Sieťové dohľadové systémy

DIPLOMOVÁ PRÁCA

Ján Gregor

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY FYZIKY A INFORMATIKY
KATEDRA INFORMATIKY

Informatika

Školiteľ záverečnej práce
Ing. Ján Muzslay

BRATISLAVA 2006

Čestne vyhlasujem, že som diplomovú prácu vypracoval samostatne, s použitím literatúry a zdrojov uvedených v závere práce.

V Bratislave, máj 2006

.....

Ďakujem svojmu diplomovému vedúcemu Ing. Jánovi Muzslayovi za odbornú pomoc .

Ďakujem aj svojej rodine a blízkym, ktorí mi poskytovali duševnú aj hmotnú pomoc a to aj v čase, keď to nebolo potrebné.

Abstrakt

Diplomová práca sa zaoberá technológiami používanými pri dohľadovaní sietí so špeciálnym zameraním na oblasť telekomunikácií. Práca vychádza zo štúdia správania sietí, informácií obsiahnutých v odbornej literatúre a praktických skúseností autora.

Práca analyzuje a popisuje proces dohľadovania a štandardy, ktoré sú pri ňom používané (SNMP, RMON). Práca sa tiež venuje nájdeniu významných spoločných čŕt v rôznych dohľadových systémoch a tieto spoločné vlastnosti sú využité vo vytvorení abstraktného modelu dohľadového systému. V rámci práce sa tiež podarilo s pomocou štandardných technológií vytvoriť dohľadovanie existujúcej metropolitnej telekomunikačnej siete.

Hlavným prínosom tejto práce je nový pohľad na niektoré aspekty dohľadovania dnešných sietí. Ďalším prínosom je vytvorenie dohľadovania siete na úrovni, ktorá sa môže porovnávať s dohľadovaním sietí v špičkových telekomunikačných firmách.

Kľúčové slová: dohľadovanie sietí, dohľadové systémy, sieťové protokoly, Simple Network Management Protocol

OBSAH:

Zoznam obrázkov a tabuliek

Zoznam obrázkov

Zoznam tabuliek

Úvod

Počítačové siete sú v súčasnosti jedným z najdynamickejšie sa rozvíjajúcich odvetví. Postupom času sú vytvárané čoraz väčšie a komplexnejšie siete a s týmto nárastom zložitosti úmerne narastá aj potreba poznať informácie o problémoch a udalostiach, ku ktorým v sieti dochádza. Štandardným riešením pre zhromažďovanie týchto informácií sú v dnešnej dobe dohľadové systémy. Dohľadový systém si je možné predstaviť ako kontrolného pracovníka, ktorý vidí celú sieť a neustále kontroluje kvalitu služieb, ktoré sú na tejto sieti poskytované. S narastajúcou komplexnosťou služieb poskytovaných na dnešných sieťach samozrejme narastajú aj požiadavky na funkcionalitu ich automatických dohľadových systémov.

Ako príklad je možné uviesť poskytovanie liniek telekomunikačnými operátormi. Na to, aby boli poskytované služby dostatočne kvalitné a spoľahlivé, je nutné vzniknuté problémy veľmi rýchlo odhaliť a následne odstrániť. Odhalenie a lokalizáciu problému vo väčších sieťach nemôžu efektívne a hlavne dostatočne rýchlo zabezpečovať priamo zamestnanci spoločnosti, musí ju zabezpečovať automatický dohľadový systém. Odstránenie odhaleného problému už potom zabezpečujú zodpovední technickí pracovníci, ktorých o danom probléme dohľadový systém upovedomí. Podobný princíp je možné aplikovať aj pre zabezpečenie banky, kde výstupy z bezpečnostných senzorov monitoruje automatický dohľadový systém. Ten spustí alarm vždy keď zistí akúkoľvek neočakávanú udalosť. Pracovníkmi zodpovednými za odstránenie vzniknutého problému sú v tomto prípade bezpečnostné zložky.

Prvé dohľadové systémy v praxi len rôznymi metódami merali latenciu a stratovosť dát v sieti. Vzhľadom k tomu, že s nárastom komplexnosti sietí narastá aj komplexnosť služieb na nich poskytovaných a ich posun do vyšších sieťových vrstiev, prestáva byť tento prístup dostačujúci. Vzniká teda potreba dohľadovať aj iné aspekty kvality služieb poskytovaných na sieťach, na čo je potrebné, aby aj dohľadové systémy boli rozsiahlejšie a robustnejšie. Toto sa ale zväčša dosahuje za cenu rýchlosti, jednoduchosti, ale hlavne prehľadnosti. Komplikácie tohoto druhu

je možné odstrániť pomocou lepšieho dizajnu dohľadových systémov, to ale samozrejme predpokladá dobré znalosti technológií, ktoré sú pre dohľadovanie sietí k dispozícii.

Napriek tomu, že dohľadovanie sietí nie je zďaleka novou problematikou a v súčasnosti už existuje veľké množstvo dohľadových systémov, bola doteraz systematickej analýze a skúmaniu dohľadovania venovaná len malá pozornosť. Preto v prípade dohľadových systémov často dochádza k chybám v návrhu, čo ich robí ťažko rozšíriteľnými a udržiavateľnými. Z tohoto dôvodu sa od širšieho používania niektorých z nich časom úplne upustilo. Táto práca je venovaná práve nájdeniu potrebných informácií a analýze dohľadovania od vzniku udalosti v sieti až po samotné vyriešenie vzniknutého problému. Cieľom je taktiež vytvoriť flexibilný model dohľadového systému, ktorý je možné použiť pri návrhu nových dohľadových systémov. V závere práce sú tieto získané informácie zúžitkované pri praktickej ukážke možností dohľadovania konkrétnej siete.

Tematicky je práca rozdelená do troch častí a to tak, aby prvé dve poskytli prehľad o technológiách, ktoré sa v tejto oblasti používajú. Tieto časti zároveň dodávajú teoretické podklady pre praktickú ukážku tvorby dohľadovania konkrétnej existujúcej siete, ktorej je venovaná tretia kapitola. Pre zabezpečenie väčšej prehľadnosti práce a lepšieho stotožnenia s textom sú tieto kapitoly členené tak, aby názorne poukázali na postup vytvárania dohľadovania a každá ich časť využíva informácie z tej predchádzajúcej.

Prvá kapitola oboznamuje čitateľa so základnými pojmami, s ktorými sa čitateľ potrebuje oboznámiť, aby pochopil z akých súčastí sa dohľadovanie skladá. Pri takomto hrubom rozdelení dohľadovania sa jedná hlavne o pojmy sieť, dohľadový systém a dohľadové centrum. Toto rozdelenie následne umožňuje jednoduchšiu analýzu procesov prebiehajúcich v rámci používania dohľadových systémov v nasledujúcich kapitolách.

