN, serverov, pracovných staníc a vôbec všetkých IP zariadení. Hlavnou úlohou a poslaním monitorovacích systémov je maximalizovať spoľahlivosť sieťovej infraštruktúry, všetkých zariadení pripojených do siete a aplikácií pomocou automatického zistenia a opravy vzniknutého problému tak, že reagujú na všetky chyby a problémy v sieti v reálnom čase. To znamená, že reagujú v najkratšom možnom čase. Systémy sú schopné aj automatickej

opravy chyby, kde vytvoria súbor so záznamom o vzniknutej chybe a vzniknutú udalosť iba nahlásia správcovi. Monitorovacie systémy môžu bežať na všetkých známych operačných systémoch, ako napr.: na Linuxu, Unixových systémoch, Netware, MacOS, Windows.

2.2 Zloženie monitorovacieho systému

Monitorovací systém v praxi tvorí skupina programov, ktorej účelom je poskytovať prehľadnou formou informácie o dohľadovanej sieti. Monitorovací systém je najčastejšie založený na modeli klient/server. Server je nazývaný tiež manažér a zbiera informácie od jednotlivých agentov. Klient je nazývaný agent a beží na sledovanom sieťovom zariadení. Jeho úlohou je monitorovať stav daného zariadenia a posielať údaje o jeho stave na server, manažérovi. Agent je takisto schopný komunikácie s jednotlivými agentmi navzájom. Manažér obsahuje väčšinou veľmi prijemné a intuitívne užívateľské rozhranie na svoju obsluhu prostredníctvom internetového prehliadača.

2.3 Druhy monitorovania

2.3.1 Ping (Packet Internet Groper)

Príkaz Ping je jedným z prvých a jeden z najpoužívanejších a najjednoduchších overení dostupnosti pripojeného aktívneho zariadenia k sieti a stal sa nenahraditeľným nástrojom pre riešenie problémov s konektivitou siete internet a miestnej siete. Funguje na princípe odosielania Echo ICMP (Internet Control Message Protocol) v sieti TCP/IP cieľovému uzlu, ktorý pri správnej konfigurácii siete túto správu prijme a odpovie na ňu správou Echo Response. Sprava Echo Response takisto potvrdí všetky dáta, ktoré odosielateľ odoslal v odchádzajúcej správe Echo. Pokiaľ uzol, ktorý bol odosielateľom príkazu Ping získa spätne správy behom dopredu daného intervalu, je to dôkaz, že dotazovaná stanica a všetky IP zariadenia medzi ňou a adresátom sú správne nakonfigurované na prenos dať v IP, čiže spojenie funguje. [5][6][3]

Príkaz Ping poskytuje mnoho rôznych dôležitých informácii ako:

- Umiestňuje jedinečné poradové číslo do každého paketu, ktorý odošle a oznamuje poradové čísla, ktoré dorazia späť. Môže tak zistiť, či boli pakety zahodené, duplikované alebo preskupené.

- Overuje (vykonáva kontrolný súčet) každý paket, ktorý vymení a detekuje tak určité formy poškodenia paketov.
- Do každého paketu umiestňuje časové razítko, ktoré je odoslané späť a je možné podľa neho zistiť dobu výmeny paketu.
- Oznamuje ďalšie správy ICMP, ktoré by sa inak stratili v systémovom softwari.

Príkaz Ping má však aj obmedzenia a existujú veci, ktoré nie je schopný zistiť:

- Nemusí vždy poskytovať dôvod, prečo na pakety nereaguje cieľová stanica, pretože niektoré smerovače zahadzujú nedoručiteľné pakety alebo sú presvedčené o tom, že pakety boli prenesené úspešné aj keď tomu tak nie je.
- Nedokáže zistiť, prečo bol paket poškodený, oneskorený alebo duplikovaný
- Nemôže poskytnúť podrobnú analýzu každého hostiteľa, ktorý paket spracováva.

2.3.2 Tracert

V určitých situáciách je potrebné skontrolovať trasu paketu medzi zdrojovým a cieľovým uzlom. Príkaz Tracer (v operačných systémoch Linux nazývaný Traceroute) je jednou z ďalších utilít protokolu TCP/IP , ktorá sleduje a zaznamenáva smerovania, ktoré paket podstúpil. To môže byť obzvlášť dôležité, keď pomalá odozva a pakety Ping naznačujú moc dlhé oneskorenie, ktoré môže byť spôsobené nesprávnym a nadmerným počtom smerovaní. Týmto spôsobom sa dá takisto nájsť posledné úspešné smerovanie pred stratením paketu. Príkaz tracert toto uskutočňuje nastavením hodnoty TTL (Time To Live) v pakete, pričom očakáva od každého priechodzieho smerovača správu ICMP time_exceeded. Hodnota TTL predstavuje povolene množstvo presmerovaní pred tým ako bude pakt zahodený. Implementácia tohto príkazu je založená na používaní kombinácií protokolov UDP a ICMP. [5][6][3]

2.3.3 SNMP (Simple Network Management Protocol)

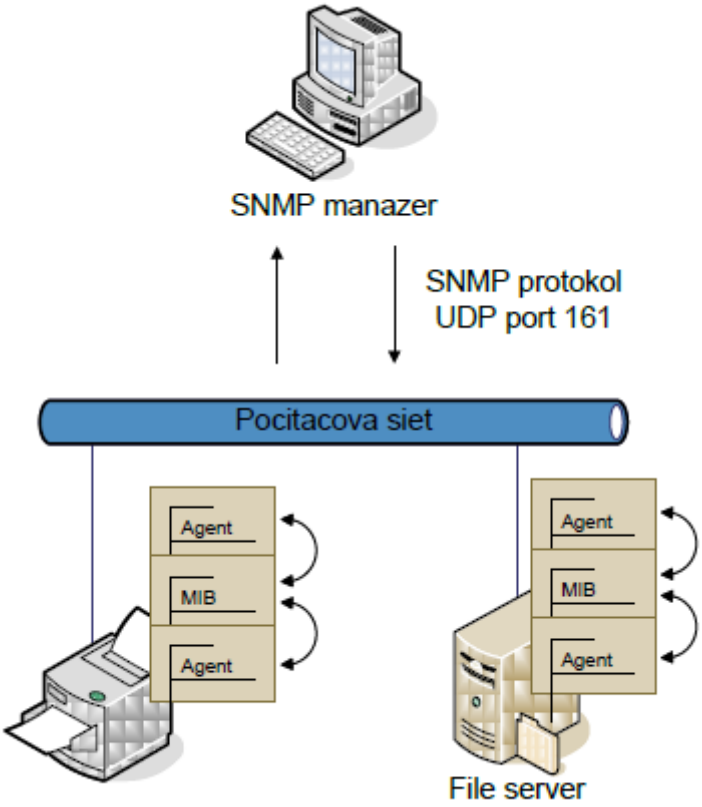
V oblasti správy sietí sa objavilo už mnoho komplexných protokolov, ale žiadny z nich sa nedokázal presadiť tak výrazne ako v prípade SNMP . SNMP je jednoduchý, široko rozšírený a užitočný štandardizovaný protokol, ktorý slúži k získavanie alebo nastavovaniu hodnôt na určitom zariadení. Protokolu SNMP je vznikol na konci 80. rokov minulého storočia. Vznikol ako náhrada protokolu SGMP (Simple Gateway Monitoring Protocol).

Bol navrhnutý koncom roku 1987 pre výmenu informácií medzi smerovačmi a bránami. Vzhľadom k tomu, že protokol SNMP presne splňoval podmienky a požiadavky na sieťovú správu, bol v roku 1990 protokol SNMP potvrdený ako štandard pre správu sietí. Na protokolu SNMP je dnes založená väčšina nástrojov a prostriedkov, ktoré sa venujú správe siete. Protokol SNMP je založený na modely klient/server. Agent beží na sledovanom sieťovom zariadení a monitoruje stav sledovaného zariadenia a posiela o jeho stave informácie manažérovi. Podporu SNMP má veľké množstvo zariadení, napríklad aktívne sieťové prvky, tlačiarne, prístupové body alebo osobné počítače a servery za pomoci softwaru a ovládačov. Hodnoty sa väčšinou získavajú v pravidelných intervaloch a tie sa následne ukladajú do databáze spolu s časom, z ktorej je možné jednotlivé hodnoty vykresliť do grafov ako jeden celok. Prehľadne sa tak dá zobraziť napríklad vyťaženie procesoru, priebeh teploty alebo dátový tok na určitom porte. [5][6][3] [10]

Ako funguje protokol SNMP

Systém správy siete s protokolom SNMP sa rozdeľuje do troch častí:

- **Zariadenie sieťovej správy *(managed device)*** – je to uzol siete, ktorý obsahuje sieťového agenta. Zhromažďuje potrebné informácie do svojej internej databáze. Zariadeniami sieťovej správy môžu byť routre, prístupové servery, prepínače, mosty, tlačiarne a ďalšie zariadenia.
- **Agent** – časť softwaru, ktorý je nainštalovaný na zariadení sieťovej správy. Agent má priamy prístup k informáciám, ktoré sú uložené v databáze. Na základe žiadostí od manažéra odpovedá na dotazy vyhľadaním príslušných dát v databáze. Agent posiela oznámenia (trapy) s hodnotami na adresu správcu v určitých definovaných situáciách (prekročenie hodnoty alebo v pravidelným intervaloch).
- **Manažer** – hlavná časť softwaru umiestnená na stanici sieťovej správy *(Network Management Station),* ktorá zodpovedá za dopredu určené činnosti na riadených objektoch. Vykonáva dohľad nad určitou skupinou zariadení pomocou agentov, s ktorými vzájomné komunikuje.



Obr. 2 Architektura SNMP protokolu

SNMP používa pre komunikáciu UDP protokol, čiže transportnú vrstvu bez spojenia v protokole TCP/IP. Ide o veľmi rýchlu komunikáciu, pričom môže ale dôjsť ku strate alebo nedoručeniu zasielaného paketu. Štandardne sa využíva port 161 (SNMP) na strane agenta (pre dotazy) a port 162(SNMPTRAP) na strane serveru (pre trapy). Klient, ktorý posiela dotaz, zvolí dynamický port, z ktorého posiela dotaz na port 161. Agent odpovedá z portu 161 na dynamický port klienta. V praxi to znamená, že pre každý dotaz je použitý iný dynamický port. [3] [10]

Verzie SNMP:

V súčasnej dobe existujú 3 verzie protokolu, ktoré síce nie sú vzájomne kompatibilné, ale bývajú často v zariadeniach implementované súbežne : SNMPv1, SNMPv2 a SNMPv3. SNMPv1 a SNMPv2c používajú pre autentizáciu community string, resp. textové heslo. V SNMPv3 je možné využiť autentizáciu pomocou mena a hesla a šifrovania.

SNMPv1:
Prvá špecifikácia protokolu SNMPv1 vznikla v roku 1989. Tato verzia používala pre autentizáciu iba ochranu heslom v reťazci community string, ktorý je súčasťou paketu. Išlo o nešifrované heslo, ktoré sa dalo pomocou filtrovania paketov veľmi ľahko odhaliť. Prevažná časť operácií funguje na princípe klient-server medzi sieťovým manažérom a agentom. Väčšina riadiacich a monitorovacích činností sa tak vykonáva na základe dotazov, ktoré sú periodicky opakovane. Existujú však udalosti, ktoré majú charakter krátkodobej zmeny a ktoré nemusia byť pravidelným dotazovaním zachytené. Tento problém riešia pasce, takzvane trapy, ktoré reagujú zaslaním informácií manažérovi aj bez jeho výzvy. [3] [10]

SNMPv2:

Predovšetkým nedostatky prvej verzie v oblasti bezpečnosti viedli k návrhu novej verzie protokolu SNMP. Ani v SNMPv2 bohužiaľ nedokázali odstrániť túto obrovskú slabinu, používa sa ale aspoň autentizácia overením identity užívateľa a služieb. Nový štandard opustil myšlienku komunít a zaviedol novú prístupovú politiku. Boli definované nové operácie, slúžiace k hromadnému zberu dát zo zariadení. Vývoj tejto verzie bol zastavený pre vnútorné nezhody vo vývojárskom tíme, napriek tomu sa stala táto verzia v dnešnej dobe najpoužívanejšia. [3] [10]

SNMPv3:

V súčasnej dobe sa začína uplatňovať nová verzia protokolu SNMP, ktorá má nahradiť obe predchádzajúce verzie. Najnovšia verzia protokolu SNMP pochádza z roku 1998 a výrazne vylepšuje bezpečnosť. Základný princíp preberá od prvej verzie, ale vylepšuje v ňom mechanizmy podľa súčasných požiadavkou na bezpečnosť sieťovej komunikácie. Umožňuje totiž šifrovanú ochranu správ behom prenosu v sieti a na overovanie zdroja SNMP správ pomocou algoritmu DES. [3] [10]

SNMP dotazy

Klasický priebeh komunikácie posielania dotazu na jednu hodnotu a následný prijem odpovedi :

- Manažér odošle dotaz – nastaví sa typ GET, zadá sa OID pre zisťovanú hodnotu, vlastní hodnota sa nastaví na NULL
- Agent vracia odpoveď – typ je nastavený na RESPONSE (2), OID na dotazovanú hodnotu a je vyplnená hodnota

Dotaz/ Odpoveď

verze	community string	PDU	ID dotazu	error status	error ID	OID	hodnota

Ukážka

1	public	GET (0)	8	no error (0)	0	1.3.6.1.4.1.311.1.1.3.1.1.1	NULL

SNMP operácie

SNMP operácie definujú povolenú formu komunikácie medzi Agentom a Manažérom a medzi Manažérmi navzájom.

- GetRequest - manažér požaduje informácie od agenta
- SetRequest - manažér požaduje od agenta nastavenie hodnoty
- GetNextRequest - používa sa pre získaní ďalší hodnoty, vezme nasledujúci OID za zadaným
- GetBulkRequest – vracia viac hodnôt jedným príkazom, umožňuje získať väčšiu časť stromu
- Response - odpoveď agenta
- Trap – pozmenený typ paketu ako zvyčajne, v prípade, že nastane dopredu daná udalosť
- InformRequest - používa sa pre komunikáciu medzi manažérmi

MIB databáze – Management Information Base

Preto, aby mohol agent získavať a odosielať informácie, musí dokonale poznať štruktúru databáze MIB. MIB je stromová štruktúra, kde sú dáta uložené v každom listu stromu.

Každý z uzlov v stromu má svoje číselné aj slovné označenie. Prístupové cesty od koreňa stromu až k danému uzlu a sú teda vždy jednoznačne určené. MIB špecifikuje aj typy dať aké môže položka obsahovať. Najčastejšie obsahuje hodnoty typu integer, string alebo inú zložitejšiu dátovú štruktúru. [10]

2.3.4 Sledovanie portov

V sieťových protokoloch port označuje číslo, ktoré je spolu s IP adresou súčasťou identifikátora konca spojenia. Toto číslo vyjadruje konkrétnu službu, ku ktorej je priradené spojenie. Takisto v hlavičke paketu sa nachádza zdrojový a cieľový identifikátor konca spojenia. Medzi protokoly využívajúce porty patria TCP, UDP a SCTP. Mnohé sieťové služby používajú pevne určený port.

Porty môžeme rozdeliť do 3 skupín:

- 0 – 1023 bežne známe porty (well-known ports)
- 1024 – 49151 registrovane porty, používajú sa pre menej známe služby, je možno si ich zaregistrovať pre vlastne aplikácie,
- 49152 – 65535 dynamické a privátne porty nemajú registrované služby

Port	Protokol	Popis
21	FTP	Zabezpečuje prenos súborov
22	SSH	Secure shell – šifrovaná podoba protokolu telnet
23	Telnet	Vzdialený terminálový klient
25	SMTP	Simple Mail Transfer Protocol - zabezpečuje prenos elektronickej pošty
80	HTTP	Zabezpečuje prenos www stránok
110	POP3	Zabezpečuje sťahovanie elektronické pošty zo serveru
443	HTTPS	Šifrovaný protokol pre prenos www stránok

Tabuľka 1 Prehľad najznámejších portov a služieb, ktoré na nich bežia

Porty sa môžu nachádzať v niekoľkých stavoch. Port môže byť otvorený, čo znamená, že na tomto porte beží už nejaká služba, ktorá aktívne prijíma TCP spojenia alebo UDP pakety. Zistenie tohto faktu je často hlavným cieľom scanovania portov. Avšak každý otvorený port je prístupný pre útok. Útočníci a testeri preniknutia chcú využívať otvorené porty, zatiaľ čo administrátori sa pokúšajú zatvoriť ich alebo chrániť ich firewallmi bez limitovania oprávnených používateľov. Port môže byť takisto uzavretý, ak na ňom žiadna služba nebeží. Zatvorený port je síce prístupný, ale žiadna aplikácia na ňom nepracuje. Môže sa ale využiť pri zisťovaní či je hostiteľská stanica aktívna na danej IP adrese. Pretože sú zatvorené porty dosiahnuteľné, môže byť užitočné vykonávať neskorší scan a s očakávaním, že niektoré môžu byt neskôr otvorené. Administrátori môžu tieto porty blokovať prostredníctvom firewallu, tak aby sa potom objavili vo filtrovanom stave. Filtrovaný port sa teda nachádza v tomto stave pokiaľ je chránený firewallom. Na filtrovanom porte nie je možné určiť, či je port otvorený, pretože filtrovanie paketov zabraňuje testom dosiahnuť tento port. Filtrovanie môže pochádzať z osobitného firewallového zariadenia, pravidiel routera alebo hostiteľského softwarového firewallu. [14] [13]

Spôsoby scanovania portov

Existuje viacero spôsobov, ako môžeme porty sledovať, scanovať. Niektoré z nich sú viac nápadné a je možné ich ľahko odhaliť, iné dokážu scanovať vzdialene porty bez toho aby si to dokázal niekto všimnúť. Väčšina typov scanov je dostupná len pre privilegovaných používateľov, z toho dôvodu, že posielajú a prijímajú neupravené pakety. Len jedna metóda môže byť použitá súčasne, s výnimkou UDP scanu, ktorý môže byt kombinovaný s ľubovoľným ďalším TCP scanom. [13]