Druhá kapitola bližšie skúma tieto pojmy a čím jednoznačnejším spôsobom poukazuje na ich vnútornú štruktúru. Taktiež poskytuje bližší pohľad na komunikáciu medzi nimi, ktorej správny návrh sa ukazuje byť jedným z najkritickejších parametrov pre správnu prácu dohľadovania siete. Taktiež táto

kapitola poskytuje stručný prehľad najvýznamnejších a najrozšírenejších dohľadových systémov používaných v dnešnej dobe. Na základe ich porovnania je v jej závere navrhnutý model dohľadovania siete.

Tretia kapitola je zameraná hlavne na reálnu aplikáciu nadobudnutých informácií v praxi s prihliadnutím aj na finančné aspekty budovania dohľadovania siete. Táto časť dáva príklad, ako je možné nasadiť dohľadový systém do existujúcej siete. Dohľadovanie, ktoré je výsledkom snahy tejto kapitoly, je reálne nasadené v produkčnom prostredí a je v ňom už tri roky používané.

Cieľovou skupinou pre túto prácu sú správcovia sietí, ktorí potrebujú informácie potrebné pre vytvorenie dohľadovania ich siete. Ďalej ju môžu využiť programátori, ktorí pre svoju prácu potrebujú pochopiť, ako dohľadové systémy pracujú vo svojom vnútri, čomu pri programovaní dohľadových systémov venovať najväčšiu pozornosť a ku akým najbežnejším chybám môže pri návrhu takéhoto systému dôjsť.

1. Analýza dohľadovania

Na začiatku tejto práce je dôležité si uvedomiť, čo vlastne dohľadovanie siete je a aké ciele sa jeho využívaním snažíme dosiahnuť. Na prvý pohľad by sa odpovede na tieto otázky mohli zdať ľahké, v kontexte správy sietí je odpovedať na ne trochu zložitejšie.

Dohľadovaním siete sa snažíme dosiahnuť nasledovné tri funkčné ciele:

- dohľadovanie výkonu siete
- dohľadovanie porúch v sieti
- dohľadovanie užívateľov siete

Dôležitosť dohľadovania siete podčiarkuje aj ten fakt, že tieto ciele sú tri z piatich funkčných oblastí, ktoré sú navrhnuté v OSI (Open Systems Interconnect) modeli. Dve ďalšie funkčné oblasti sú manažment konfigurácií a manažment bezpečnosti siete. Tieto ale nespadajú do oblasti dohľadovania sietí, preto im v tejto práci nebude ďalej venovaná pozornosť.

Dohľadovanie výkonu siete obsahuje tri dôležité aspekty. Za prvé znalosti o aktuálnom vyťažení siete môžu byť využívané pri plánovaní ďalšej expanzie siete a pomáha hľadať úzke hrdlá v sieti. Týmto spôsobom je možné odhaliť veľa problémov, ktoré sú spôsobené preťažením niektorej časti siete. Druhým aspektom je doba dohľadovania výkonu siete. Ak je táto dostatočne dlhá, je možné na základe získaných informácií vytvoriť model bežného správania siete a ten následne využiť pri odhaľovaní častých problémov v sieti, ktoré sa vyskytujú s určitou pravidelnosťou. Tretím aspektom dohľadovania výkonu siete je výber parametrov, ktoré je v sieti potrebné merať. V dnešných sieťach totiž hrá svoju rolu veľké množstvo parametrov, ale nie všetkými z nich má reálny význam sa zaoberať. Je potrebné nájsť kompromis medzi množstvom dohľadovaných parametrov a cenou za ich dohľadovanie. Skupina parametrov, ktoré sú nakoniec zvolené za smerodajné pre výkon siete sú nazývané s*ieťové indikátory*. Typickými indikátormi v moderných počítačových sieťach sú napríklad latencia, dostupnosť zariadení v sieti, alebo chybovosť.

Dohľadovanie porúch v sieti má na starosti zistenie všetkých problémov, ku ktorým v sieti v priebehu jej používania dochádza. Tak isto ako dohľadovanie výkonu siete, má aj dohľadovanie porúch viacero aspektov. Za prvé je potrebné si uvedomiť, že sieťové modely sa skladajú z vrstiev. Správne určenie, ktorá vrstva spôsobila problém je kľúčové pre odhalenie a vyriešenie problému. V prípade ak by sme nezisťovali, ktorá vrstva spôsobuje problém, je pravdepodobné, že namiesto odstránenia príčiny problému by došlo len k odstráneniu následkov. Problém tak môže vzniknúť neskôr v inej časti siete, spravidla v podstatne väčšom rozmere. Druhým aspektom je určiť normálny výskyt chýb v sieti za dlhšie časové obdobie. Každá sieť má istú mieru normálnej chybovosti, táto chybovosť ale nemusí znamenať, že sieť má neustále problémy. Niektoré problémy sú totiž očakávané a ich výskyt nie je možné odstrániť. Napríklad sa môže jednať o rušenie na vedení spôsobujúce chybovosť na linke, ale napríklad aj o pravidelné plánované reštarty niektorého zo zariadení v sieti.

Dohľadovanie užívateľov v sieti sa stará o sledovanie počtu a aktivity užívateľov, ktorí k nej pristupujú. V rámci dohľadovania tohoto atribútu sú udržované záznamy o tom, ktoré zariadenia sú do akej miery využívané užívateľmi siete. Tieto informácie je potom možné použiť pre fakturáciu zákazníkov a predpovedanie využitia siete do budúcna. Nie pre všetky siete a služby na nich poskytované má ale dohľadovanie užívateľov rovnako veľký význam. Napríklad pre dátové prenosy medzi dvomi pobočkami v rámci jednej siete je počet užívateľov len málo zaujímavý (podstatne zaujímavejšie je množstvo prenesených dát), no napríklad v kontexte hlasových služieb je ale sledovanie počtu a dĺžky volaní užívateľov jedným z najdôležitejších aspektov dohľadovania siete vôbec.