Niektoré bežné metódy používané pri scanovaní portov:

Scan TCP SYN

SYN scan je predvoleným a najobľúbenejším typom scanu. Medzi jeho hlavné výhody patrí rýchlosť, keď dôkaze scanovat tisícky portov za sekundu v sieti bez firewallov. SYN scan je pomerne nenápadný a tajný, pretože nikdy nedokončí fázu nadväzovania TCP spojenia. Je schopný takisto spoľahlivo rozlíšiť stavy portov medzi otvorenými,

zatvorenými a filtrovanými. Tato metóda scanovania je tiež známa ako polootvorene scanovanie, pretože nie je potrebne otvárať plné TCP spojenie. Odošle sa iba SYN paket ako keby sa nadväzovalo skutočné spojenie a potom sa čaká na spojenie. Spiatočný SYN/ACK paket naznačuje, že port je otvorený, kým paket RST, čiže reset, udáva že port je zatvorený. Ak nebude doručená žiadna odpoveď ani po viacerých opakovaniach, port sa označí ako filtrovaný. Takéto označenie sa použije, aj keď príde chybová správa ICMP unreachable error (typ 3). [13]

Scan TCP connect()

Scan TCP connect() je predvoleným typom TCP scanu, ak SYN scan nepatrí medzi možnosti. K tomu dochádza, ak používateľ nemá privilégia na odosielanie neupravených paketov, alebo pri scanovani sietí s protokolom IPv6. Ak je dostupný SYN scan, je obyčajne lepšou voľbou. Scan TCP connect() sa snaží o normálne nadviazanie spojenia s otvoreným portom cieleného hostiteľa namiesto polootvoreneho scanovania SYN scan. Tento postup nielenže trvá dlhšie, ale takisto vyžaduje viac paketov na získanie tých istých informácií. Jednotlivé scanovania môžu byť zaznamenávané do logu a cieľových zariadeniach, z ktorého by administrátor, nemal mať problém rozpoznať, že išlo o scanovanie s cieľom nadviazať spojenie. [13]

UDP scany

Aj keď väčšina obľúbených služieb na internete funguje na TCP protokole, UDP služby sú tiež široko používané. Tri najbežnejšie z nich sú DNS, SNMP a DHCP. Pretože scanovanie UDP je všeobecne pomalšie a náročnejšie ako TCP, niektorí správcovia si tieto porty nevšímaj. Zneužitie UDP služieb je však celkom bežnou vecou. UDP scan odosiela cieľovému portu prázdnu hlavičku UDP header bez dát. Port je zatvorený ak sa vráti chybová sprava ICMP port unreachable error (typ 3, kod 3). Ostatné chybové správy ICMP (typ 3, kódy 1, 2, 9, 10 alebo 13) označujú port ako filtrovaný. Ak služba odpovedá UDP paketom, port je otvorený. Ak sa ani po opakovaných pokusoch neprijme žiadna odpoveď, port je označený ako otvorený/filtrovaný. To znamená, že port by mohol byt otvorený alebo možno paketové filtre blokujú komunikáciu. [13]

TCP Null, FIN a Xmas scany

Tieto tri typy scanov využívajú malú dieru v štandarde TCP RFC, aby rozlíšili porty, či ide o otvorené a zatvorené. Po prijatí paketu RST sa port považuje za zatvorený. Žiadna odpoveď označuje port za otvorený/filtrovaný. Port sa označí ako iba filtrovaný, ak dorazí chybová správa ICMP unreachable (typ 3, kod 1, 2, 3, 9, 10 alebo 13). Výhodou týchto scanov je, že ich pakety dokážu preniknúť aj cez bezstavové firewally a routre s filtrovaním paketov. Okrem toho sú ešte viac tajnejšie ako SYN scan, no aj tak detekovateľné. [13]

Scan TCP ACK

Tento typ scananovania sa líši od ostatných v tom, že slúži výhradné na zistenie, či je port filtrovaný, nikdy neurčuje porty v stave otvorený. Testovací ACK paket sa odošle na príslušný port, ak je daný port otvorený alebo zatvorený, vráti sa RST paket. Systém ich označí ako nefiltrovane, čo znamená, že sú dostupne pomocou ACK paketu. Porty, ktoré neodpovedajú sú označené ako filtrovane. [13]

FTP bounce scan

Jednou z funkcií protokolu FTP je podpora takzvaných proxy FTP spojení, čo umožňuje používateľovi pripojiť sa k jednému FTP serveru a potom žiadať o to, aby sa súbory posielali serveru tretej strany. Táto vlastnosť je ideálna a veľakrát zneužívaná, takže mnohé servery ju prestali podporovať. FTP server dokáže scanovat porty ostatných hostiteľských staníc a je možné požiadať FTP server o zaslanie súboru na hociktorý port cieľového hostiteľa. Podľa chybovej správy sa dá zistiť, či je port otvorený alebo nie. [13]

3 MONITOROVACIE METÓDY A NÁSTROJE

3.1 Meracie metódy

V priebehu niekoľkých rokov sa počet vytvorených sietí, prepojení medzi používateľmi niekoľko násobne zvýšil. Tento nárast je zapríčinený rozmachom celosvetovej siete, neustálym technických vývojom a objavovaním nových možností prenosu dát, ako napr. digitálna komunikácia. To malo za následok zvýšenú kontrolu, vylepšenia a zbieranie informácií o sieťovej prevádzke. Monitorovanie sieťovej prevádzky sa tak stalo sa stalo súčasťou spravovania sietí (network management). Súčasťou spravovania sietí je aj pasívne a aktívne meranie. [5] [15]

3.2 Pasívne monitorovanie

Účelom pasívneho monitorovania je sledovanie sieťového prenosu, činnosti a správania sa toku paketov, bez jeho modifikácie, resp. navyšovania jeho hodnoty práve týmto monitorovaním. To znamená, že sa do siete neposielajú žiadne testovacie pakety. Pasívne monitorovanie teda v tomto prípade dodatočne nezaťažuje prevádzku v počítačovej sieti ani jej zariadenia a monitoruje tak iba reálny sieťový prenos. Analyzujú a vyhodnocujú sa iba časové a objemové charakteristiky užívateľskej prevádzky, ktoré nie je možné namerať aktívnym monitorovaním. Meranie je uskutočňované sieťovými zariadeniami (routre, switche), ktoré sú nakonfigurované na realizáciu týchto meraní. Namerané informácie sú následne zozbierané bez akéhokoľvek ovplyvňovania sieťového prenosu. [5] [15]

Pasívne meranie slúži na získanie rôznych typov informácií, hlavne poznatkov o :

- rýchlosti doručovania paketov
- paket timing-u
- trafficu

Pasívne meranie je založené na zbere informácií potrebných pre zhodnotenie výsledku. Využívajú sa na to predovšetkým protokoly, ktorých vlastnosti a možnosti toto umožňujú a sú na nich založené bežne používané meracie nástroje pre meranie a monitorovanie stavu siete.

Medzi tieto protokoly patria:

- IPFIX
- SNMP
- RMON
- CMIP

Zhromažďovať dáta zo siete sa dá týmito spôsobmi:

1. Kopírovaním dát v uzle siete.

2. Pasívnym počúvaním.

3. Hardwarový merací prístroj.

3.2.1 Kopírovanie dát v uzle siete

Niektoré sieťové zariadenia, napr. prepínače (switche), ktoré pracujú na 2.vrstve OSI modelu, môžu byť nakonfigurované na preposielanie alebo zrkadlenie všetkých prechádzajúcich paketov z jedného portu na druhý, kde sa budú zhromažďovať. Toto riešenie je však náročné na výkon a môže hroziť preťaženie, kedy sa prepínač snaží preposlať viacej rýchlostných liniek na jeden port. [5]

3.2.2 Pasívne počúvanie

Pomocou rozbočovača (splitter) je možné pri pasívnom počúvaní zachytávať dáta na dátových vedeniach. Pasívne počúvať je možné na metalických aj na optických spojeniach. Rozbočovač je pasívny prvok a preto merania neovplyvňujú bežnú prevádzku. Rozbočovače nepotrebujú žiadne napájanie, čo je ich veľká výhoda, keďže dokážu fungovať aj pri výpadkoch napätia. [5]

3.2.3 Hardvérový merací prístroj

Použitie hardvérového meracieho prístroja je z týchto uvedených možnosti asi tá najhoršia. Hlavnou nevýhodou je nefunkčnosť zariadenia v prípade výpadku napätie a tým pádom aj celej sieťovej prevádzky, keďže zariadenie je priamo napojené do sieťovej infraštruktúry a všetka komunikácia musí prejsť cez neho. Tento problém sa dá však pomerne ľahko odstrániť napojením zariadenia na záložný zdroj energie APC. Zapojenie tohto monitorovacieho zariadenia je v celku jednoduché stačí ho iba umiestniť na ľubovoľné miesto, ktoré chceme monitorovať. Zariadenie následne kopíruje a analyzuje všetky

prechádzajúce dáta. Keďže z daného zariadenia sa dajú namerané údaje pomerne ľahko získať, je potrebne zabezpečiť prístup k tomuto zariadeniu len osobám na to určeným. Ďalšie problémy môžu nastať v prípade monitorovania vysokorýchlostnej linky, keď aj relatívne veľké uložisko dát v objeme jednotkách TB môže postačovať na monitorovanie len niekoľkých hodín alebo dni. Pri odstránení všetkých týchto záporov je ale monitorovanie pomocou hardwarového zariadenie veľmi praktické a dostačujúce riešenie. [5]

3.3 Aktívne monitorovanie

Aktívny prístup k meraniu sa zakladá na schopnosti vloženia testovacích paketov do siete alebo zaslania paketov na servery a aplikácie, ktorých stav chceme monitorovať. Hlavnou nevýhodou tohto merania je možné zvýšenie zaťaženia siete pripadne aj jej úplné preťaženie. Pri tomto meraní je preto dobre zvážiť či zasielanie týchto paketov výraznejšie nenaruší zaťaženie sieťovej infraštruktúry a namerane hodnoty nebudú skreslene oproti pôvodným hodnotám. Ďalším z možných problém môže nastať v prípade keď sa na sieti vyskytne problém v časovom úseku, na ktorý sa pravé nedotazujeme. Pre administrátora to môže znamenať, že sa o danej chybe na sieti ani nemusí dozvedieť. Medzi bežne používané nástroje aktívneho monitorovania patria napr. ping, ktorý meria oneskorenie a stratu paketov, a traceroute, ktorý pomáha určiť topológiu siete. Oba tieto meracie nástroje posielajú ICMP pakety na hostiteľské zariadenie a čakajú na jeho spätnú reakciu, z ktorej získavajú potrebne informácie. [5] [15]

4 VÝBER VHODNÉHO MONITOROVACIEHO SYSTÉMU PRE IMPLEMENTÁCIU

4.1 Kritéria pre výber vhodného kandidáta

Požiadavky, ktoré by mal byt monitorovací systém schopný vykonávať sú hlavné kritéria pre výber vhodného kandidáta. Pri monitorovacích systémoch je potrebné sledovať najmä dostupnosť a funkčnosť hardwarových a softwarových častí siete, ako aj kľúčových služieb na systémoch. Pri sledovaní systémov pomocou agentov je vhodne sledovať predovšetkým kľúčové parametre operačného systému (využitie procesoru, dostupnosť pamäte, voľná kapacita diskových polí). Dané sledované parametre je potreba zaznamenávať a štatisticky vyhodnocovať pomocou grafov v nastaviteľnej čase dobe.

V prípade výskytu problémového stavu alebo výpadku niektorej zo služieb by mal byť monitorovací systém schopný zaslať správu (email, SMS, RSS) administrátorovi, ktorý môže tak okamžite reagovať na vzniknutý stav. Pomocou skriptov alebo automatických príkazov je takisto možné použiť automatizovanú nápravu priamo na serveri (napr.: reštart servera). Možnosť sledovania výkonnostných parametrov databázových a webových serverov, aktívnu činnosť užívateľov na monitorovacích zaradeniach (prihlásenie, spustenie služieb a programov) patri takisto medzi dôležité požiadavky na monitorovací systém.

4.2 Požiadavky na monitorovací systém

4.2.1 Monitorovanie stavu operačného systému a jeho služieb

Systém by mal byť schopný v pravidelných intervaloch testovať dostupnosť sieťových služieb, merať hodnoty dôležitých parametrov systému, monitorovať súbory s logovacími informáciami atď.

4.2.2 Oznamovanie

Pri vyskytnutí sa kritických alebo nebezpečných problémov by malo dôjsť k archivovaniu dát napr.: do databáze a následnému upozorneniu administrátora, väčšinou pomocou mailu alebo SMS. Nastavenia kritických hlásení sa konfigurujú najčastejšie pomocou webového rozhrania. V správe by nemalo chýbať potrebné množstvo informácií potrebných k dostatočnému popisu problému a jeho riešenia.

4.2.3 Znalosť monitorovacích prvkov

Systém by mal dostatočne poznať vlastnosti a operácie jednotlivých monitorovaných prvkov aby mohol jednoznačne rozhodnúť či ide len o zvýšenú záťaž, a nealarmovať zbytočne správcov alebo sa blíži problémový stav. Dobrou konfiguráciou monitorovacieho systému sa dá vyhnúť týmto falošným poplašným oznámeniam.

4.2.4 Robustnosť systému a odolnosť voči výpadkom

Systém dokáže detekovať problémy s agentmi (chybový stav) a je schopný ich automaticky obnoviť. Sebakontrola serveru alebo kontrola z iného zariadenia by mala byť dostatočná ochrana pred zlyhaním serveru.

4.2.5 Bezpečnosť

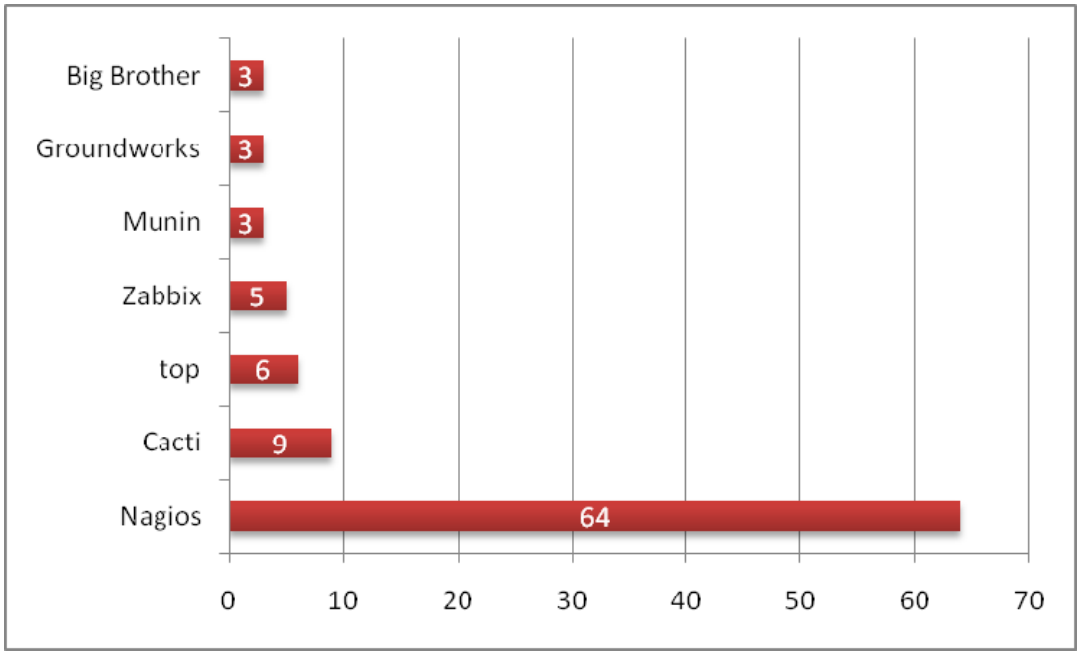
Prvky monitorovacieho systému by mali medzi sebou komunikovať zabezpečeným spojením, aby sa zabránilo nežiadanému úniku nameraných informácií.

4.2.6 Administrácia a správa

Možnosť konfigurácie a nastavenia parametrov monitorovacieho systému a jeho súčasti. Najjednoduchšia a najpraktickejšia administrácia je prostredníctvom webové rozhranie na danej IP adrese. Definovanie užívateľov s rôznymi oprávneniami na správu tohto webového rozhrania.

5 NAGIOS

Dá sa povedať zrejme najznámejším a najpoužívanejším sieťovým monitorovacím systémom je program Nagios. História Nagiosu sa píše od roku 1999, kedy ho začal vyvíjať Ethan Galstad pod názvom NetSaint. Od roku 2002 bol projekt kvôli licenčným nezhodám s podobnou značkou nútený zmeniť názov. Premenoval na súčasný názov Nagios. Názov N.A.G.I.O.S. je skratkou slovného spojenia – „Nagios Ain't Gonna Insist On Sainthood“, čo sa dá preložiť ako : „Nagios, nie je pripravený stať sa svätým“. Názov a logo Nagios sa stali ochrannou známkou vzniknutej spoločnosti Nagios Enterprises, ktorej prezidentom je pravé Ethan Galstad . Projekt je distribuovaný pod licenciou GNU GPL (GNU's Not Unix General Public Licence), čo motivovalo ostatných vývojárov zapojiť” sa do jeho vývoja. Program pod touto licenciou je možné voľne kopírovať, distribuovať, modifikovať pre osobné a komerčné použitie. Po viac než 10 ročnom vývoji je Nagios považovaný za jeden z najlepších monitorovacích systémov o čom svedčia aj každoročné ocenenia medzi monitorovacími systémami. Nagios nemonitoruje iba sieťové zariadenia (server, switch, tlačiareň), ale ponúka komplexné lokálne a vzdialené testovanie aj serverových (mailová pošta, web server, databáza) a sieťových služieb (ping, bežiace procesy, zaťaženie systému, system uptime, vyťaženosť procesorov atď). [1] [5] [6]



Obr. 3 Graf z roku 2009, zobrazujúci anketu “Best of Open Source Software Awards” od webovej IT stránky InfoWorld

5.1 Možnosti a charakteristika:

- Monitorovanie sieťových služieb SMTP, POP3, HTTP, NNTP, PING, atd.
- Monitorovanie hostiteľských zdrojov napr. : záťaž procesoru, využitie diskov a pamätí, bežiace procesy, logovacie súbory atd.
- Monitorovanie Unix/Linux, Windows, and Netware serverov
- Monitorovanie aktívnych prvkov napr.: router and switch
- Monitorovanie teploty komponentov hostiteľskej stanice
- Použití svojich vlastných kontrolných skriptov a mechanizmov
- Schopnosť definovať sieťovú hostiteľskú hierarchiu
- Možnosť zaslania varovnej správy (SMS, e-mail) rôznym kontaktným skupinám
- Uchovanie stavu zariadení a služieb aj po reštarte
- Vizualizácia problémov a aktuálneho sieťového stavu pomocou WWW rozhrania
- Nastavenie rôznych prístupových povolení pre jednotlivé užívateľské skupiny

Systémové požiadavky :

- PC s operacním systémem Linux
- Web server napr. Apache
- PHP
- MySQL

5.2 Architektúra

Monitorovací systém Nagios funguje na pomerne jednoduchom princípe. Pomocou definovaných príkazov (pluginov) vykonáva kontroly na hostiteľských zariadení a ich služieb. Ak kontrola skončí chybou, udalosť je nahlásená zodpovedajúcim osobám, administrátorom, formou oznámenia s potrebnými informáciami na jej odstránenie. [8]

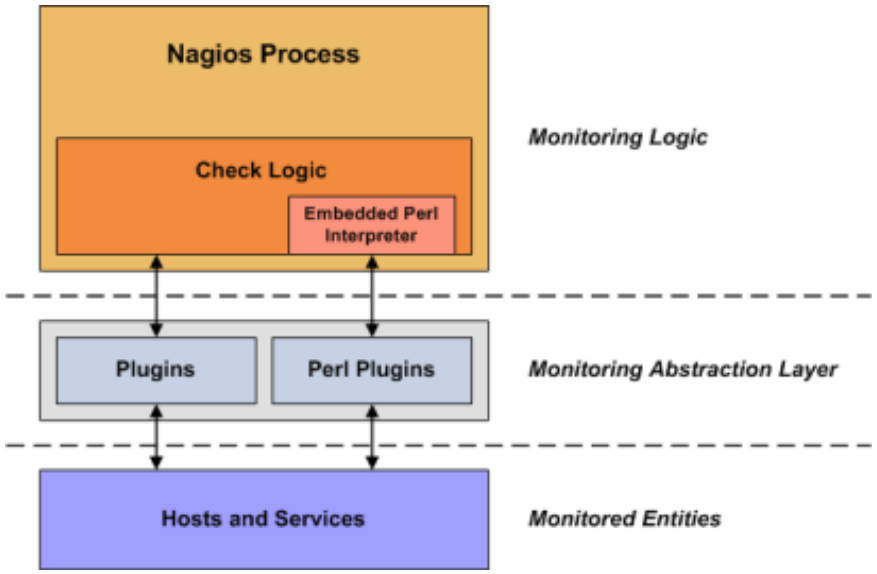
5.2.1 Nagios Demon

Hlavnou časťou Nagiosu je démon, ktorý sám o sebe nemá žiadnu schopnosť ani neobsahuje žiadne funkcie pre samotné monitorovanie. Na to aby bol systém Nagios, a jeho démon schopný monitoringu je potrebne doinštalovať zásuvné moduly (pluginy), ktoré vykonávajú monitorovacie a testovacie funkcie. Zásuvné moduly sú preto nevyhnutnou súčasťou pre monitorovanie siete. Monitorovanie prebieha na základe načítania hlavného konfiguračného súboru nagios.cfg a ďalších konfiguračných súborov jednotlivých pluginov, ktoré sa využívajú na monitorovanie. Namerane hodnoty sú najskôr

ukladané do dočasných súborov a z nich sú následne ukladané do databáze. Webové rozhranie, ktoré slúži na zobrazovanie výsledných hodnôt, je realizované pomocou niekoľkých CGI skriptov. Tie pristupujú do databáze a zobrazujú ich ako HTML stránky. [8] [6]

5.2.2 Pluginy

Samotné jadro Nagiosu neobsahuje žiadne interné mechanizmy na sledovanie hostiteľských staníc a ich služieb na sieti. Preto Nagios využíva pluginy, čiže externé programy a skripty (Perl skripty, shell skripty), ktoré vykonávajú testy jednotlivých služieb. Nagios spúšťa plugin vždy keď je nutné skontrolovať potrebné zriadenie alebo službu. Plugin vracia späť na terminál výstup, ktorý musí obsahovať do 80 znakov a návratovú hodnotu 0 do 3, ktorá reprezentuje stavy, ktoré vie Nagios z pluginov vyhodnotiť. [8]



Obr. 4 Pluginy vo funkcii abstraktnej vrstvy medzi démonom a monitorovanými zriadeniami a službami

5.2.3 Stavy a návratové hodnoty

Stav hostiteľa alebo jeho služby je vyhodnocovaný návratovými kódmi zo zásuvných modulov. Každý z návratových kódov, presne reprezentuje status služby alebo hostiteľa v akom sa nachádza. Status služby môže nadobúdať jeden zo 4 stavov:

Návratový kód zásuvného modulu	Status služby	Status hostiteľa
0	ok	UP
1	warning	UP or DOWN
2	critical	DOWN/UNREACHABLE
3	unknown	DOWN/UNREACHABLE

Tabuľka 2 Návratové hodnoty z pluginov

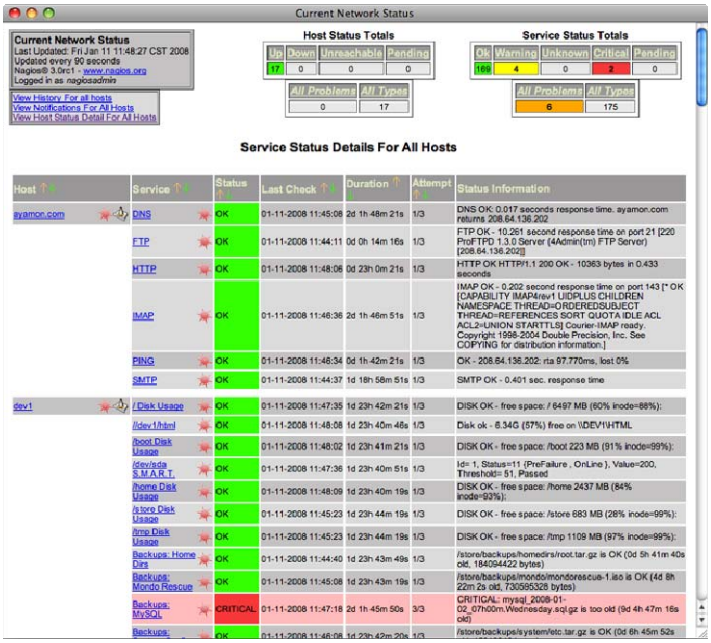
Statusy služby:

- **OK** – Plugin môže danú službu otestovať a je vyhodnotená ako správne pracujúca služba.
- **WARNING** – Plugin je schopný otestovať službu, no získal varovnú hodnotu zadefinovanú administrátorom. Ide však o problém, ktorý neohrozuje funkčnosť služby.
- **UNKNOWN** – Plugin nie je schopný otestovať službu alebo sa stav služby nedá spoľahlivo určiť.
- **CRITICAL** –Plugin vyhodnotí , že daná službu z nejakého dôvodu nie je funkčná alebo dosiahla kritickú hodnotu.

Statusy hostiteľa:

- **OK** – Hostiteľ odpovedá na Ping
- **DOWN** – Hostiteľ neodpovedá na Ping
- **UNREACHABLE** – Hostiteľ je nedostupný, ak závisí na nejakom inom Hostiteľ. Nagios teda nemôže hostiteľa skontrolovať, preto ho označí, že je v nedosiahnuteľný. Tieto stavy majú 2 typy:
- **SOFT** – V mäkkom stave sa hostiteľ alebo služba nachádza, ak kontrola skončí v jednom z chybových stavov a kontrola služby prebehla menejkrát ako je nastavený maximálny počet opakovaní. Pri tomto stave, sa ešte žiadne upozornenia neodosielajú.

- **HARD** – Nastáva ak počet opakovaní kontrol dosiahne maximálny limit a služba je stále nedostupná. Pri detekovaní hostiteľa alebo služby v tomto stave Nagios posiela notifikácie na určené kontakty o možnom chybovom stave. Rozlíšenie tvrdých a mäkkých stavov zabraňuje zbytočným zasielaniam poplašných sprav.



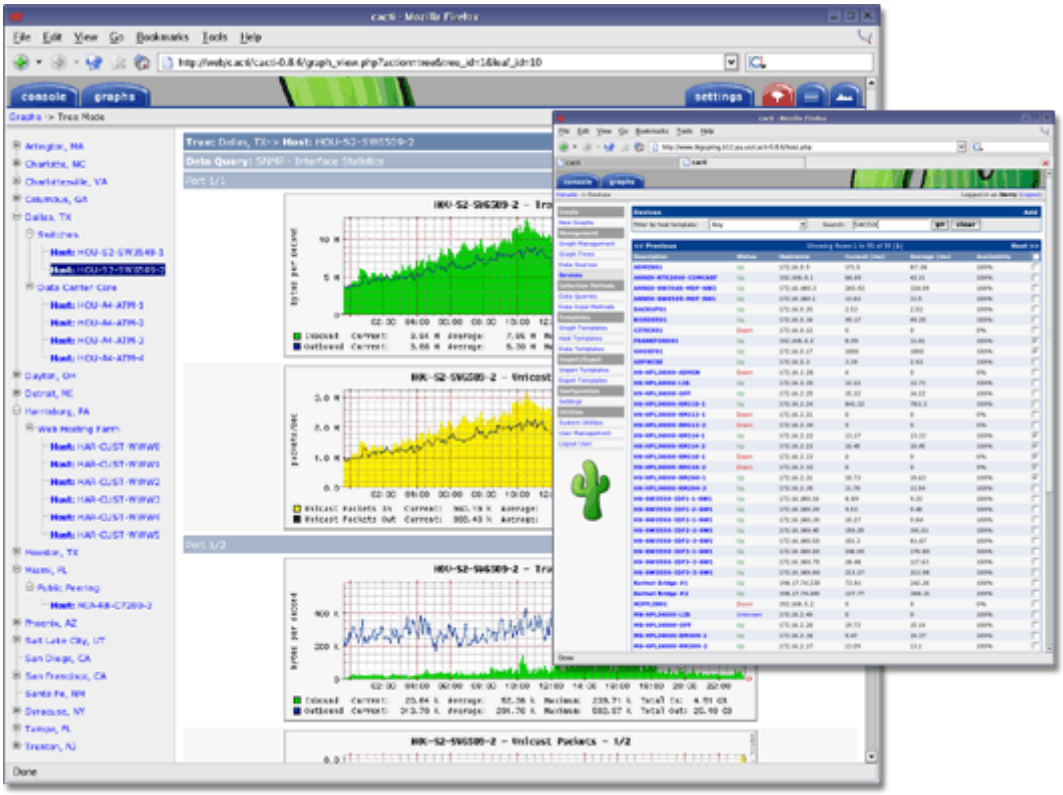
Obr. 5 Detailné zobrazenie stavu služieb v administratívnom webovom rozhraní.

6 CACTI

Cacti je takisto veľmi populárny open-source monitorovací nástroj, ktorý je na rozdiel od Nagiosu napísaný v jazyku PHP. Ide o vynikajúci a bezplatný nástroj pre monitorovanie zariadení a ich služieb v sieti s výstupom v podobe pekných a prehľadných grafov.

Cacti je veľmi univerzálny monitorovací systém, keďže je podporovaný stále silnejšou komunitou užívateľov, ktorí sa zapájajú do jeho rozvoja prostredníctvom rôznych šablón a skriptov, takže bežné použitie je pomocou nich oveľa jednoduchšie. Celý systém je nadstavbou nad nástrojom RRDTool (Round Robin Database Tool). RRDTool je softwarový open-source nástroj slúžiaci k merania, ukladaniu a zobrazovaniu štruktúrovaných dát vo forme grafického výstupu. Je nástupcom obdobného, veľmi populárneho nástroja MRTG, ktorý bol ale primárne určený k monitorovaniu a grafovaniu sieťových kariet. Mal však niekoľko obmedzení, ktoré podnietili vznik RRDTool, napr. : zobrazovanie maximálne dvoch hodnôt v grafe, vzhľad grafu sa dal meniť iba minimálne, chýbala podpora vyberania časových úsekov, za ktoré chceme zobraziť graf.

Cacti je nástroj, ktorý umožňuje monitorovať a vytvárať grafy takmer zo všetkých obliatí monitorovania. Disponuje veľmi kvalitným a intuitívnym webovým rozhraním, množstvom pluginov a šablón. Tieto komponenty mu dávajú otvorenosť pre vlastné získavanie dát a vytváranie svojich grafov a prehľadov. Vytváranie grafov uľahčujú šablóny, predinštalované sú napr. šablóny pre Unix/Linux, Windows, Novell (CPU, pamäť, dátový tok), sieťové karty atď. Vďaka šablónam od užívateľov je ale možné monitorovať aj napr. : Cisco switche (vyťaženie portov, chyby na portoch), tlačiarne (zostávajúce množstvo náplne), odozvy na ping atd. [11] [12] [6]



Obr. 6 Grafické rozhranie softwaru Cacti

Ďalšie vlastnosti Cacti:

- udržuje zoznam a dostupnosť monitorovaných zariadení aj po reštarte
- Schopnosť zasielať varovné e-maily v prípade poruchy
- grafy môžu byť združované do prehľadov a zobrazované za ľubovoľné obdobie
- možnosť importu a exportu šablón (xml)
- možnosť exportu nameraných dát
- tvorba vlastných zdrojov dát, šablón, grafov, šablón celých zariadení
- nastaviteľné pravá pre užívateľov na prezeranie grafov
- rozšíriteľnosť vďaka pluginom

Systémové požiadavky:

- Cacti funguje pod operačnými systémami Linux/Unix a Windows

Potrebný software:

- Apache server
- Cacti software

- Spine
- RRDTool
- PHP 4.3.6+ or 5.x
- MySQL 4.x or MySQL 5.x
- Cygwin
- Net-SNMP
- Perl – potrebný pre niektoré skripty

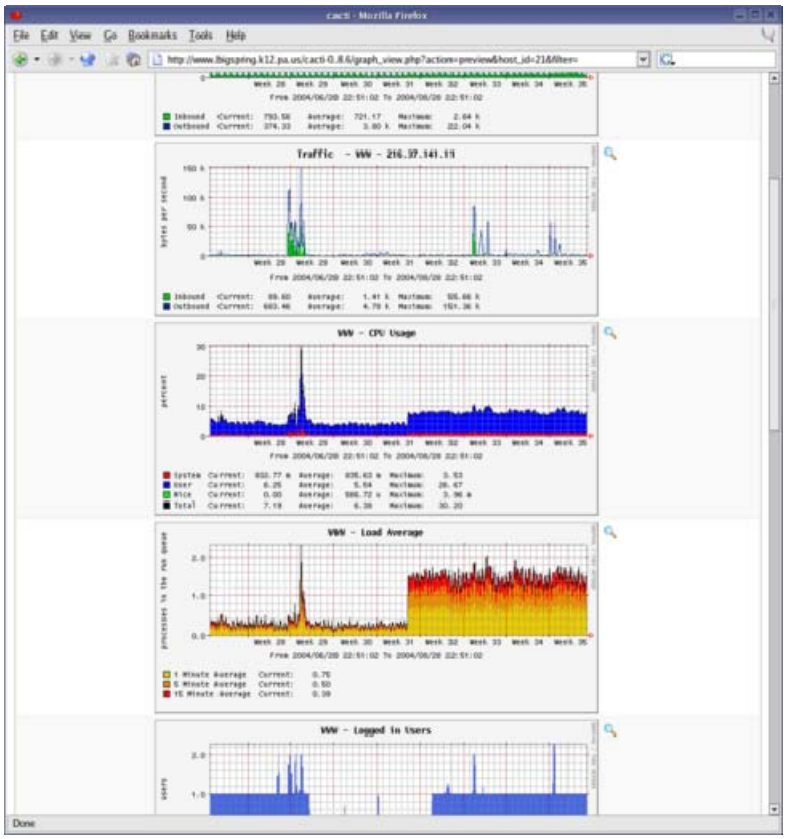
6.1 Architektúra

Úloha Cacti by sa dala rozdeliť do troch časti:

- získanie dát
- uloženie dát
- zobrazenie dát

Existujú dva základné spôsoby získavania dát – SNMP a skripty. Primárne sa dáta získavajú pomocou protokolu SNMP, ale je možné využiť aj rôzne typy skriptov. SNMP je podrobne popísané v kapitole 2 . V systému je niekoľko šablón pracujúcich s SNMP. Na získavanie požadovaných hodnôt z monitorovacích zariadení slúži tzv. poller (ten je operačným systémom plánovaný k pravidelnému spúšťaniu), ktorý pomocou PHP získava dáta. Pooler je možné prispôsobiť potrebám monitorovania podľa vlastných predstáv, napr. : je možné nastaviť počet spúšťaných procesov, počet dotazov, ktoré môže každý z nich vykonávať, časové intervaly, v ktorých ma prebiehať zber dát. V prípade problémov sa do logu môžu zaznamenávať aj jednotlivé dotazy a odpovedi. Cacti obsahuje aj vlastní parser logu, ktorý dokáže z logu vybrať požadované dáta. [11] [12] [6]

Takisto ukladanie prebieha dvoma spôsobmi. Niektoré dáta sa ukladajú do SQL databáze, ale hlavné dáta sa s pomocou RRDToolu ukladajú do kompaktného súboru. RRDTool slúži takisto aj k zobrazeniu týchto dát do grafov.