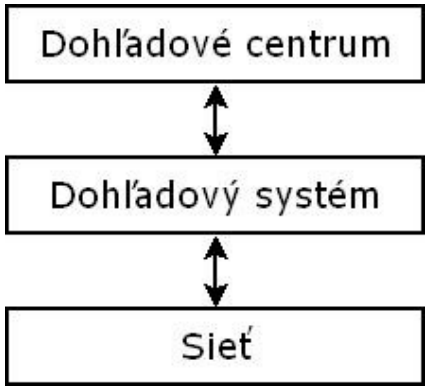
Ďalšou dôležitou otázkou je, čo to vlastne dohľadovanie je. Existuje veľa rôznych definícií dohľadovania, pre účely tejto práce ale adoptujeme nasledovnú definíciu:

> *Dohľadovanie siete je proces využívania systému, ktorý neustále sleduje počítačovú sieť a hľadá v nej pomalé alebo nefungujúce systémy. Takisto sa*

stará o informovanie zodpovedných pracovníkov o vzniknutých problémoch v sieti.

Dôležitou informáciou z predchádzajúcej definície dohľadovania je to, že sa jedná o dynamický proces a nie o stav. Tento proces je teda treba udržiavať v chode a starať sa o jeho správne fungovanie, pričom najčastejšou údržbou je v praxi aktualizovanie dokumentácie. Dohľadovanie v dnešnej dobe ale samozrejme nie je proces, ktorý by bol vykonaný v jednom kroku. Dohľadované zariadenie totiž vo väčšine prípadov nevie priamo a v zrozumiteľnej forme povedať zodpovednej osobe, že sa s ním niečo udialo, ale navyše pri bezprostrednej komunikácii so sieťou môže ľahko dojsť k bezpečnostným incidentom. Je preto potrebné umiestniť medzi zariadenia v sieti a cieľového užívateľa dohľadovania rozhranie, ktoré tieto informácie od zariadení prevedie do formy, ktorej je možné porozumieť a odfiltruje aj prípadné bezpečnostné útoky na sieť. Týmto rozhraním je automatický dohľadový systém, ktorý sa o zber a prezentáciu týchto informácií stará.

Na základe tohoto faktu je potrebné dohľadovanie sietí rozdeliť na niekoľko častí. Ako aj sieťové modely sú štandardne delené na vrstvy, je tak možné rozdeliť aj dohľadovanie sietí. Toto rozvrstvenie logicky rozdeľuje zložky dohľadovania na základe funkcie, ktorú v ňom zohrávajú. Jednotlivé vrstvy sú prepojené cez ich rozhrania a navzájom komunikujú pomocou vopred definovaných protokolov.
Schéma tohoto rozvrstvenia je zobrazená na obrázku 1.1.,



Obrázok 1.1 – Rozdelenie dohľadového procesu

Najnižšia vrstva v tejto schéme je sieť. Táto sieť obsahuje telekomunikačné zariadenia, produkčné servery, senzory a iné zariadenia, ktoré sú cieľom dohľadovania. Vo všeobecnosti sa môže jednať o ľubovoľné *sieťové zariadenie*. Každé zariadenie v sieti poskytuje užívateľovi siete istú množinu služieb. Služba môže predstavovať konkrétny proces bežiaci na zariadení (SMTP, HTTP, …), ale napríklad aj počet prihlásených užívateľov, čas odpovede na ping, alebo snímanie pohybového senzora. Služba je zároveň najmenšou jednotkou, s ktorou pri dohľadovaní sietí pracujeme.

Na komunikáciu medzi sieťou a nasledujúcou vrstvou (dohľadový systém) je využívané množstvo protokolov. Tento veľký počet protokolov vyplýva hlavne z množstva rôznych zariadení a služieb na nich poskytovaných. Cieľom moderných dohľadových systémov je samozrejme možnosť dohľadovať čím väčšie množstvo z nich.

Nasledujúca vrstva v procese dohľadovania je samotný dohľadový systém. Ten by mal vedieť komunikovať so zariadeniami v sieti, zhromažďovať a spracovávať informácie o udalostiach v sieti a zabezpečovať prehľadný prístup k nim pre dohľadové centrum. Táto úloha dohľadového systému ale nie je taká jednoduchá, ako by sa na prvý pohľad mohlo zdať. Dohľadový systém ďalej musí pre svoju prácu zabezpečovať plánovanie kontrol služieb v sieti, spracovávanie získaných informácií a ich následnú prezentáciu zodpovedným osobám.

Komunikácia medzi dohľadovým systémom a dohľadovým centrom taktiež prebieha pomocou väčšieho množstva rôznych protokolov. V praxi je ich ale podstatne menej ako protokolov medzi sieťou a dohľadovým systémom a je cítiť väčšiu snahu o ich štandardizáciu. Je to hlavne preto, že je badateľná snaha o čím väčšie zjednodušenie komunikácie zo strany dohľadového centra a v rámci neho vytvorenie tenkého klienta pre prístup k dohľadovému systému. V súčasnosti sa na prístup k dohľadovému systému využíva hlavne protokol HTTP.

Vrstva dohľadového centra zabezpečuje riešenie prípadných problémov, ktoré dohľadový systém zaeviduje. Väčšinou sa jedná o tím ľudí, ktorí podľa definovaných procesov zabezpečujú komunikáciu so zákazníkmi. Samotné dohľadové centrum je jedným z klientov dohľadového systému. Klientom

dohľadového systému budeme po zvyšok práce nazývať oprávnenú osobu, ktorá pristupuje k informáciám obsiahnutým v dohľadovom systéme. Táto diplomová práca sa bude venovať dohľadovému centru len okrajovo, pretože táto problematika spadá skôr do oblasti manažmentu ľudských zdrojov.

2. Vrstvy dohľadovania

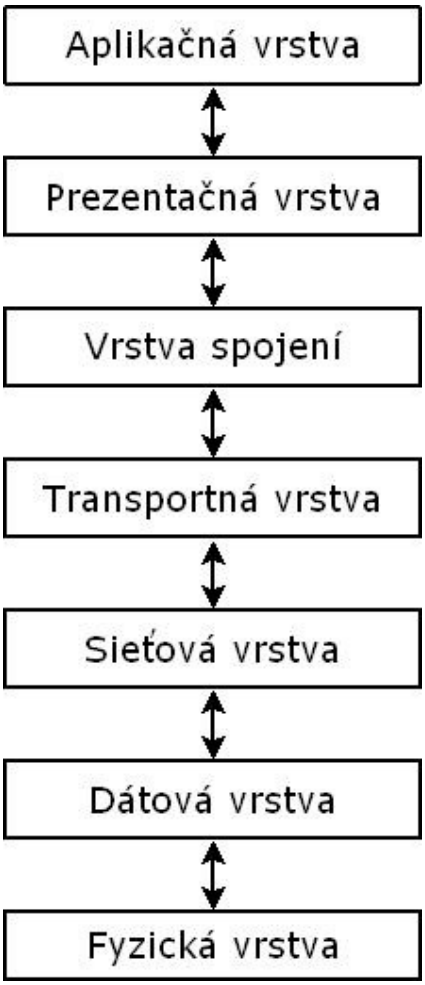
V predchádzajúcej kapitole bol proces dohľadovania rozdelený do troch vrstiev na základe ich rozdielneho zamerania. Toto rozdelenie umožňuje pristupovať k procesu dohľadovania s potrebnou dávkou abstrakcie od existujúcich technológií a viac sa zamerať na ich všeobecné parametre. Táto kapitola je venovaná postupnej analýze týchto parametrov a návrhu riešení v tých oblastiach dohľadovania, ktoré ešte neboli dostatočne zmapované a pri ktorých vznikajú viaceré nejasnosti.