Obr. 7 Ukážka grafického vyhodnotenia nameraných hodnôt

6.2 Vytvorenie sledovania

Ako prvé je vždy potrebné vytvoriť zariadenie, ktoré chceme monitorovať pomocou Devices. Stačí teda iba pridať hostiteľa, vyplniť názov zariadenia spoločne s jeho IP adresou, zvoliť verziu SNMP, ktorú chceme využívať pri overovaní jeho dostupnosti (ping nebo SNMP). Následne pomocou šablóny vytvoriť zdroj dát (Data Sources), z ktorého sa pomocou Graph Managementu vytvorí výsledný graf, ktorý je pridaný do zvolenej skupiny pre zobrazenie (Graph Trees). Takto pripravené grafy je možné ďalej exportovať (pomocou ftp).

6.3 Pluginy a šablóny

Na používanie prídavných externých pluginov je najskôr nutné nainštalovať Plugin Architecture. Implementácia pluginov je už potom iba otázkou nakopírovania daných súborov na správne miesto a zapísanie pluginu do konfiguračného súboru. Veľkou výhodou je široká základňa užívateľov, ktorí na servery spoločnosti Cacti umiestňujú dostatočné množstvo šablón a pluginov na stiahnutie, ktorých inštalácia je veľmi jednoduchá. Šablóny sú uložené vo formáte XML a pre inštaláciu ich je potrebné iba

importovať pomocou webového rozhrania. Export funguje na rovnakom princípe. Exportovať je možné aj vlastné šablóny a poskytnúť ich ostatným alebo ich iba importovať na iný Cacti server. [11]

Niektoré najznámejšie a najpoužívanejšie pluginy:

Backup – umožňuje zazálohovať konfiguráciu a dáta celého Cacti systému.
Discovery – plugin automaticky vyhľadá v sieti zariadenia používajúce SNMP a umožní ich ľahko pridať do Cacti pre možné monitorovanie.
Thold – umožňuje vytvoriť, nastaviť a monitorovať tresholdy a zasielať e-mailové upozornenia pri prekročení limitnej hodnoty.

Reports - Umožňuje definovať časové úseky, v ktorých sa budú e-mailom zasielať grafy.

Manage - Umožňuje vzdialene spravovať zariadenia, servery, služby a monitorovať ich stav.

NCP - Nagios Plugin for Cacti. Umožňuje prepojenie s monitorovacím systémom Nagios.

7 PRTG NETWORK MONITOR

PRTG (Paessler Router Traffic Grapher) Network Monitor je vysoko účinný nástroj pre dohľad a monitorovanie počítačové infraštruktúry od nemeckej spoločnosti Paessler, ktorá je už od roku 1997 certifikovaným partnerom spoločností Cisco, Microsoft a Vmware. Hlavným zameraním tohto programu je proces sledovania jednotlivých funkčných procesov celej počítačovej siete vrátané všetkých pripojených zariadení. Účelom tohto moderného nástroja je bezpečnosť, maximálna výkonnosť a prevencia pred výpadkami. PRTG Network Monitor dokáže sledovať dátový tok na linkách vo vnútri sieti, zachytávať pakety, zaznamenávať objem dát pretekajúci cez sieťové zariadenie aj s podporou SNMP (router, switch, firewall,…). Podporuje aj hĺbkové analýzy a vytvára správy o pozorované činnosti. PRTG Network Monitor je prioritne určený pre chod na platforme Windows v sieti s neustálym zaznamenávaním parametrov. Zaznamenané údaje sú uložené v internej databáze pre neskoršie použitie. Pomocou použiteľného webového užívateľského rozhrania je možné ľahko konfigurovať zariadenia a senzory, ktoré chcete sledovať. Pre vzdialený prístup disponuje PRTG Network Monitor vstavaným webovým serverom, ktorý zaisťuje ľahký prístup ku grafom a tabuľkám. [7]

PRTG podporuje všetky bežné metódy pre získavanie dát:

- SNMP and WMI
- Packet Sniffing
- NetFlow, jFlow, and sFlow

7.1 Základne vlastnosti a funkcie

Program zaisťuje kompletný monitoring siete

- Monitorovanie downloadu a uploadu
- LAN, WAN, VPN a viacsieťový monitoring
- Zobrazovanie výsledkov pomocou grafov
- Pre všetky typy sietí
- Rozhranie API (Application programming interface) na bázy protokolu HTTP slúžiace k prepojeniu s ďalšími aplikáciami
- Automatická konfigurácia zisťovania sieti a senzorov

7.2 Systémové požiadavky pre PRTG Network Monitor

- PC, server alebo virtuálny stroj
- Priemerne výkonné CPU (doporučené od roku 2007)
- 1024 MB RAM
- Microsoft® Windows (32/64 bit), Linux, MacOS
- Google Chrome (doporučený), Firefox alebo Internet Explorer

Priemerný PC/sever vyrobený v roku 2007 a neskôr by mal byť schopný monitoringu až pomocou 1000 senzorov súčasne (výnimku môžu robiť senzory s podporou SNMP v3, WMI, packet sniffing a VMware). [7]

7.3 Základný popis činnosti

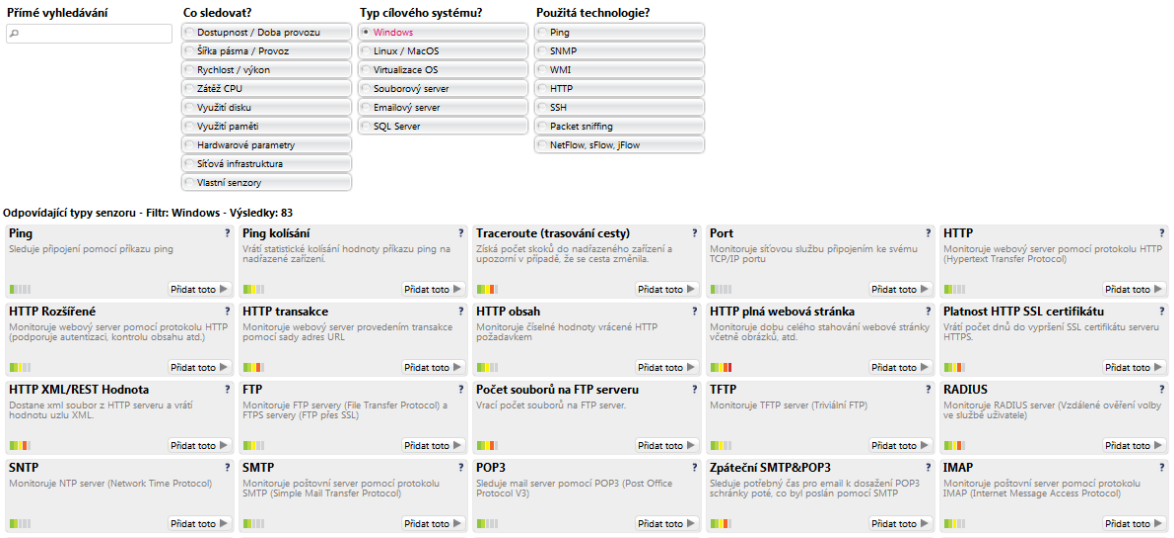
Služba pozostáva z aktívnych senzorov umiestnených na sonde, ktoré vykonávajú samotnú kontrolu danej služby, aplikácie, hodnoty a podobne. Tieto senzory kontrolujú všetky bežné hodnoty, ako sú ping, miesto na disku, zaťaženie CPU, sieťový tok atd. Sonda je malá výkonná aplikácia, ktorá býva inštalovaná priamo na server v lokálnej sieti. Rovnako tak je možné inštalovať sondu aj do virtuálneho prostredia. Základným prvkom je hlavní server (core server), ktorý zaisťuje zber dát a ich následné vyhodnotenie, archivovanie, upozornenie na prípadne problémy, vyhotovenie reportov a mnoho ďalších činností. Senzor vyhodnocuje hodnoty a stavy a údaje predáva sonde, ktorá dáta spracováva, komprimuje a šifrovaným kanálom posiela na hlavný server. Ak je niektorá hodnota mimo dovoleného rozsahu, okamžite sa odosielajú potrebne notifikácie. [7]

7.3.1 Senzory a protokoly

PRTG Network Monitor zahrňuje veľké množstvo senzorov pre všetky bežné sieťové služby (napr. Ping, HHTP, SMTP, POP3, FTP atd.), umožňujúce sledovanie sieťových systémov.

- Viac ako 100 typov senzorov (Ping, HTTP, WMI, SMTP, POP3, DNS, FTP a mnoho ďalších)
- Prenos v sieti a analýza chovania pomocou SNMP, NetFlow a sledovania paketov
- Automatické rozpoznávanie a monitorované viacprocesorových systémov - chytré senzory
- Predkonfigurované šablóny zariadení pre routre Cisco, servery SQL, sieťové tlačiarne

- Senzory pre monitorovanie virtuálne prostredia (VMware, XEN, HyperV apod.)
- Programovateľné triggery a senzory
- Virtual Server Monitoring
- SLA monitoring
- QoS Monitoring (VoIP)
- IPv6 support



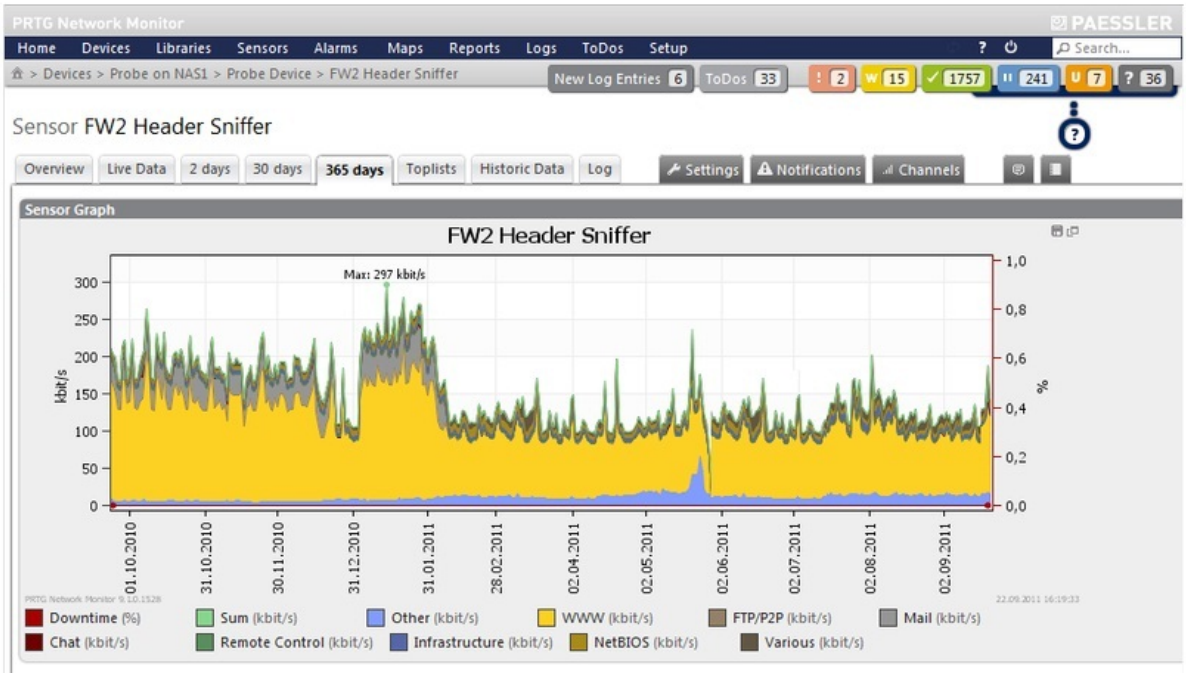
Obr. 8 Ukážka niekoľkých senzorov pre platformu Windows

7.3.2 Zobrazenie a webové rozhranie

PRTG je užitočný nástroj pre zistenie aktuálneho stavu využitia siete, identifikáciu problematických mies. Používa diagramy zobrazujúce stav v reálnom čase a dlhodobej štatistiky. Vzdialený prístup je umožnený aj cez špeciálne mobilné rozhranie mobilného prehliadača. Ďalším spôsobom je využitie tejto aplikácie na systémoch MAC s plnou podporou pre iPhone a iPad alebo cez tiež Android aplikáciu pre mobilné zariadenia a tablety postavene na tomto operačnom systéme. [7]

- Elegantné, rýchle a výkonné webové rozhraní
- Integrácia aplikácie Google Maps
- Voliteľné grafické rozhraní Windows GUI
- Natívna Windows aplikácia dostupná v 7 jazykoch
- Hierarchické zobrazení (sondy, skupiny, zariadenia, senzory, kanály)

- Zoznam senzorov (abecední, najrýchlejší, najpomalší, podľa typu, podľa OS atd.)
- Prepracované grafy zobrazujúce monitorované dáta v reálnom čase, za posledné hodiny 2/24/48, posledných 30 dní a posledných 365 dní
- 'Mapy' umožňujúce vlastné nastavenie, ktoré prepojujú stav monitorovania, grafy a tabuľky, a umožňujú individuálne rozloženie



Obr. 9 Grafické zobrazenie nameraných hodnôt za obdobie 365 dni cez webové užívateľské rozhranie

7.3.3 Oznámenia a reporty

PRTG ponúka niekoľko možností oznámenia. Najčastejšie sa využívajú notifikácie vo forme emailu alebo SMS správ, spustení aplikácie, zaslaním syslog správy, prehraním zvukov atd. Časy jednotlivých reportov sú neustále zaznamenávané v databáze a je možné spätne spracovať výpadky z ktoréhokoľvek okamžiku. PRTG je schopený vytvoriť alebo ukladať denné/týždenné/mesačné/ročné reporty o vybraných senzoroch. Reporty je možné konfigurovať a môžu byť zasielané e-mailom ako PDF alebo sa ukladajú na pevný disk. K dispozícii sú rôzne šablóny, ktoré zahrňujú rôzne sady dátových tabuliek a grafov. [7]

- Upozornenie podľa individuálne nakonfigurovaných kritérií
- Rôzne spôsoby oznamovania (e-mail, SMS, správa na pager, žiadosť HTTP, syslog apod.)

- Periodické hlásenia s možnosťou vlastného nastavenia (HTML, PDF)

7.3.4 Prečo sa nedá použiť SQL databáza

SQL server je vhodný pre mnoho vecí, ale pre ukladanie mnoho malých dát v krátkych intervaloch to nie je vhodné riešenie. Preto program PRTG využíva svoju vlastnú databázu vo formáte, ktorý je optimalizovaný pre ukladanie nameraných dát. Tato databáze je integrovaná v „core“ servere a nie je potreba dáta nikam inam prenášať a je až 100x rýchlejšia ako SQL Server. Navyše nie treba žiadna údržba a konfigurácia, všetko riadi „core“ server sám.

8 POROVNANIE VYBRANÝCH MONITOROVACÍCH RIEŠENÍ

8.1 Nagios

Nagios je jeden z prvých voľne šíriteľných monitorovacích systémov. Je neustále vyvíjaný a vylepšovaný pod licenciou GNU/GPL, čím sa stal jedným z najlepších open source monitorovacích systémov. Primárne je určený na monitorovanie serverov a služieb na platforme Linux a Unix, ale dokáže monitorovať aj systémy na platforme Windows.

Obr. 10 Logo Nagios

Nagios je vhodným pre monitoring väčších sietí so skúsenými administrátormi linuxového operačného systému. Inštalácia je jednoduchá, no sfunkčnenie a konfigurácia prináša veľa problémov, no s pomocou dobré nápovedy a užívateľského manuálu je tento proces o niečo jednoduchší. Na konfiguráciu nie je vytvorené žiadne rozhranie, musí sa robiť manuálnou editáciou konfiguračných súborov. Akákoľvek chyba, napríklad v syntaxi ktoréhokoľvek konfiguračného súboru, má za následok pád a nefunkčnosť celého systému. Nagios neponúka mnoho funkcionality pre správu databázy. Výstupy sú používateľovi prístupné pomocou web rozhrania, ktoré je celkom kvalitne spracované, avšak pri väčšom množstve výstupov sa stáva pomerne neprehľadné. Navzdory tomu, že Nagios je kvalitný monitorovací nastroj a patrí medzi tie najkvalitnejšie, kvôli veľkej náročnosti konfigurácie a ladeniu systému, tento program nie je potrebné inštalovať na serveri U5.

Výhody:

- konfigurácia pomocou šablón
- GNU/GPL licencia
- rozšírenie pomocou pluginov
- podpora monitorovania bez agenta, s agentom alebo kombináciu oboch prístupov

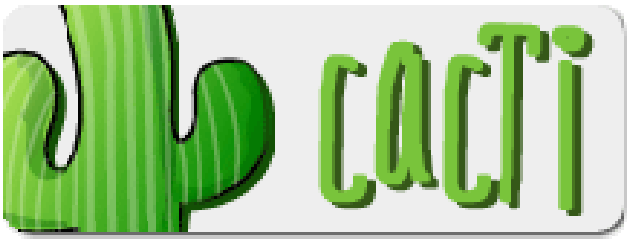
Nevýhody:

- zdĺhavá a zložitá konfigurácia
- chýba podpora vykresľovania grafov

- veľa pluginov nemá definované príklady nastavení

8.2 Cacti

Cacti je plne graficky orientovaný open source monitorovací nástroj založený na RRDTool. Primárne bol vyvíjaný pre linuxový operačný systém, v dnešnej dobe je ho možné inštalovať už aj na zariadenia so systémom Windows, ktoré je možné aj monitorovať. Samotná inštalácia je pomerne zložitá keďže je na plné fungovanie nutné nainštalovať niekoľko externých programov(PHP, MySQL, webový server atd.), ktorých konfigurácia aj podľa užívateľského manuálu nie je jednoduchá. Kompletnú administráciu a ovládanie je možné vykonávať v prehľadnom jednoduchom a intuitívnom grafickom rozhraní, ktoré je najsilnejšou stránkou tohto nastroja. Ďalšou výhodou Cacti je existencia množstva šablón a tiež pluginov, ktoré dokážu viacnásobne rozšíriť primárne funkcie programu. Cacti je výborným monitorovacím nástrojom pre menšie LAN siete ako aj pre rozsiahly komplex sieti s tisíckami zariadení.



Obr. 11 Logo Cacti

Výhody:

- Open Source
- jednoduché používanie pomocou webového rozhrania
- integrovaná podpora vykresľovania grafov
- grafy môžu byť zväčšované pomocou Javascriptu
- veľká podpora vývojárskej komunity

Nevýhody:

- zložitejšia inštalácia
- obmedzená možnosť použitia interaktívnych dynamických grafov
- zmena frekvencie kontroly spôsobí stratu doposiaľ nameraných hodnôt

8.3 PRTG

PRTG Network Monitor je výkonný komerčný prostriedok pre monitorovanie všetkých druhov sietí. Navzdory tomu že ide o komerčné riešenie, je možné využiť trial a freeware verzie tohto programu. Trial verzia poskytuje kompletnú funkcionalitu programu po dobu 30 dni, zatiaľ čo monitorovanie freeware verziou je možné iba pomocou 10 senzorov, čo je však dostačujúce pre mnoho užívateľov, čoho dôkazom je aj 150 000 freeware užívateľov po celom svete. Využíva širokou radu technológii k meraniu vyťaženia stavu siete a monitorovaniu dostupnosti sieťových zariadení a všetkých bežných sieťových služieb. Inštalácia a konfigurácia prvého merania je otázkou niekoľkých minút. Pridávanie senzorov je takisto veľmi intuitívne a jednoduché, k čomu pomáhajú aj výstižné popisy jednotlivých senzorov. Grafické webové rozhranie je prispôsobené užívateľskému rozhraniu Windows. Vykresľovanie grafov je možné hneď po spustení monitorovania s následnou širokou konfiguráciou jednotlivých grafov.

Obr. 12 Logo PRTG

Výhody:

- aj vo verzii freeware veľmi kvalitný monitorovací nástroj
- jednoduchá inštalácia a konfigurácia
- konfigurácia grafov
- 5 rôznych rozhraní pre monitorovanie a správu dát

Nevýhody:

- komerčné riešenie je pre menšie firmy s jednoduchým monitorovaním príliš drahé
- menej známy monitorovací nástroj

8.4 Výber vhodného monitorovacieho systému

V dnešnej dobe existuje na trhu veľké množstvo monitorovacích systémov a kvalita voľne šíriteľných systémov je už viac-menej porovnateľná s komerčnými riešeniami. Pravé Nagios a Cacti patria medzi tie najkvalitnejšie open sourcové monitorovacie nástroje. Hlavne svojou inštaláciou a následnou konfiguráciou samotného systému však nepatria medzi jednoduché systémy a vyžadujú adekvátne zručnosti. PRTG je síce komerčným produktom, no vo svojej freeware verzii je vďaka svojej jednoduchosti, ovládateľnosti a dobre spracovanými grafmi ideálnym nástrojom na monitorovanie záťaže hlavného sieťového uzlu na budove U5.

II. PRAKTICKÁ ČÁST

9 IMPLEMENTÁCIA NÁSTROJA PRTG NETWORK MONITOR

V praktickej časti tejto diplomovej práce sa budem venovať aplikovaniu vybraného nástroja PRTG Network Manager, ktorý bude monitorovať a analyzovať dátový tok hlavného servera Fakulty Aplikovanej Informatiky. Monitoring by mal slúžiť na dlhodobé sledovanie a kontrolu dátového toku na tomto serveri, aby bolo zo získaných informácií možné rozpoznať prípadné zvýšené zaťaženie siete a jeho dôvody. Pomocou tohto riešenia bude možné ľahko určiť, ktorá služba alebo zariadenie vyťažuje sieťovú infraštruktúru najviac a poprípade prehodnotiť ich ďalšie využívanie. Grafické a tabuľkové spracovanie nameraných údajov je na vysokej úrovni, pomocou filtrácie a konfigurácie je možné výraznou mierou uľahčiť analýzu a vyhodnotenie nameraných dát.

9.1 Vytvorenie testovacieho servera

Keďže testovanie a skúšanie jednotlivých monitorovacích nástrojov prebiehalo za plnej prevádzky servera, nebolo vhodné vykonávať tieto operácie na hlavnom fyzickom serveri. Pri konfigurácií a ladeniu nástrojov by mohlo ľahko dôjsť k znefunkčneniu servera, čo by malo za následok prerušenie spojenia medzi budovou U5 a okolitého sveta. Z tohto dôvodu bola vytvorená kopia toho servera, určená výhradne na testovanie a konfiguráciu. Ďalej bolo potrebne vyčleniť pre toto zariadenie verejnú IP adresu 195.178.94.9 pre možnosť vzdialeného prístupu.

9.1.1 Inštalácia a konfigurácia

Aby bolo možné na danom mirrory sledovať dátový tok hlavného servera, bolo nutné pomocou par príkazov nakonfigurovať Cisco switch. Táto funkcia sa vola Switched Port Analyzer (SPAN), port mirroring alebo port monitoring.

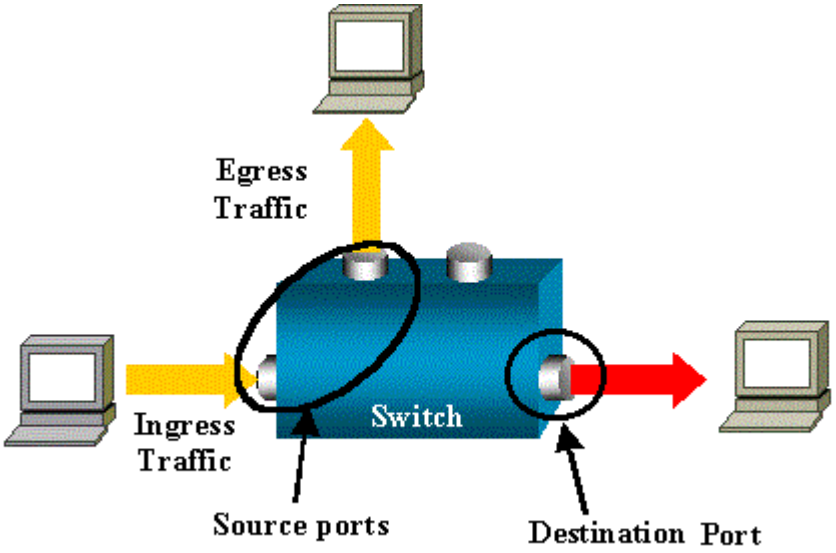
Switch(config)# no monitor session 1

Switch(config)# monitor session 1 source interface Gi0/49

Switch(config)# monitor session 1 filter vlan 51 – 650

Switch(config)# monitor session 1 destination interface Gi0/16

Pomocou príkazu *no monitor session 1* zrušíme prípadné vytvorené prepojenie session 1. Príkaz *monitor session 1 source interface Gi0/49* bol použitý na monitorovanie zdrojového portu 0/49 na Gigabitovom pripojení. Port 0/49 je vstupný port na hlavnom serveri, cez ktorý smeruje cely dátový tok budovy U5. Nasledujúci príkaz *monitor session 1 filter vlan 51 – 650* definuje rozsah VLAN sieti , na ktorých bude možné prebiehať monitorovanie a príkaz *monitor session 1 destination interface Gi0/16* definuje cieľový gigabitový port 0/16, na ktorý bude dané spojenie kopírované. V tomto prípade ide o port na vytvorenej kópii hlavného servera.[4]

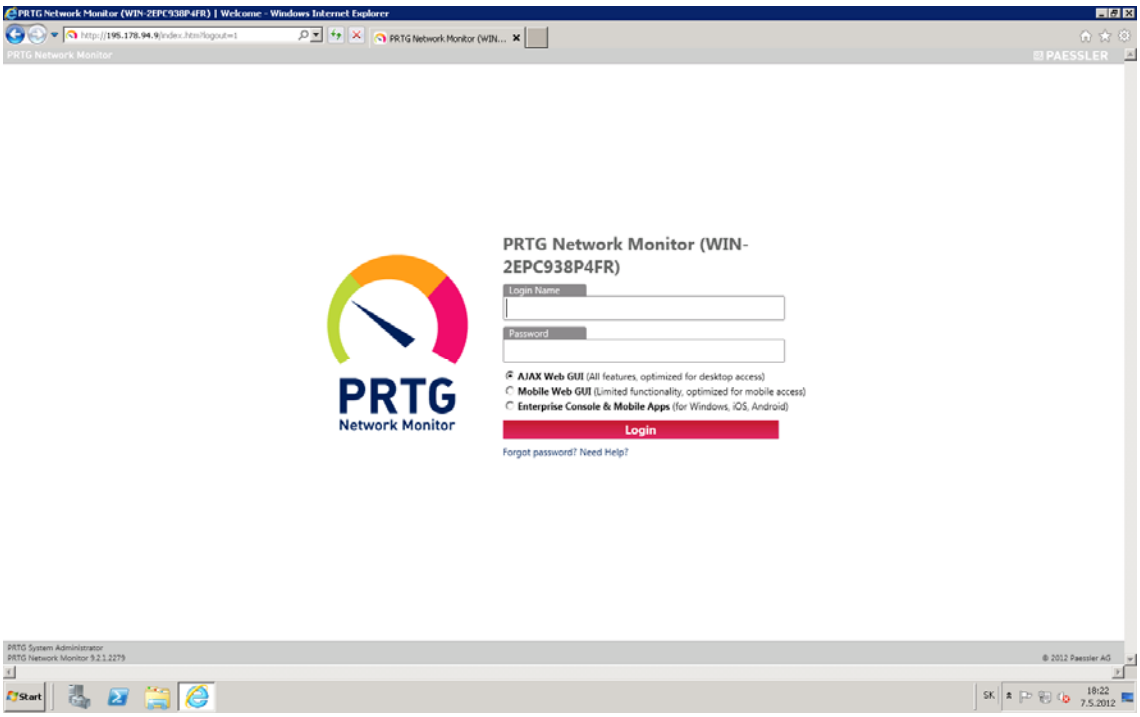


Obr. 13 Popis funkcie SPAN - Switched Port Analyzer

- Ingress traffic – dátový tok vstupujúci do switchu.
- Egress traffic – dátový tok vystupujúci zo switchu.
- Source port – zdrojový/monitorovaný port.
- Destination port – cieľový port, monitoruje zdrojový port (často býva na neho pripojený sieťový hardwarový analyzátor).

9.2 Inštalácia monitorovacieho nástroja

Keďže spoločnosť Peassler vyvíjala tento software prioritne pre platformu Windows, na vytvorenej kópii servera bol nainštalovaný Windows Server 2008 R2 Standard SP1. PRTG Network Monitor nepotrebuje na inštaláciu a využívanie žiadne externé programy ani doplnky, preto pre nainštalovanie bolo potrebné iba stiahnuť inštalačný balíček z domovskej stránky http://www.paessler.com/download. Po aplikovaní aktivačného kľúča sa nám sprístupní 30 dňová trial verzia, ktorá ma rovnaké vlastnosti ako zakúpená verzia. Po uplynutí tejto doby sa software zmení na verziu freeware, ktorá podporuje monitorovanie iba s desiatimi súčasne aktívnymi senzormi, čo je pre účely tohto monitorovania viac ako dostačujúce. Po úspešnej inštalácii už nie je nutné ďalej nič konfigurovať, po zadaní IP adresy (195.178.94.9) tohto servera do jedného z podporovaných prehliadačov sa automaticky spusti logovacie okno webového grafického rozhrania.



Obr. 14 Logovacie okno do systemu PRTG

Prvé logovanie do tohto rozhrania je možné iba prostredníctvom tlačidla *Default login*, ktoré sa automaticky stratí po prvom prihlásení a užívateľ je vyzvaný na okamžitú zmenu hesla. Ide o výborný spôsob ako zabrániť nežiadanému vstupu, keďže zistiť defaultné prihlasovacie údaje nie je problém.

Podporované sú 3 druhy prihlásení:

AJAX Web GUI (všetky funkcie, optimalizované pre bežný desktopový prístup)

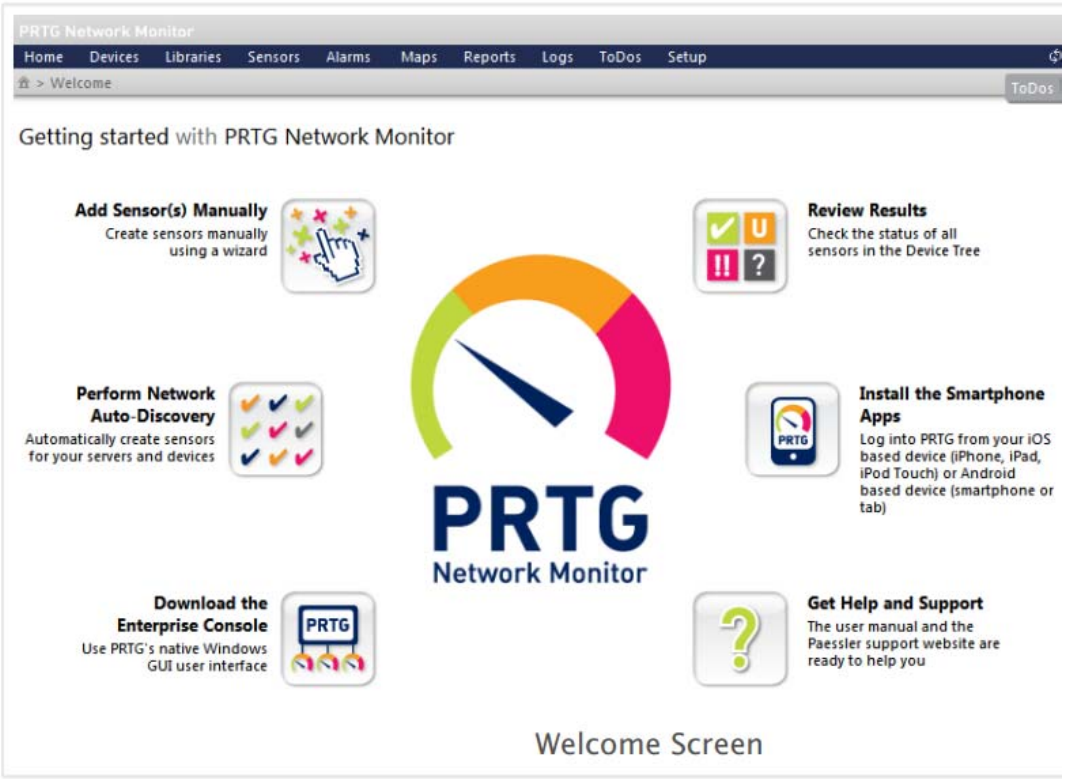
Mobile Web GUI (obmedzená funkcionalita, optimalizované pre mobilný prístup)

Enterprise Console & Mobile Apps (pre iOS a Android)

9.2.1 Vytvorenie sledovania pomocou rozhrania Ajax Web Interface

Ajax (Asynchronous JavaScript and XML) je populárny nástroj na umiestňovanie interaktívnych komponentov na webové stránky. Vďaka tejto technológií je možné z webového prehliadača elegantne komunikovať s webovým serverom a vymieňať si s ním dáta, ktoré sa môžu ihneď uložiť na server alebo naopak zobraziť u klienta.

Webové rozhranie založené na tomto princípe je hlavným vstupom do PRTG. Využíva sa na konfiguráciu zariadení a senzorov, analýzu monitorovaných údajov, správu upozornení a vytvorenie reportov.



Obr. 15 Uvítacia obrazovka PRTG s uľahčeným prístupom ku všetkým potrebným informáciám a nastaveniam

9.2.2 Pridanie nového zariadenia

Prvým krokom k spusteniu monitorovania je pridanie zariadení, ktoré chceme monitorovať. Každé zariadenie pridané do zoznamu reprezentuje reálne hardware zariadenie s vlastnou IP adresou v sieti ak napr.:

- Webový alebo súborový server
- Osobný počítač (Windows, Linux, Mac OS)
- Router alebo switch

PRTG podporuje dva druhy pridávania zariadení:

- Auto-Discovery
- Manuálne pridanie

Auto-discovery

Funkcia auto-discovery je výborný spôsob ako automaticky vytvoriť sofistikovanú a ucelenú sadu senzorov pre celu sieť. Primárne sa využíva pre menšie a stredne siete LAN s podporou SNMP a WMI. Proces auto detekcie sa rozdeľuje na 3 fázy:

- Skenuje časti siete a hľadá všetky dostupné zariadenia pomocou Pingu
- Zisťuje o aké typy zariadení ide pomocou SNMP, WMI a ostatných protokolov
- Vytvorenie sady senzorov pre jednotlivé zariadenia

Auto detekcia môže byť spúšťaná aj v pravidelných intervaloch (hodina, deň, týždeň) a okamžite môžu byť do zoznamu pridané novo pripojené zariadenia. Do zoznamu monitorovaných zariadení môžu byť pridané iba zariadenia odpovedajúce na Ping. Ak firewall blokuje žiadosti echo, zariadenie neodpovedá a nie je možné ho pridať do zoznamu.

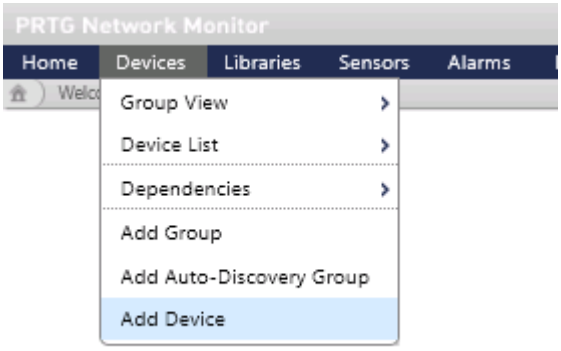
Spustenie auto detekcie je možné dvoma spôsobmi:

- Na uvítacej obrazovke použiť možnosť *Perform Network Auto-Discovery*
- Z hlavného menu zvoliť *Devices | Add Auto-Discovery Group*

Keďže úlohou tejto práce je iba monitorovať dátový tok na hlavnom serveri, uprednostnil som radšej možnosť manuálneho pridania zariadenia.