2.1. Sieť

Najnižšou vrstvou v procese dohľadovania je samotná sieť, ktorú je cieľom dohľadovať. Typov sietí, ktoré je potrebné dohľadovať, je veľké množstvo a v každom sa používajú iné zariadenia a na každom z nich sú poskytované iné služby. Ako príklad dvoch sietí s úplne odlišnou architektúrou môžu poslúžiť siete na báze ethernetu a synchrónne siete. Tieto majú samozrejme aj odlišné parametre, ktoré je potrebné dohľadovať a tomu treba prispôsobiť metódy dohľadovania.

Pre snahu o čím väčšiu jednoznačnosť je žiadúce rozdeliť zariadenia a služby v sieti na základe presných kritérií. Vhodných kritérií pre takéto rozdelenie sa ponúka hneď viacero, napríklad rozdelenie na lokálne a vzdialené služby, alebo rozdelenie na základe typu siete (SDH, Ethernet, ATM, …). Žiadne z dnešných kritérií používaných na rozdelenie zariadení a služieb ale nedosiahlo významnejší úspech. Každý tvorca dohľadovania svojej siete si teda väčšinou vytvoril vlastný návrh, čo prináša veľké množstvo rôznych prístupov k dohľadovaniu tých istých technológií.

V tejto práci teda zavedieme vlastné rozdelenie služieb na základe sieťových vrstiev, do ktorých spadajú. Služby prislúchajúce každej sieťovej vrstve majú samozrejme odlišný charakter. Pre rozdelenie použiteľné pre čím väčšie množstvo sietí sa ukazuje rozdelenie na vrstvy pomocou modelu OSI, teda na 7 vrstiev. Vrstvy OSI modelu sú zobrazené na obrázku 2.1.



Obrázok 2.1 – Vrstvy OSI modelu

Fyzická vrstva je najnižšou vrstvou v OSI modeli. Stará sa o vysielanie a prijímanie bitov z použitého prenosového média. Zaoberá sa problémami súvisiacimi s mechanickými, elektrickými a procedurálnymi rozhraniami a s fyzickým prenosovým médiom. Na dohľadovanie služieb na sieťovej vrstve postačuje teda sledovanie stavu rozhraní na zariadeniach v sieti.

Dátová vrstva sa stará o vytváranie a rozpoznávanie hraníc rámcov a detekciu poškodených rámcov vznikajúcich počas prenosu dát. Dohľadovanie služieb na dátovej vrstve teda pozostáva zo sledovania počtu chýb na rozhraniach prislúchajúcich týmto službám.

Sieťová vrstva rozširuje služby dátovej vrstvy o mechanizmy smerovania, kontrolu zahltenia a stará sa o prepájanie heterogénnych sietí. Vzhľadom k povahe

sieťovej vrstvy už ale pri dohľadovaní nestačí sledovať len rozhrania, ktoré prislúchajú tejto službe. Dohľadovanie služieb na sieťovej vrstve spočíva hlavne v sledovaní zmien v smerovacích tabuľkách na jednotlivých zariadeniach a ich dostupnosti v rámci siete.

Transportná vrstva sa stará o kompletné prepojenia zo zdroja k cieľu. V nižších sieťových vrstvách sa jedná len o komunikáciu medzi dvomi bezprostrednými susedmi v sieti. Dohľadovanie transportnej vrstvy spočíva vo vytváraní spojení zo zdroja do cieľa a sledovania toho, či bolo spojenie úspešne vytvorené.

Vrstva spojení a prezentačná vrstva v OSI modeli sú v moderných sieťach vynechávané. Pre dohľadovanie služieb týchto dvoch vrstiev je ale možné použiť tie isté metódy ako pre dohľadovanie transportnej vrstvy.

Aplikačná vrstva je najvyššou v OSI modeli. Zabezpečuje viaceré protokoly, ktoré sú bežne používané (HTTP, SMTP, FTP, …). Do tejto vrstvy spadá sieťová komunikácia medzi všetkými aplikáciami vyskytujúcimi sa v sieti. Dohľadovanie kvality služieb v aplikačnej vrstve prebieha pomocou priameho pristupovania k týmto službám a sledovania ich správania.

Je dôležité si uvedomiť, že problém na ľubovolnej vrstve v OSI modeli spôsobuje nepredvídateľné správanie všetkých vyšších vrstiev. Preto napríklad pre zmysluplné dohľadovanie služby na sieťovej vrstve je potrebné mať zabezpečené dohľadovanie služieb na fyzickej aj dátovej vrstve.

2.2. Komunikácia medzi sieťou a dohľadovým systémom

V doterajších častiach bolo zatiaľ len málo povedané o komunikácii medzi sieťou a dohľadovým systémom. Napriek tomu práve táto komunikácia je jedným z kľúčových faktorov pri dohľadovaní siete. Dobrý dizajn tejto komunikácie značne zjednodušuje budovanie všetkých ďalších vrstiev dohľadovania. Aj keď sa k týmto vrstvám dostaneme až v priebehu nasledujúcich kapitol, pri abstrakcii od konkrétnych zariadení v sieti a dohľadového systému vieme získať o tejto komunikácii zaujímavé informácie. V praxi sa ukazuje, že práve táto abstrakcia

umožňuje rozdelenie metód dohľadovania tak, aby bolo použiteľné pre všetky druhy sietí. Najlogickejším a najčastejšie používaným rozdelením protokolov medzi sieťou a dohľadovým systémom je na základe toho, či bola komunikácia iniciovaná zo strany siete, alebo samotného dohľadového systému. Vo zvyšku práce budeme pre rozdelenie dohľadovania používať nasledovnú definíciu:

Dohľadovanie je klasifikované ako aktívne, ak jeho merania sú založené na dátach, ktoré sú vkladané do siete, inak sa jedná o pasívne dohľadovanie.