Manuálne pridanie

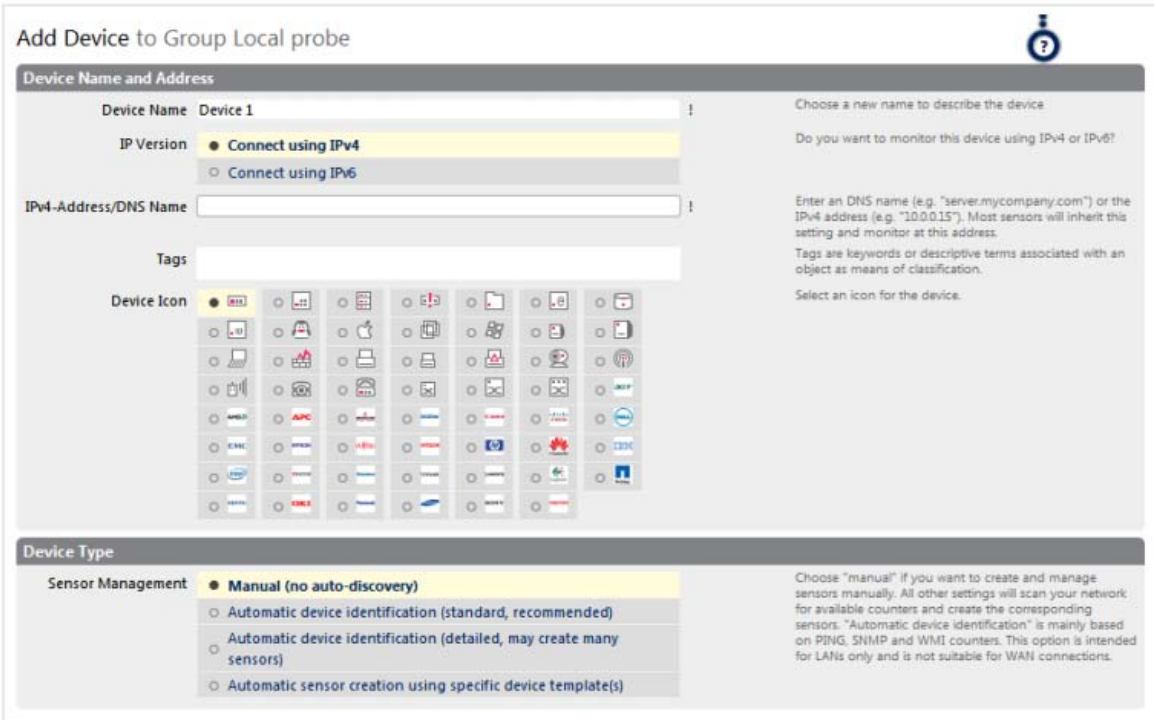
Využitie funkcie auto-discovery nie je vždy potrebné alebo dostačujúce, preto existuje aj možnosť manuálneho pridania zariadení. Využíva sa hlavne na pridanie zariadení, ktoré sa nepodarilo rozpoznať pri auto detekčnom hľadaní.



Obr. 16 Pridanie zariadenia z hlavneho menu

Manuálne pridanie zariadenia je veľmi jednoduché. Z hlavného menu zvolíme možnosť Devices | Add Device a pomocou asistenta vyplníme všetky potrebne informácie:

- Názov zariadenia
- Verzia IP adresy
- IP adresu alebo DNS názov
- Typ zariadenia



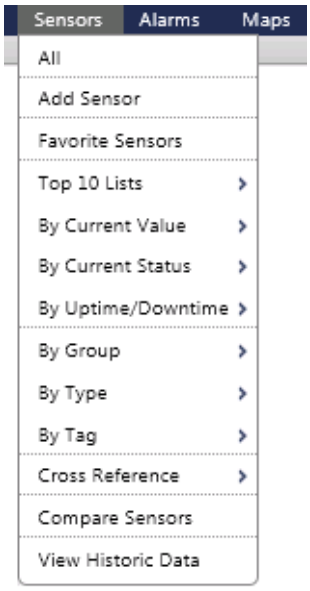
Obr. 17 Asistent nastavenia a konfigurácie nového zariadenia

Zariadenie je týmto spôsobom pridane do zoznamu a pripravené na aplikovanie potrebných senzorov. Software PRTG dodatočné automaticky pridáva zariadenie *Probe Device*. Ide o interné systémové zariadenie, ktoré reprezentuje zariadenie, na ktorom je umiestnená monitorovacia sonda. V tomto prípade ide o mirror hlavného servera čiže nie je nutné opätovne pridávať rovnaké zariadenie druhý krát.

9.2.3 Pridanie senzorov

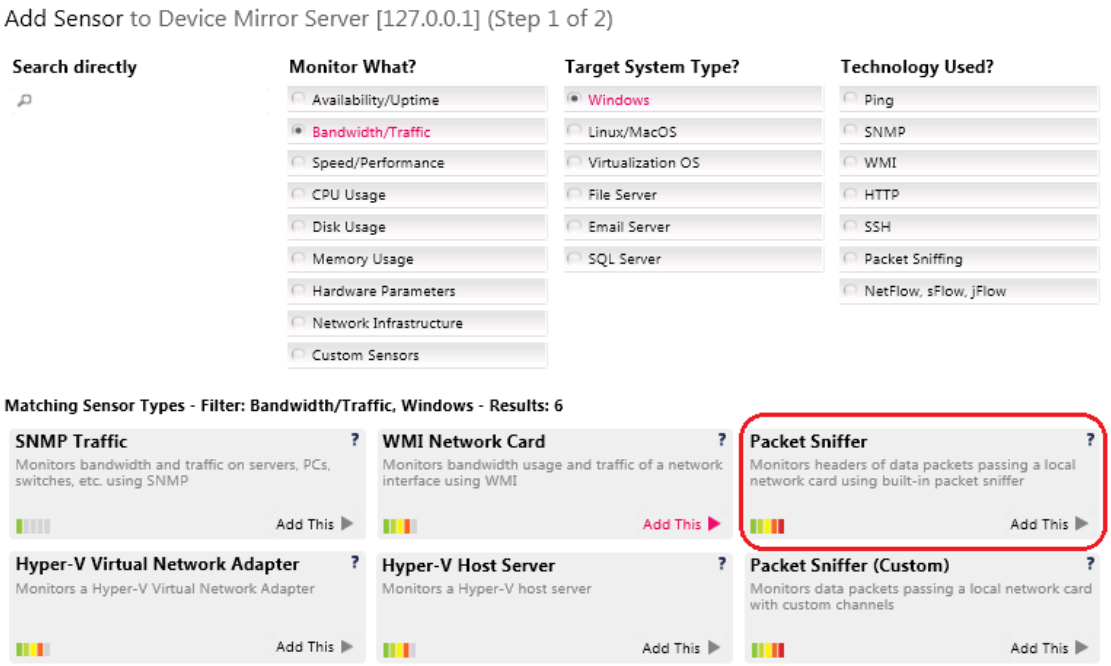
Na každé zariadenie je možné pripojiť niekoľko senzorov, z ktorých každý monitoruje jeden aspekt daného zariadenia. Takisto existuje viacero spôsobov ako je možné pridať senzor na zariadenie.

- Na uvítacej obrazovke použiť možnosť *Add Sensors Manually*
- Z hlavného menu zvoliť *Sensors* | *Add Sensor*



Obr. 18 Pridanie senzorov podľa rôznych kategórii

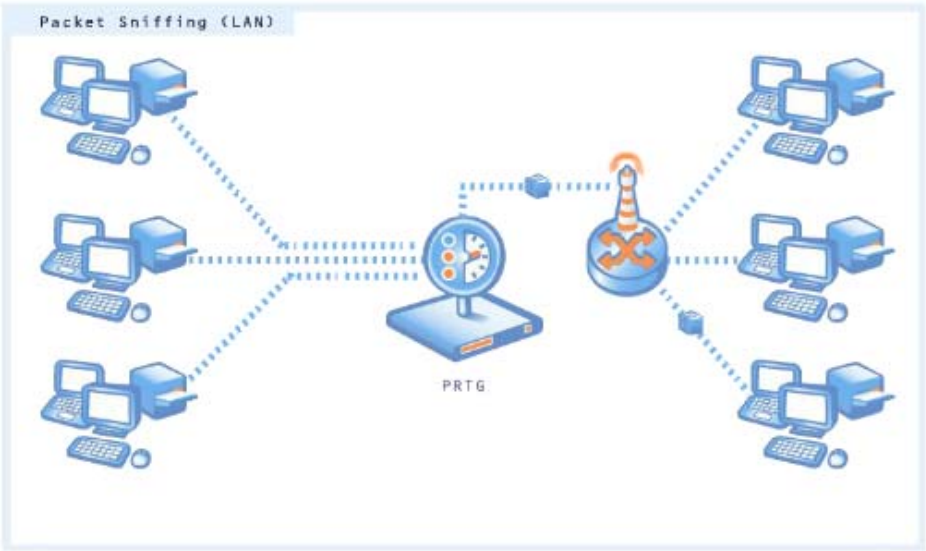
Hlavné menu ponúka širokú možnosť výberu senzorov. Na výber je okolo 100 senzorov rozdelených podľa rôznych kategórií. Ešte než si dáky senzor vyberieme, je nutné zvoliť zariadenie, na ktoré ho chceme pripojiť. Potom už môžeme vybrať senzor, ktorý vyhovuje naším požiadavkám. Na naše účely je vhodných niekoľko senzorov, ktoré dokážu monitorovať dátový tok rôznymi technológiami. Keďže hlavný firewall celej univerzity blokuje zber informácií pomocou protokolu SNMP, zvolil som senzor s technológiou Packet Sniffing.



Obr. 19 Všetky dostupné senzory pre platformu Windows na monitorovanie dátového toku v sieti

9.3 Senzor Packet Sniffer

Packet Sniffer senzor monitoruje hlavičky dátových paketov prechádzajúcich sieťovou kartou pomocou vstavaného paketového snifferu. Je ideálnym monitorovacím prostriedkom, pokiaľ potrebujeme zistiť, ktoré aplikácie alebo IP adresy spôsobujú vyťaženie siete. Obsahuje preddefinovane kanály s možnosťou ich pridania a odobratia. Tento senzor môže byť umiestnený iba na zariadení Probe Device. PRTG vypočítavá celkovú záťaž siete zo všetkých sieťových dátových paketov, ktoré prechádzajú sieťovou kartou alebo sú posielane monitorovacím portom na switchi (obr.).



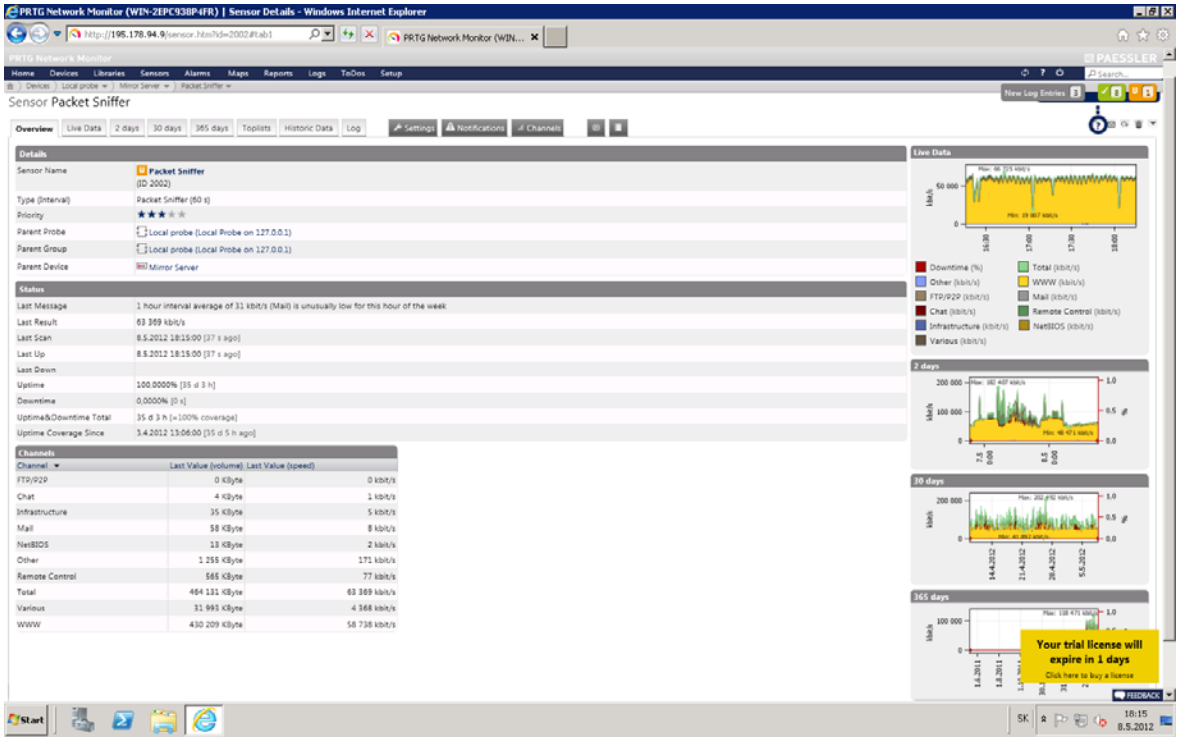
Obr. 20 PRTG monitorovanie zariadení prostredníctvom Packet Sniffer senzoru

Použitie Packet Sniffera zvažujeme hlavne vtedy ak sieťové zariadenia nepodporujú SNMP protokol alebo ak je potrebne rozlíšiť vyťaženie siete jednotlivými protokolmi a IP adresami. Senzor Packet Sniffer podporuje využívanie Toplistov, v ktorých si môžeme prehľadne pozrieť tabuľku či grafické prevedenie Top užívateľov, Top spojení, Top odosielateľov atd. V porovnaní so všetkými štyrmi podporovanými technológiami na monitorovanie dátového toku a vyťaženosti liniek v programe PRTG (SNMP, WMI, xFlow and Packet Sniffer) pravé Packet Sniffer spôsobuje sledovaním každého jedného paketu najvyššie vyťaženie procesora a zaťaženie linky, preto by mal byt využívaný iba v malých a stredných sieťach, na dedikovaných (vyhradených len na jeden účel) počítačoch veľkých sietí alebo individuálnych počítačoch. Packet Sniffer prezerá iba hlavičku každého paketu s cieľom zistiť IP adresu a port odosielateľa a prijímateľa. Ide o veľmi rýchlu a efektívnu metódy, aj keď nie vždy presnú, napr. : monitorovanie záťaže protokolu HTTP je možné iba na bežných portoch 80, 8080 a 443, záťaž na neštandartných portoch nie je možné identifikovať.

9.3.1 Detailný pohľad na senzor Packet Sniffer

Už na prvý pohľad pôsobí užívateľský veľmi prijemne a orientovať sa v ňom dokáže takmer ktokoľvek aj bez potrebných administrátorských zručnosti. Z úvodnej obrazovky

tohto senzora mame okamžitý prístup ku všetkým nameraným dátam v rôznych podobách, ku konfigurácii a nastaveniam senzora, ako aj notifikáciám, logom a archivácii dát.



Obr. 21 Úvodná obrazovka senzoru Packet Sniffer

Úvodná obrazovka poskytuje kompletný prehľad s najdôležitejšími údajmi. V prvom okne sú základne informácie o senzore, jeho názov a ID, typ senzoru s intervalom monitorovania a názvy zariadenia, sondy a skupiny ktorým je sonda pridelená.

Details	
Sensor Name	Packet Sniffer
	(ID 2002)
Type (Interval)	Packet Sniffer (60 s)
Parent Probe	Local probe (Local Probe on 127.0.0.1)
Parent Group	Local probe (Local Probe on 127.0.0.1)
Parent Device	Mirror Server

Tabuľka 3 Detaily o senzore Packet Sniffer

Ďalšia tabuľka zobrazuje podrobne informácie o fungovaní senzoru, kde nájdeme hodnotu posledného merania, čas posledného skenovania a údaje o celkovej dobe prevádzky s možnými výpadkami a hláseniami.

Status	
Sensor Status (for Complete Cluster)	
Last Message	1 hour interval average of 1 661 kbit/s (Other) is unusually high for this hour of the week
Last Result	117 009 kbit/s
Last Scan	9.5.2012 12:34:00 [48 s ago]
Last Up	9.5.2012 12:34:00 [48 s ago]
Last Down	-
Uptime	100,0000% [35 d 22 h]
Downtime	0,0000% [0 s]
Uptime & Downtime Total	35 d 22 h [=100% coverage]
Uptime Coverage Since	3.4.2012 13:06:00 [35 d 23 h ago]

Tabuľka 4 Informácie o aktivite senzora Packet Sniffer

Posledný tabuľkový údaj z úvodnej obrazovky senzoru je vyhodnotenie rýchlosti a preneseného objemu dát za posledné meranie pre všetky aktívne kanály.

Channels		
Channel	Last Value (volume)	Last Value (speed)
Total	931 651 KByte	127 201 kbit/s
WWW	732 129 KByte	99 960 kbit/s
Remote Control	133 991 KByte	18 294 kbit/s
Various	63 807 KByte	8 712 kbit/s
Mail	1 098 KByte	150 kbit/s
Infrastructure	419 KByte	57 kbit/s
Other	113 KByte	15 kbit/s
NetBIOS	81 KByte	11 kbit/s
Chat	10 KByte	1 kbit/s
FTP/P2P	3 KByte	0,43kbit/s

Tabuľka 5 Vyhodnotenie rýchlosti a preneseného objemu dát za posledné meranie

Na pravej strane úvodnej obrazovky máme k dispozícii náhľady grafov za posledné časové obdobia, ktoré ponuku ju rýchly prehľad o stave monitorovania. Po rozkliknutí

ktoréhokoľvek náhľadu sa nám zobrazí na celu obrazovku detailne spracované grafické vyhodnotenie s príslušnou tabuľkou údajov. Obe reprezentácie nameraných hodnôt sú aktualizované podľa nastavenej dobe skenovania, v tomto prípade 60s.

9.3.2 Konfigurácia senzoru Packet Sniffer

Konfigurácia senzora nie je potrebná pre bežné využívanie. Všetky potrebné parametre sú automaticky nastavené pri inštalácii senzora. Nastaviť sa dá pomerne veľké množstvo parametrov ako napr: interval skenovania, jednotky v grafe, konfigurácia kanálov, prístupové pravá ku grafom alebo filtrovanie paketov. Spomeniem predovšetkým filtrovanie paketov, ktoré som musel aj aktívne využiť. Paket Sniffer vo svojom základnom nastavení nerozoznáva uploadované a downloadované pakety, ale vyhodnocuje všetky odchádzajúce a prichádzajúce pakety dokopy. Aby bolo možné monitorovať zvlášť upload a download, musel som na zariadenia pridať ďalšie dva senzory typu Paket Sniffer, ktoré som pomocou nastavenia Include Filter zadefinoval rozsahy všetkých IP adries, ktoré sú na budove U5 a ktoré môžu komunikovať s okolitým svetom. Zadefinovanie týchto adries muselo byt presne podľa noriem, ktoré je schopný PRTG spracovať. Paket Sniffer následné po prehliadnutí hlavičiek paketov a analyzovaní IP adries zisti či ide o prichádzajúci alebo odchádzajúci paket a buď ho cez filter prepustí alebo ho ignoruje.

Zoznam IP adries na budove U5:

10.5.8.0/22

10.5.16.0/22

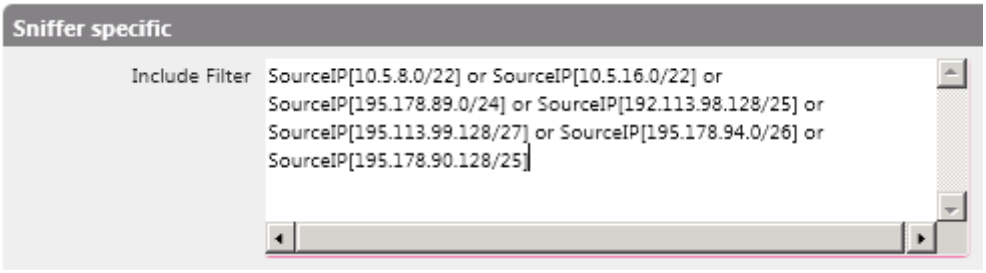
195.178.89.0/24

195.113.98.128/25

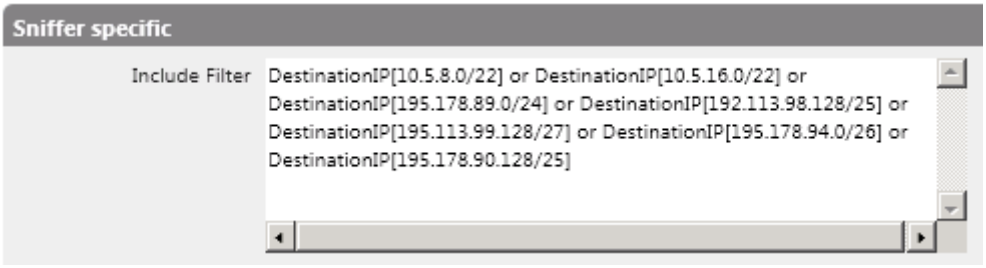
195.113.99.128/27

195.178.94.0/26

195.178.90.128/25



Obr. 22 Nastavenie Include Filtru pre Packet Sniffer – uplink, filtrujúci všetky zdrojové IP adresy



Obr. 23 Nastavenie Include Filtru pre Packet Sniffer – downlink, filtrujúci všetky cieľové IP adresy

10 ANALÝZA NAMERANÝCH DÁT

Analýza dátových tokov umožňuje identifikovať spôsob spracovávania informácii a dát so zameraním na ich prenos, výmenu a uchovávanie. Výstupom analýzy je správa popisujúca najmä kľúčové miesta spracovávania informácii a spôsoby ich prenosu. Súčasťou správy môžu byť aj prehľadné diagramy dátových tokov zachytávajúce celý životný cyklus stanovených informácií. Výstup merania a analýzy je vhodný aj pre využitie v ďalších možných projektoch fakulty, ktorej cieľom môže byt napríklad optimalizácia dátových liniek a skvalitnenie poskytovaných služieb.

Hlavne dôvody na analýzu dátového toku:

- lokalizácia kľúčových miest spracovávania informácii
- podporuje optimalizáciu komunikácie a interných procesov
- napomáha pri rozhodovaní o možných nových zmenách súčasného informačného systému

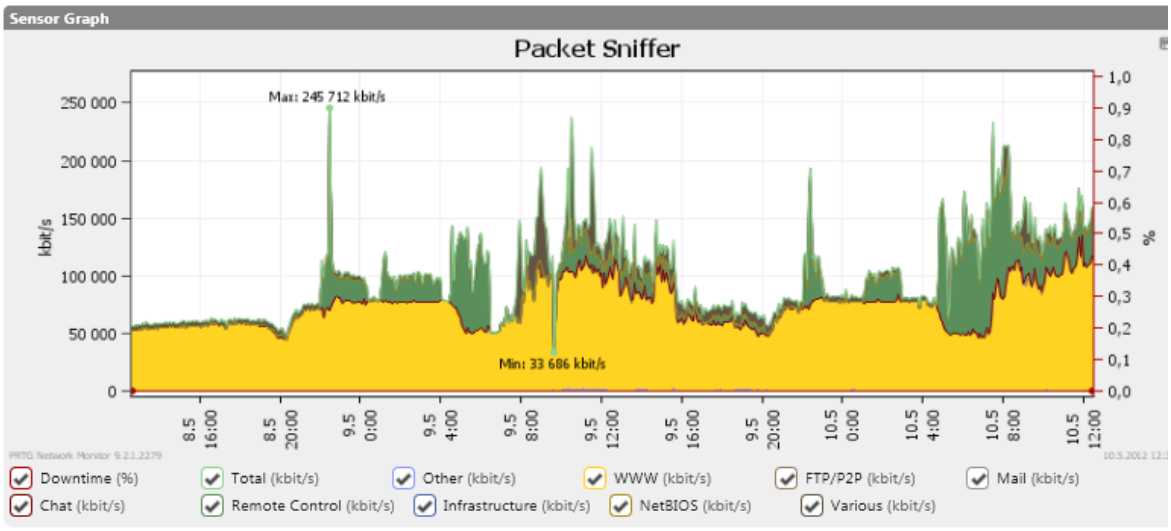
Medzi najčastejšie a najdôležitejšie parametre analýzy dátových tokov patria:

- objem prenesených dát medzi lokalitami
- akou mierou sa aplikácie podieľajú na vyťažení linky
- kto s kým komunikuje
- počet nadväzovaných spojení
- najaktívnejšie stanice
- rozloženie záťaže v jednotlivých hodinách
- najvhodnejšie doby pre údržbu siete

10.1 Analýza 2 dňového monitorovania

Ako je možné vidieť na obrázku nižšie, prevažná časť vyťaženia linky je spôsobená službou WWW (žltá farba), čiže protokolmi HTTP a HTTPS. Dalo sa očakávať, že pravé táto služba vyťažuje dátovú linku najviac keďže zabezpečuje takmer všetku komunikáciu. Výraznou mierou sa na tom podieľa aj kamerový systém menzy a meteorologickej stanice, ktoré pomocou tejto služby zapríčiňujú neustálu komunikáciu počas celého dňa, vrátane nočných hodín. V nočných hodinách sieťovú linku zaťažuje celkom veľkou mierou takisto

vzdialená správa zariadení (zelena farba), protokolmi RDP - Remote Desktop Protokol, SSH - Secure Shell, Telnet, VNC - Virtual Network Computing. Záťaž ostatných služieb v porovnaní s týmito dvoma službami je prakticky minimálna. Až po vyfiltrovaní služieb WWW a Remote Control by sme boli schopní bližšie analyzovať ich reálne zaťaženie na dátovú linku. Filtrovanie je možné priamo v grafe, kde sa graf zobrazuje podľa aktívnych kanálov.



Obr. 24 Grafické zobrazenie nameraných dát počas 2 dní (8.5 - 10.5)

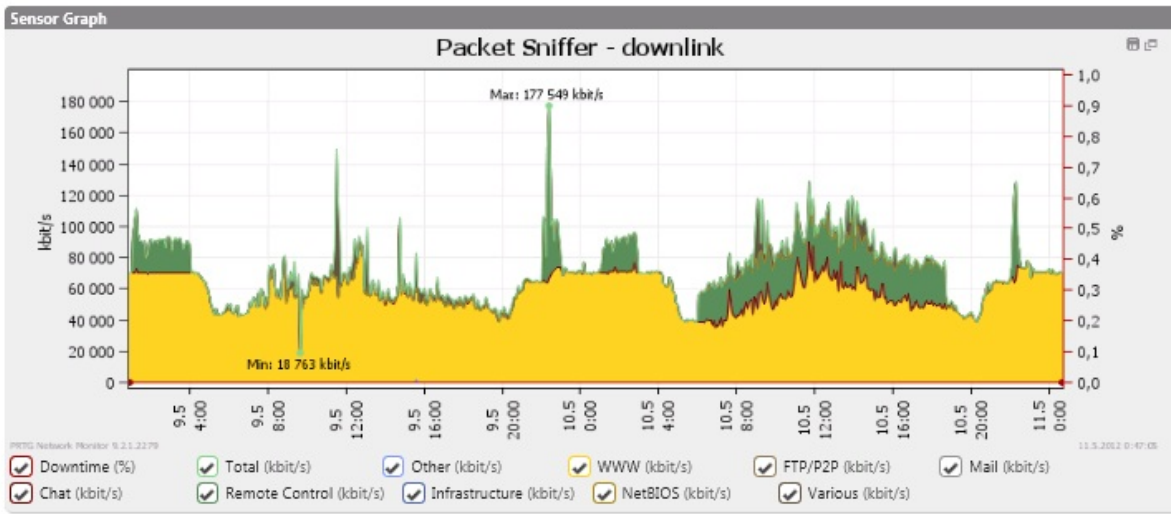
V rozsahu 2 dni bolo v rámci mimo školskej komunikácie prenesených celkovo 2,14 TB dát, v priemere 3,718 GB za interval meranie, čiže 60 sekúnd. Približne 75% týchto dát bolo prenesených službou WWW s celkovým objemom 1,569 TB dát. Spravovanie vzdialenej plochy dokázalo preniesť ceckovo 388,3 GB dát s priemerným prenosom 674 MB za 60 sekúnd.

Date Time	Total (volume) MB	Total (speed) kbit/s	WWW (volume) MB	WWW (speed) kbit/s	RC (volume) MB	RC (speed) kbit/s
Sums	2 141 759		1 569 812		388 347	
Averages	3 718	101 611	2 725	74 476	674	18 424
Date Time	FTP/P2P (volume) MB	FTP/P2P (speed) kbit/s	Chat (volume) MB	Chat (speed) kbit/s	Other (volume) MB	Other (speed) kbit/s
Sums	373,5		28,482		3 315,40	
Averages	0,648	18	0,049	1	5,756	157

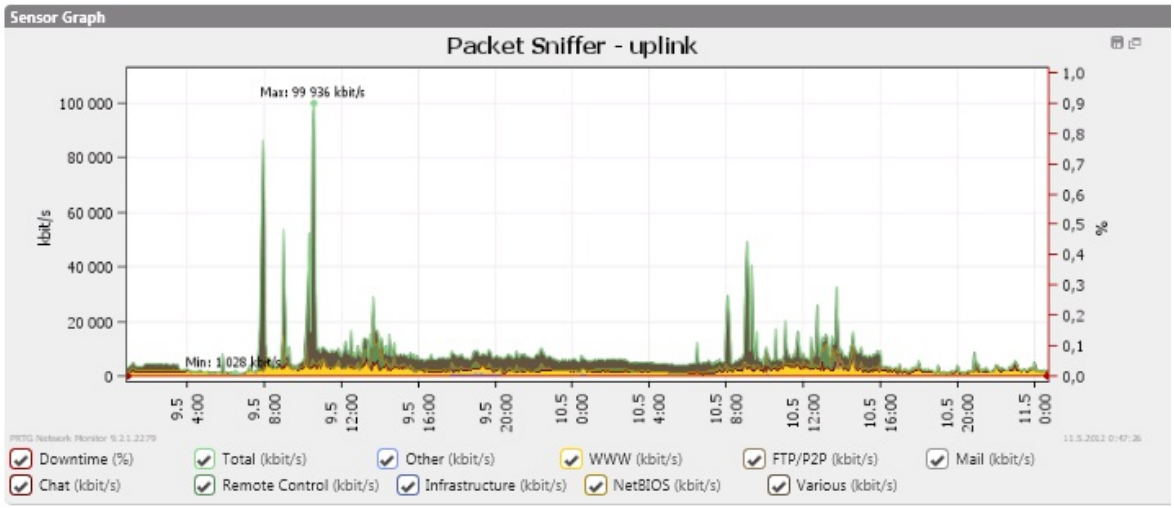
Tabuľka 6 Tabuľka znázorňujúca celkový objem prenesených dát za 2 dni rozdelené podľa jednotlivých služieb

10.1.1 Analýza stiahnutých a odoslaných dát

Z nižšie uvedených grafov je viditeľný rozdiel medzi množstvom odoslaných a prijatých dát za dvojdňové obdobie. Zatiaľ čo množstvu stiahnutých dát vládnu stále služby WWW a Remote Control, medzi odoslanými dátam vyniká služba FTP a Remote Control. Z toho vyplýva, že takmer všetka komunikácia prebieha smerom do vnútra budovy.



Obr. 25 Grafické zobrazenie stiahnutých dát počas 2 dní (9.5-11.5)



Obr. 26 Grafické zobrazenie odoslaných dát počas 2 dní (9.5-11.5)

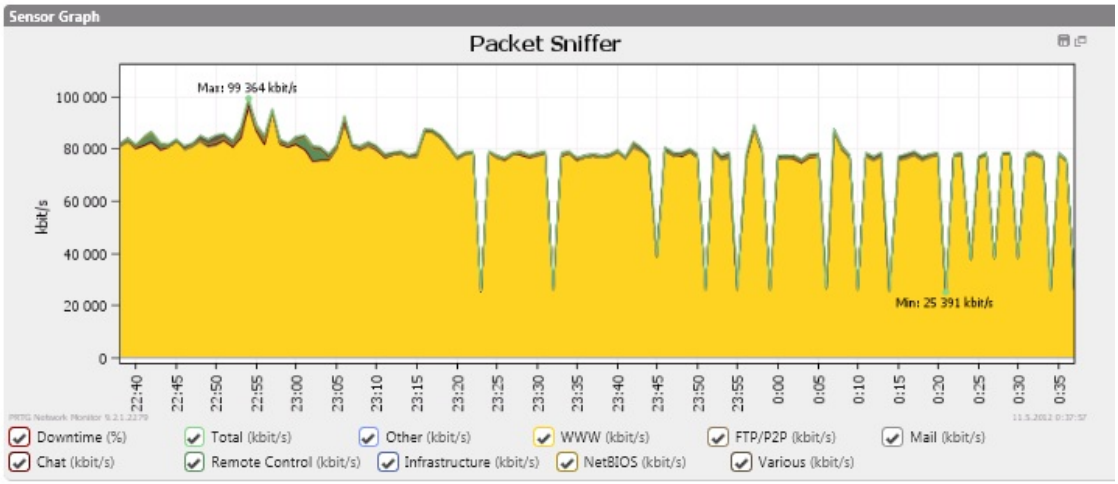
Z grafického i tabuľkového vyhodnotenia je vidieť, že linka sa využíva prevažne na sťahovanie dát a to v pomere približne 10:1 oproti dátam odoslaným. Za dva dni bolo stiahnutých 1,5 TB dát priemernou rýchlosťou 71 944 kbit/s a odoslaných iba takmer 152 GB dát s priemernou rýchlosťou uploadu 7 203 kbit/s.

Date Time	Total (volume) MB DOWNLOAD	Total (speed) kbit/s DOWNLOAD	Total (volume) MB UPLOAD	Total (speed) kbit/s UPLOAD
Sums	1 516 442		151 878	
Averages	2 632	71 944	263,6	7 203

Tabuľka 7 Porovnanie odoslaného a prijatého množstva dát za 2 dni (9.5-11.5)

10.1.2 Analýza nočnej prevádzky

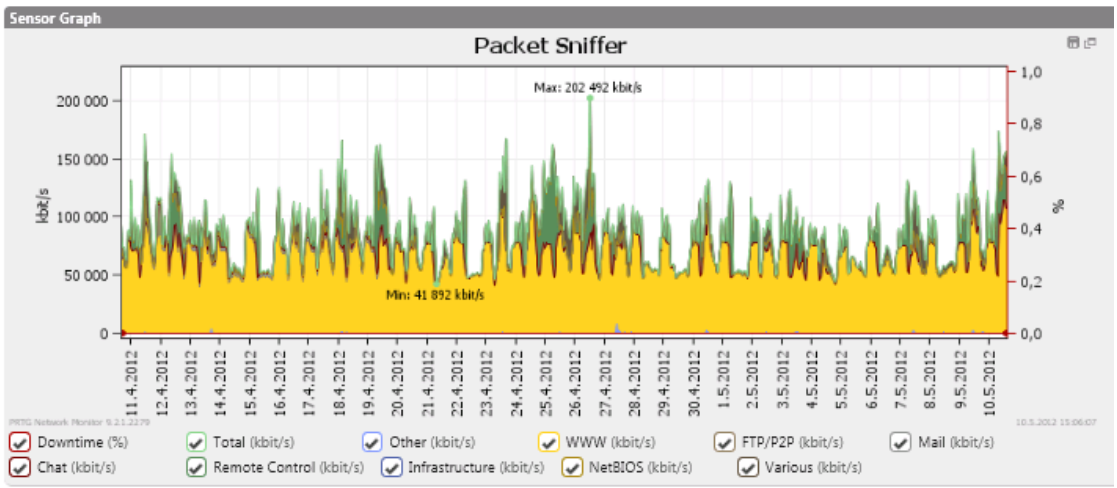
V nočných hodinách je sieť podľa očakávaní vyťažená iba protokolmi HTTP a HTTPS. Prekvapujúca je ale priemerná rýchlosť prenosu dát, ktorá je takmer konštantná na úrovni 80 Mbit/s. Táto hodnota je pomerne vysoká na to, že v nočných hodinách na škole neprebieha žiadna výuka.