Pomenovanie aktívne a pasívne dohľadovanie nie je zvolené náhodne. Z pohľadu dohľadového systému musí pri aktívnom dohľadovaní vyvíjať aktivitu vysielaním dát do siete, pri pasívnom dohľadovaní, dohľadový systém pasívne očakáva správy zo siete.

Získavanie informácií o stave služby v prípade, že sa jedná o aktívne dohľadovanie, pozostáva z dvoch častí:

1. Dohľadový systém sa spýta zariadenia na stav jednej alebo viacerých jeho služieb
2. Zariadenie overí či má dohľadový systém oprávnenie pre prístup k informáciám o týchto službách. Ak áno, následne pošle späť informáciu o stave služieb, na ktoré sa dohľadový systém pýtal.

V prípade pasívneho dohľadovania pozostáva zo získania informácií o službe len z jednej časti, ktorou je odchytenie informácií zo siete v rámci dohľadového systému. V tomto prípade dohľadový systém neposiela zariadeniam v sieti žiadne požiadavky.

Podľa týchto parametrov je možné z pohľadu dohľadovateľnosti rozdeliť služby na 4 skupiny: služby bez možnosti dohľadovania, služby s možnosťou aktívneho dohľadovania, služby s možnosťou pasívneho dohľadovania a služby s možnosťou aktívneho aj pasívneho dohľadovania. Toto rozdelenie je zobrazené na obrázku 2,2.

		Aktívne dohľadovanie	
		Nie	Áno
Pasívne dohľadovanie	Nie	Služby bez možnosti priameho dohľadovania	Služby s možnosťou aktívneho dohľadovania
	Áno	Služby s možnosťou pasívneho dohľadovania	Služby s možnosťou aktívneho aj pasívneho dohľadovania

Tabuľka 2.1 – Rozdelenie služieb na základe možnosti dohľadovania

V nasledujúcich častiach budú jednotlivé skupiny podrobnejšie opísané.

2.2.1. Služby bez možnosti dohľadovania

Tento druh služieb je pre proces dohľadovania najnevýhodnejší. Nielen že nevieme o týchto službách zistiť nič priamo, ale ak v prípade poruchy ich funkčnosti spôsobujú problémy ďalších zariadení a služieb, je často nemožné odhaliť presnú príčinu problémov. Ako príklad z praxe môžeme uviesť výpadky elektrickej energie. V prípade, že nemáme možnosť dohľadovať úroveň napájania zariadenia, môže byť toto zariadenie vypnuté a nebudeme vedieť určiť, či k jeho výpadku došlo z dôvodu nefunkčnosti zariadenia alebo došlo k výpadku napájania.

Ale práve tento vplyv priamo nedoľadovateľnej služby na iné dohľadovateľné služby bežiace na zariadeniach v sieti je možné využiť na nepriame dohľadovanie tejto služby. Takéto dohľadovanie sa nazýva dohľadovanie pomocou závislostí. V praxi vyzerá scenár takéhoto dohľadovania nasledovne:

1. Pri konfigurácii dohľadového systému zadefinujeme službu, ktorá nebude dohľadovaná pasívnou ani aktívnou metódou
2. Pre túto službu zadefinujeme jednu, alebo viac závislostí na iných službách.
3. V prípade, že dôjde k problémom všetkých týchto služieb, dohľadový systém vyhlási, že problém má aj táto služba

Využitie takéhoto dohľadovania je možné demonštovať na predchádzajúcom príklade s napájaním zariadenia. S dostatočne vysokou pravdepodobnosťou

môžeme predpokladať, že ak vypadnú postupne všetky služby bežiace na jednom zariadení, tak došlo k výpadku elektrickej energie a je možné spustiť akcie naväzujúce na tento výpadok. Pri osobnej kontrole sa potom tento problém môže, ale aj nemusí potvrdiť.

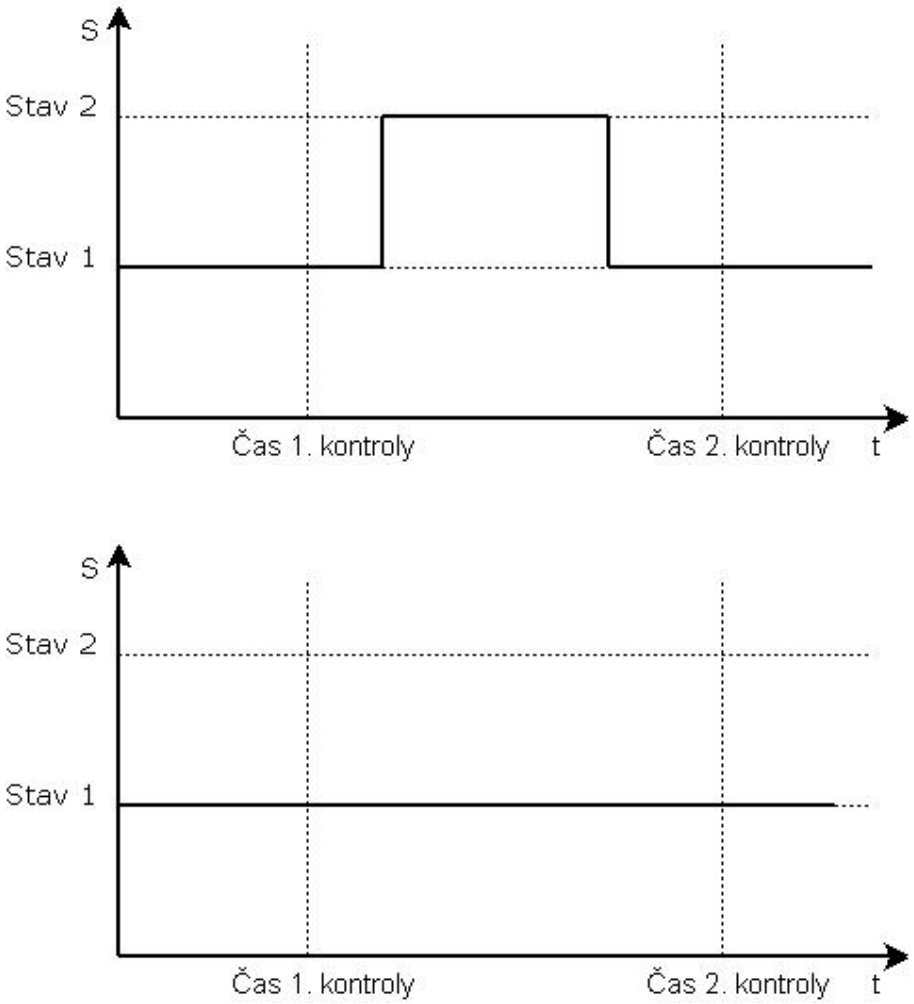
V praxi je často podstatne výhodnejšie podniknúť akciu na odstránenie potenciálneho problému, ako jeho neodstránenie vôbec. Z tohoto dôvodu sa vyskytuje aj takéto využitie nepriameho dohľadovania služieb.

2.2.2. Služby s možnosťou aktívneho dohľadovania

Služby z tejto kategórie je možné dohľadovať na základe posielania požiadaviek príslušným zariadeniam. V prvom kroku sa dohľadový systém spýta zariadenia na stav jednej alebo viacerých z jeho služieb, v druhom pošle zariadenie späť dohľadovému systému informáciu o stave príslušnej služby. Tento proces je po vopred definovanom čase opakovaný.

Takýto spôsob dohľadovania umožňuje získať informáciu o stave príslušnej služby v jednotlivých časových okamihoch. Medzi dvomi takýmito okamihmi musíme predpokladať, že stav služby ostáva nemenný. Tento predpoklad so sebou ale prináša viac problémov.

Najhlavnejším problémom je, že dohľadový systém nemôže zaregistrovať zmenu stavu príslušnej služby ak došlo k zmene jej stavu a návratu do pôvodného medzi dvomi po sebe nasledujúcimi kontrolami. Výskyt problému je zobrazený na obrázku 2.3.

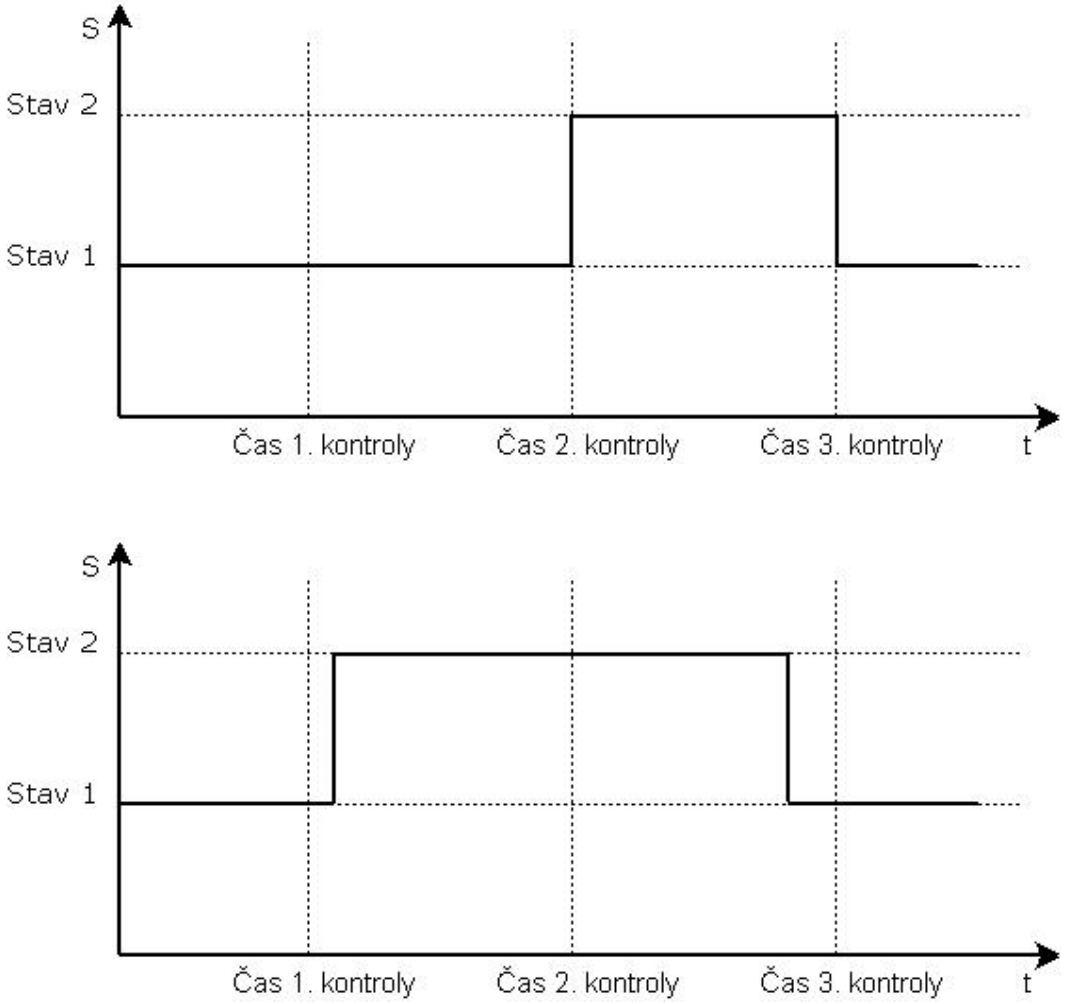


Obrázok 2.2 – Reálny priebeh udalosti v sieti
a priebeh zaregistrovaný dohľadovým systémom

V tomto príklade dohľadový systém nezaregistroval zmenu zo stavu 1 do stavu 2 a späť počas intervalu medzi dvomi kontrolami služby.

Takéto krátkodobé zmeny stavov služieb nie je potom možné pomocou dohľadového systému overiť. Niektoré zariadenia udržujú vlastnú históriu záznamov, pomocou ktorej je možné tieto udalosti neskôr overiť, ale už samotné nezaevidovanie ich existencie dohľadovým systémom nepridáva tejto metóde dohľadovania na dôveryhodnosti. Navyše pri väčšine zariadení je táto história pri reštarte zmazaná, prípadne sa v nej udržuje len obmedzený počet záznamov o posledných udalostiach ku ktorým došlo.

Ďalším problémom pri aktívnom dohľadovaní je aj zistenie presnej dĺžky výpadku. V prípade, že k zmene stavu služby dôjde v čase medzi dvomi kontrolami stavu služby, nie je možné určiť kedy presne došlo k zmene. Toto je veľký problém v prípade, že je potrebné určiť presnú dĺžku trvania výpadku. Príklad takéhoto problému je zobrazený na obrázku 2.4.



Obrázok 2.3 – Skutočná doba trvania udalosti
a doba trvania zaregistrovaná dohľadovým systémom

V tomto prípade nie je možné určiť presné trvanie výpadku služby vôbec. Podľa informácií, ktoré má k dispozícii dohľadový systém, výpadok trval presne dĺžku intervalu medzi dvomi kontrolami služieb, reálny stav v sieti bol však iný.