Obr. 27 Grafické zobrazenie dátového toku v nočných hodinách (aktuálne dáta)

10.2 Analýza 30 dňového monitorovania

Takisto v období 1 mesiaca je najvyužívanejšia služba WWW, ktorá prakticky každý deň dosahuje identické hodnoty s kolísaniami medzi dnom a nocou. Vzdialená správa má väčšinou impulzný charakter a prenos cez tuto službu nie je konštantne vysoký. Graf mesačného monitorovania nám dáva už bližšiu ucelenú predstavu o vyťaženosti linky. V ostatných mesiacoch by toto zaťaženie nemalo byť moc odlišné, ikeď ho môžu ovplyvniť rôzne nežiaduce faktory, ako napr. : skúškové obdobie a s tým spojenú zvýšenú aktivitu študentov, odstávka niektorej z kamier, pridanie novovzniknutého spojenia atd. Kapacita linky na budove U5 je podľa nameraných hodnôt dostačujúca a nie je potreba jej modernizácia.



Obr. 28 Grafické zobrazenie celkových prenesených dát za obdobie 30 dní

10.3 Analýza TopListov

TopListy sú ďalšou formou zobrazovania nameraných dát. V tomto prípade ide viac-menej o percentuálne vyjadrenie a porovnanie nameraných hodnôt vzhľadom k celkovému prenosu.

PRTG Network Monitor podporuje 3 druhy TopListov :

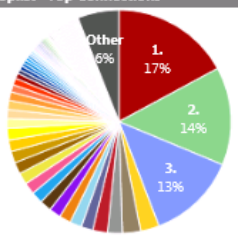
- Top Spojenia
- Top Protokoly
- Top Užívatelia

TopListy sú tvorené vždy v určitých časových intervaloch, bežne je tento interval nastavený na dobu 15minut. V jednotlivých časových intervaloch je možné listovať a je tak možné zistiť percentuálne vyťaženie v ktoromkoľvek časovom okamihu v priebehu dna.

10.3.1 Top spojenia

Z grafického a tabuľkového vyhodnotenia je zrejmé, že dáta sú najčastejšie posielané medzi 3 uzlami. Na prvom mieste je so 17% prichádzajúce spojenie do budovy U5 zo zariadenia v Slavičíne. Ďalšie 2 spojenia s percentami 13% a 14 % predstavujú obojsmernú komunikáciu medzi 2 hlavnými servermi v rámci sieťovej infraštruktúry celej UTB. Toto spôsobuje celkové tretinové zaťaženie siete, ktoré môže naznačovať zle zvolené umiestnenie týchto serverov a zlú komunikáciu medzi dvoma VLAN sieťami, v ktorých sa servery nachádzajú.

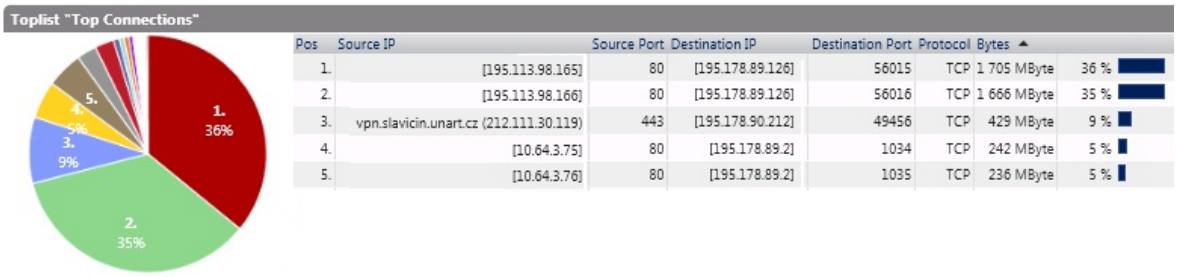
Toplist "Top Connections"



Pos	Source IP	Source Port	Destination IP	Destination Port	Protocol	Bytes	
1.	slavek.slavicin.unart.cz (212.111.30.125)	22	[195.178.90.212]	60997	TCP	442 MByte	17 %
2.	[195.113.98.165]	80	[195.178.89.126]	56015	TCP	367 MByte	14 %
3.	[195.113.98.166]	80	[195.178.89.126]	56016	TCP	334 MByte	13 %
Other						154 MByte	6 %
4.	[10.64.3.76]	80	[195.178.89.2]	1035	TCP	70 MByte	3 %
5.	[10.64.3.75]	80	[195.178.89.2]	1034	TCP	68 MByte	3 %
6.	[195.113.98.137]	80	VOJTA-SKOLA (195.178.89.155)	42139	TCP	55 MByte	2 %
7.	[195.113.98.137]	80	jirimi.fai.utb.cz (195.178.89.111)	50236	TCP	55 MByte	2 %
8.	[93.99.92.16]	80	[195.178.91.241]	25935	TCP	44 MByte	2 %
9.	[93.99.92.16]	80	[195.178.91.241]	22591	TCP	44 MByte	2 %
10.	[93.99.92.3]	80	[195.178.91.241]	25989	TCP	44 MByte	2 %

Obr. 29 Zobrazenie 10 top spojení v čase 14:45-15:00

V nočných hodinách sa komunikácii medzi týmito dvoma hlavnými servermi zvýši až na 70%.

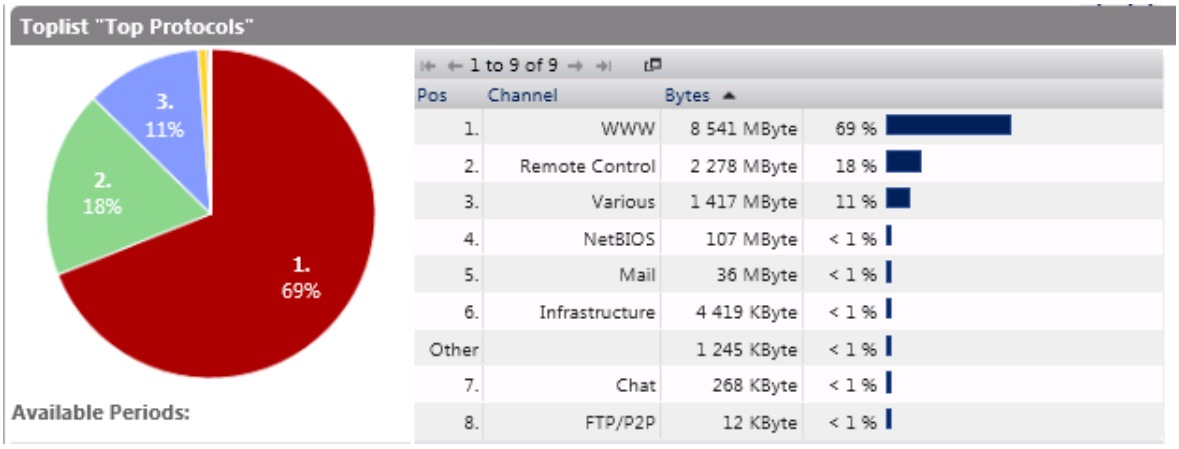


Pos	Source IP	Source Port	Destination IP	Destination Port	Protocol	Bytes	
1.	[195.113.98.165]	80	[195.178.89.126]	56015	TCP	1 705 MByte	36 %
2.	[195.113.98.166]	80	[195.178.89.126]	56016	TCP	1 666 MByte	35 %
3.	vpn.slavicin.unart.cz (212.111.30.119)	443	[195.178.90.212]	49456	TCP	429 MByte	9 %
4.	[10.64.3.75]	80	[195.178.89.2]	1034	TCP	242 MByte	5 %
5.	[10.64.3.76]	80	[195.178.89.2]	1035	TCP	236 MByte	5 %

Obr. 30 Zobrazenie 5 top spojení v čase 00:30-00:45

10.3.2 Top protokoly

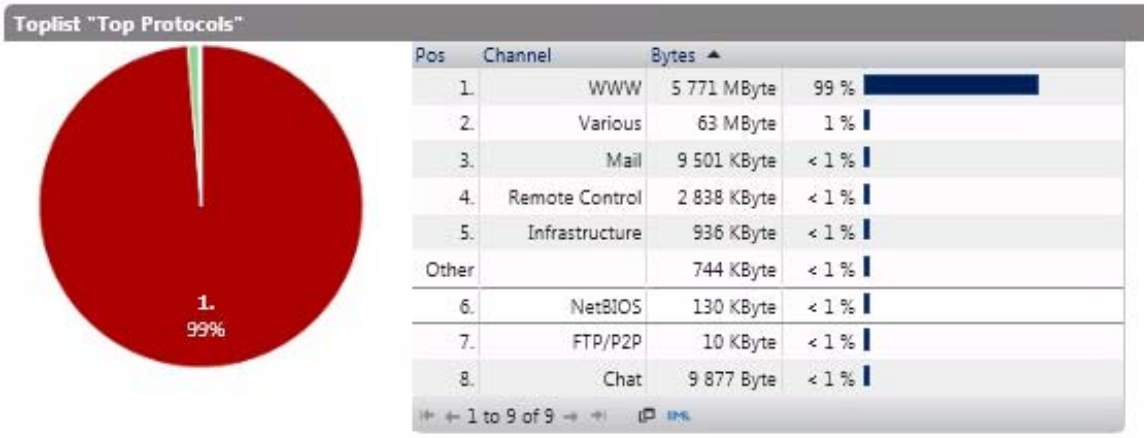
Ako už bolo písané v rozbore dvoj dňového monitorovania, najväčšiu mieru na zaťažení siete majú služby WWW a Remote Control. V TopListe protokolov však ide o percentuálne znázornenie a porovnanie na rozdiel presných číselných hodnôt prenesených dát.



Pos	Channel	Bytes	
1.	WWW	8 541 MByte	69 %
2.	Remote Control	2 278 MByte	18 %
3.	Various	1 417 MByte	11 %
4.	NetBIOS	107 MByte	< 1 %
5.	Mail	36 MByte	< 1 %
6.	Infrastructure	4 419 KByte	< 1 %
Other		1 245 KByte	< 1 %
7.	Chat	268 KByte	< 1 %
8.	FTP/P2P	12 KByte	< 1 %

Obr. 31 Percentuálne zobrazenie využívaných služieb a protokolov (14:45-15:00)

Aj TopList z nočných hodín dokazuje, že služba WWW vyťažuje linku takmer na 100%, pravdepodobne spôsobované už spomínaným kamerovým systém.



Obr. 32 Percentuálne zobrazenie využívaných služieb a protokolov (00:30-00:45)

10.4 Ďalšie využitie monitorovacieho systému PRTG

Monitorovací nástroj PRTG Network Monitor dôkaze monitorovať samozrejme omnoho viac parametrov siete. Napriek tomu, že je momentálne využívaný len na monitorovanie dátového toku na budove U5, vďaka svojej ľahkej rozšíriteľnosti môže byť v budúcnosti použitý aj na monitorovanie iných parametrov podľa potreby. PRTG ponúka široký výber senzorov, pomocou ktorých je možné monitorovať takmer čokoľvek. V dnešnej dobe nie je na možné využívať senzory založené na technológii SNMP, keďže tento protokol je blokovaný hlavným firewallom siete UTB. Po dodatočnej konfigurácii by bolo možné využívať aj senzory tohto typu na zbieranie potrebných informácii od všetkých zapojených zariadení v sieti podporujúcich protokol SNMP. Takisto by bolo možné implementovať senzory na monitorovanie hardwarových a softwarových parametrov hlavného servera aby bola viditeľná zaťaž monitorovania na toto zariadenia. Počet aktívnych senzorov je však limitovaný na 10 kusov, pri väčšom počte už je potrebné zakúpiť požadovanú licenciu alebo uvažovať nad opensourcovým riešením.

ZÁVĚR

Predmetom diplomovej práce bolo implementovať vhodný monitorovací systém na budovu U5 Fakulty Aplikovanej Informatiky, Univerzity Tomáše Bati, schopný monitorovať zaťaženie dátovej linky. Implementácia bola vykonaná na zistenie dátového toku celej lokálnej siete na tejto budove s následnou analýzou nameraných dát.

Začiatok teoretickej časti je venovaný základným pojmom v oblasti monitorovania počítačovej siete, druhom monitorovania a dôvodom na zavedenie samotného monitorovania. V ďalšej kapitole som sa venoval jednotlivým najpoužívanejším monitorovacím metódam a nástrojom. V závere teoretickej časti som sa detailnejšie venoval trom monitorovacím nástrojom, od ich architektúry cez spôsob fungovania, až po ich výhody a nevýhody. Z nich som vybral vhodného kandidáta, ktorý spĺňa zadané požiadavky a implementoval som ho na hlavný server na budove U5.

Praktická časť rieši inštaláciu samotného monitorovacieho nástroja PRTG Network Monitor na testovací server. V úvode praktickej časti popisujem vytvorenie daného testovacieho servera pomocou presmerovania dátového toku z hlavného servera a podrobnú inštaláciu a konfiguráciu vybraného monitorovacieho systému. Konfigurácia PRTG systému zahŕňa pridanie monitorovaného zariadenia a potrebných senzorov. V ďalšej kapitole som sa bližšie venoval senzoru Packet Sniffer, ktorý je potrebný pre dané monitorovania. Zvyšok práce je venovaný analýze a vyhodnoteniu nameraných dát. Z nich sa podarilo zistiť dostatočne veľké zaťaženie dátovej linky službou WWW počas celého dňa, aj v nočných hodinách, ktoré je spôsobené pravdepodobne kamerovým systémom a nie práve optimálnou komunikáciou medzi hlavnými servermi v rámci VLAN sietí UTB.

Táto diplomová práca môže slúžiť ako pomôcka pre začínajúcich správcov siete, ktorí by sa rozhodli pre zavedenie monitorovacieho systému do lokálnych sieti. Pri práci som sa snažil zužitkovať všetky moje teoretické a praktické vedomosti z oblasti počítačových sietí.

ZÁVĚR V ANGLIČTINĚ

The subject of the thesis was the implementation of a suitable monitoring system for the building U5 of the Faculty of Applied Informatics, Tomas Bata, which would be able to monitor the data line load. The purpose of the implementation was to determine the data flow in the whole LAN in the building and consequently analyze the collected data. The beginning of the theoretical part describes the basic concepts of computer network monitoring, monitoring types and the reasons for the implementation of monitoring. The next chapter describes the most commonly used monitoring methods and tools. The conclusion of the theoretical part closely focuses on the three monitoring tools - their architecture, how they actually work, their advantages and disadvantages. Out of these three was chosen the right candidate, which matched specified requirements, and which was further used for implemention on the main server for building U5.

The field study describes the actual installation of the monitoring tool PRTG Network Monitor on the test server. In the introduction is described the creation of the test server via forwarding the data flow from the main server and thorough installation and configuration of the selected monitoring system. Configuration of the PRTG system involves the addition of the necessary monitoring equipment and sensors. The next chapter focuses on Packet Sniffer sensor, which is necessary for the monitoring. The rest of the thesis covers the analysis and evaluation of collected data. The results showed sufficiently large data line load for WWW service not only throughout the day, but also at night, which is likely caused by a camera system as well as the non-optimal communication between the main servers within the VLANs of UTB.

This thesis can serve as a guide for rookie network administrators, who have decided to implement a monitoring system to the local network. While writing this thesis I tried to utilize all of my theoretical and practical knowledge of computer networks.

SEZNAM POUŽITÉ LITERATURY

[1] DONDICH, Taylor. Network monitoring with Nagios. Sebastopol, CA: O\'Reilly, 2006. ISBN 978-059-6528-195.

[2] KRETCHMAR, James M. Administrace a diagnostika sítí: pomocí OpenSource utilit a nástrojů. 1. vyd. Brno: Computer Press, 2004, 216 s. ISBN 80-251-0345-5.

[3] BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.

[4] MCQUERRY, Steve, David JANSEN a Dave HUCABY. Cisco LAN switching configuration handbook. 2nd ed. Indianapolis, IN: Cisco Press, c2009, 333 s. Cisco Press networking technology series. ISBN 15-870-5610-0.

[5] MIHOK, Bc. Miroslav. Monitorování počítačových sítí a aplikací pomocí programu Nagios. Zlin, 2010. Diplomová práca

[6] MATÚŠŮ, Jindřich. Monitorování stavu rozsáhlých sítí. Zlín, 2008. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Tomáš Dulík.

[7] PRTG Network Monitor [online]. [cit. 2012-05-05]. Dostupné z: http://www.paessler.com/

[8] Nagios Core 3.x Documentation [online]. [cit. 2012-05-05]. Dostupné z: http://nagios.sourceforge.net/docs/3_0/toc.html

[9] BOUŠKA, Petr. Začínáme s monitoringem sítě. *Connect!*. Computer Press, 2009, roč. 2009, č. 09. ISSN 211-3085.

[10] SNMP - Simple Network Management Protocol. In: [online]. 20.12.2006. [cit. 2012-05-15]. Dostupné z: http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/

[11] Cacti [online]. [cit. 2012-05-15]. Dostupné z: http://www.cacti.net/

[12] Cacti: vše důležité v jednom monitoru. In: [online]. [cit. 2012-05-15]. Dostupné z: http://www.root.cz/clanky/cacti-vse-dulezite-v-jednom-monitoru/

[13] Spôsoby scanovania portov. In: [online]. [cit. 2012-05-15]. Dostupné z: http://nmap.org/man/sk/man-port-scanning-techniques.html

[14] Základy scanovania portov. In: [online]. [cit. 2012-05-15]. Dostupné z: http://nmap.org/man/sk/man-port-scanning-basics.html

[15] Metódy pre monitorovanie sieťovej prevádzky. In: [online]. [cit. 2012-05-15]. Dostupné z: http://wiki.cnl.sk/Sandbox/MetodyMonitorovania#MyAnchor

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CGI	Common Gateway Interface
CPU	Central Processing Unit
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
Ping	Packet InterNet Groper
PHP	Hypertext Preprocessor
RDP	Remote Desktop Protokol
QOS	Qality of Service
SSH	Secure Shell
SNMP	Simple Network Management Protocol
TCP	Transmissin Control Protocol
TTL	Time To Live
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
WAN	Wide Area Network
WMI	Windows Management Instrumentation
WWW	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM TABULEK