Aby sa minimalizovali dôsledky predchádzajúcich dvoch problémov je potrebné zmenšiť interval medzi dvomi kontrolami služieb na minimálnu možnú hodnotu. Keď napríklad potrebujeme, aby dohľadové centrum dostávalo informácie najviac s minútovým oneskorením oproti reálnemu stavu, je potrebné tomu prispôsobiť dĺžku intervalu medzi dvomi kontrolami. Pri veľkom množstve dohľadovaných služieb to môže spôsobiť zahltenie dohľadového systému a jeho znefunkčnenie. Maximálnu dĺžku intervalu medzi dvomi kontrolami služieb je možné odvodiť od garantovanej dostupnosti služby.

Ako praktický príklad použitia aktívneho dohľadovania je možné použiť dohľadovanie kvality služieb servera, ktorý komunikuje s klientmi cez protokol HTTP. Dohľadovanie bude v tomto prípade obsluhovať jednoduchý HTTP klient, ktorý sa pripojí na službu HTTP bežiacu na serveri, vypýta si konkrétnu stránku a čaká na odpoveď. Ak za vopred stanovený časový interval nedostane odpoveď, alebo sa mu vráti chyba, vyhlási službu HTTP za nefunkčnú. Ak odpoveď obdrží, na základe času ktorý prešiel od odoslania požiadavky vyhlási službu HTTP za problematickú alebo v poriadku. Príslušné časové intervaly musia byť samozrejme zadefinované vopred. Keď bude tento program periodicky spúšťaný, budeme poznať stav služby HTTP v konkrétnych časových intervaloch.

2.2.3. Služby s možnosťou pasívneho dohľadovania

Pasívne dohľadovanie je do značnej miery odlišné od aktívneho. Kým aktívne dohľadovanie vyžaduje plánovanie kontrol služieb, pri pasívnom dohľadovaní nie sú plánované žiadne kontroly, dohľadový systém očakáva správu od zariadenia bez predchádzajúcej výzvy. Takúto správu budeme vo zvyšku textu nazývať notifikáciou. Notifikácia od zariadenia väčšinou prichádza pri zmene stavu služby, ale nemusí to byť pravidlom. Typickým príkladom kedy je to inak je dohľadovanie charakteristiky dát prechádzajúcich po sieti. Tento spôsob dohľadovania je podstatne efektívnejší ako aktívne dohľadovanie, tiež však so sebou prináša viacero problémov. Tieto problémy sú ale inej povahy ako tie, s ktorými sa stretávame pri aktívnom dohľadovaní.

Prvým z nich je, že v momente pridania služby do dohľadového systému nie je možné nič určiť o stave kontrolovanej služby. Táto služba teda ostáva v neznámom stave až do prvej notifikácie o zmene jej stavu. Toto môže spôsobovať problémy vtedy, keď na začiatku dohľadovania služby bola v kritickom stave. Až do prijatia notifikácie o zmene jej stavu o tomto probléme dohľadový systém nevie. Jediným spôsobom, ako dostať do dohľadového systému informáciu o aktuálnom stave služby je mu manuálne poslať notifikáciu. Takúto umelú notifikáciu nie je ale možné vždy úspešne vytvoriť a odoslať.

Ďalším problémom pri tejto metóde je možná strata notifikácie od zariadenia hosťujúceho danú službu. Ak protokol pre posielanie správ nepočíta s potvrdzovaním správ, prípadnú stratu správy nie je možné zistiť. Napriek tomuto zjavnému problému je potvrdzovanie prijatia správ vytvorené len veľmi zriedkavo. Je tomu hlavne preto, lebo pasívne dohľadovanie služieb počíta s tým, že dohľadované zariadenie nesmie vedieť o tom, že ním posielané dáta sú odchytávané a spracúvané. Strata notifikácie môže byť dokonca spôsobená stratou spojenia medzi dohľadovým systémom a zariadením, napríklad pri výpadku elektrickej energie. Len na základe prijímania dát od zariadenia nie je možné takýto problém vôbec zistiť.

Tretím problémom, ktorý vzniká pri pasívnom dohľadovaní je zabezpečenie bezpečnosti. Pri scenári, v ktorom sú zachytávané akékoľvek dáta voľne prechádzajúce po sieti môže dôjsť k nežiadúcemu úniku informácií. Preto je potrebné nasádzať pasívne dohľadovanie dátových tokov veľmi opatrne. Úroveň potrebnej bezpečnosti sa ale samozrejme líši od prípadu k prípadu v závislosti od dôvernosti informácií prechádzajúcich po danej sieti.

Ako praktický príklad aplikácie dohľadovania služby čisto pasívnou metódou je možné použiť už spomínané dohľadovanie dát pretekajúcich po sieti. Pre takéto dohľadovanie je potrebné na zariadení vytvoriť sieťové rozhranie, na ktoré sa budú kopírovať všetky dáta prechádzajúce týmto zariadením a na tomto rozhraní sledovať prenášané dáta, prípadne vložiť do siete premostenie a sledovať prenášané dáta na ňom. Takto zozbierané informácie je následne možné analyzovať a v prípade, že charakter prenášaných dát prekročí vopred stanovené kritériá, zmení

sa stav príslušnej služby v dohľadovom systéme. Takýto prístup k dohľadovaniu však prináša bezpečnostné aj výkonové problémy, je preto často potrebné na prijímané dáta aplikovať vhodným spôsobom filter a až následne spracovávať.

Iným príkladom použitia čisto pasívneho dohľadovania je dohľadovanie fyzickej sieťovej vrstvy. Moderné zariadenia s podporou odosielania notifikácií jednému alebo viacerým adresátom majú väčšinou možnosť odoslať notifikáciu pri zmene stavu ľubovolného z ich rozhraní. V rámci dohľadového systému sú tieto informácie odchytávané a prevádzané na zmeny stavu dohľadovanej služby.

2.2.4. Služby s možnosťou pasívneho a aktívneho dohľadovania

Poslednou kategóriou služieb sú služby, ktoré je možné dohľadovať aktívnou aj pasívnou metódou. Aktívne a pasívne dohľadovanie tej istej služby je možné rôznymi spôsobmi kombinovať a postaviť tak dostatočne vhodný model dohľadovania služby. Cieľom tejto kombinácie je spojiť prednosti aktívneho a pasívneho dohľadovania a zároveň vzájomne eliminovať ich nedostatky. Zo všetkých možností kombinácie týchto dvoch metód dohľadovania vyberám dva najčastejšie používané.

Prvá možnosť ich kombinácie je vo svojej podstate len rozšírením pasívneho dohľadovania služby o občasné aktívne kontroly. Pasívne dohľadovanie umožňuje dohľadovému systému čakať na správu od zariadenia, pričom si v pravidelných intervaloch (spravidla podstatne väčších ako pri čisto aktívnom dohľadovaní) aktívne skontroluje, či nedošlo k strate správy od zariadenia o zmene stavu služby. Využitie tejto metódy je výhodné hlavne vtedy, keď sú pasívne správy od zariadenia sporadické a vyskytujú sa v nepravidelných intervaloch, napríklad výpadky elektrickej energie, alebo výpadky na telekomunikačných okruhoch.

Druhá možnosť kombinácie pasívneho a aktívneho dohľadovania je trochu komplikovanejšia. V podstate sa tiež jedná o rozšírenie pasívneho dohľadovania, zásadný rozdiel je ale v tom kedy sa plánujú aktívne kontroly služieb. Využíva sa tu informácia o tom, kedy naposledy došla správa o zmene stavu služby, pričom sa neberie do úvahy informácia, či sa stav služby „zmenil“ na ten istý stav. Jedná sa o teda o *čerstvosť informácie* o stave služby. Aktívna kontrola stavu služby je

naplánovaná až v momente, keď čerstvosť informácie prekročí vopred danú hodnotu. Táto kombinácia je vhodná hlavne vtedy, ak vie zariadenie posielať správu o tom, že služba pracuje v poriadku, ale nevie zistiť alebo poslať správu, keď služba pracovať prestane. Túto metódu je vhodné použiť aj v prípade častého a pravidelného odosielania notifikácií.

Ako príklad z praxe môže slúžiť server pre elektronickú poštu. Tento server prijíma elektronickú poštu a pri každom prijatí správy vie odoslať dohľadovému systému informáciu o tom, že sa mu to podarilo. Takisto je možné poslať notifikáciu, keď sa korektnú správu nepodarilo doručiť, napríklad pre nedostatok miesta na pevnom disku. Môže ale tiež dôjsť ku chybe, ktorá spôsobí zaseknutie poštového servera, pričom často sú za takéto narušenia činnosti zodpovedné antivírové programy na kontrolu elektronickej pošty. V takomto prípade dohľadový systém nedostane informáciu o zastavení činnosti, čerstvosť informácie prekročí vopred stanovenú hranicu a je naplánovaná aktívna kontrola služby. Tá následne problém zistí.

Samozrejme existujú aj iné možnosti, ako je možné skombinovať výhody aktívneho a pasívneho dohľadovania. Na väčšinu dohľadovaných služieb je ale možné jednoducho aplikovať jednu z predchádzajúcich dvoch metód.

2.2.5. Štandardy

Komunikácia medzi sieťou a dohľadovým systémom bola dlhú dobu neštandardizovaná. Každé zariadenie komunikovalo pomocou vlastného, väčšinou uzavretého protokolu. Navyše vedelo komunikovať len s jedným dohľadovým systémom, ktorý bol zväčša dodávaný k zariadeniu, pretože žiadny iný nevedel komunikovať pomocou daného protokolu. V dnešnej dobe tento problém pretrváva u väčšiny PDH zariadení, ktoré komunikujú cez sériový port pomocou vlastných protokolov. Dohľadové centrum teda muselo využívať množstvo dohľadových systémov, ktorých vzájomná informačná integrácia bola v podstate nemožná. Z tejto patovej situácie mohol dohľadovanie vytiahnuť len štandardizovaný protokol pre dohľadovanie sietí.

Takýmto štandardom medzi protokolmi sa stal Simple Network Management Protocol, skrátene SNMP, slúžiaci pre manažment TCP/IP sietí. Slovko manažment nie je zvolené náhodne, protokol SNMP totiž okrem dohľadovania podporuje aj nastavovanie zariadení v sieti. Túto funkcionalitu používajú bežne manažmentové konzoly, napríklad HP OpenView alebo Novell ManageWise. Protokol SNMP bol vyvinutý začiatkom roku 1988. Jeho prvá verzia, často uvádzaná ako SNMPv1, pozostáva z troch komponentov. Každý z nich bol uvedený vo forme vlastného RFC:

- Structure of Management Information (SMI) v RFC 1155
- Management Information Base (MIB) v RFC 1156
- Samotný protokol SNMP v RFC 1157

Ako pri každej novej technológii sa aj pri protokole SNMP objavili jeho slabé stránky a priestor pre vylepšenia. Ako hlavný nedostatok protokolu SNMPv1 bola označená bezpečnosť, keďže využíval len triviálnu metódu overovania užívateľov pomocou *komunít*. Tento nedostatok sa stal hlavnou motiváciou pre vytvorenie novšieho štandardu.

Prvým pokusom doplniť dodatočnú bezpečnosť do protokolu SNMP bol v roku 1992 protokol SNMPsec, ktorý definoval nový spôsob overovania užívateľov pomocou lokálnych identifikátorov nazývaných *skupiny (parties)*. Tento pokus ale nebol širšie akceptovaný a pozornosť sa upriamila na novú verziu protokolu SNMPv2. Tento obsahoval overovanie užívateľov pomocou skupín ako tomu bolo pri SNMPsec, doplnil však aj ďalšie rozšírenia. Podstatným rozšírením bolo napríklad rozšírenie SNMP počítadiel z pôvodných 32 bitových na 64 bitové z dôvodu vzniku rýchlejších sieťových rozhraní. Tento protokol ale z dôvodu svojej zložitosti tiež nebol akceptovaný. Stal sa ale základom pre viacero „dcérskych“ protokolov:

- SNMPv2p, ktorý je v podstate pôvodným protokolom SNMPv2
- SNMPv2c, ktorý sa vracia ku komunitám používaným v protokole SNMPv1
- SNMPv2u, ktorý namiesto komunít prináša overovanie užívateľov pomocou užívateľských mien

Z týchto protokolov sa stal paradoxne najúspešnejším a najširšie podporovaným práve protokol SNMPv2c, aj keď v oblasti bezpečnosti bol krokom späť k protokolu SNMPv1. Napriek tomu, že RFC 1901 definujúce tento štandard je ešte stále kategorizovaný ako experimentálny, dosiahol protokol SNMPv2c úspech, aký sa žiadnemu inému z protokolov odvodených od SNMPv2 nikdy nepodaril.

Tento zmätok v množstve protokolov odvodených od SNMPv2 viedol k snahe štandardizovať nový protokol. Vyvrcholením tejto snahy sa stal v roku 1998 návrh protokolu SNMPv3, ktorý je najnovším z rodiny SNMP protokolov a prináša vyššiu mieru bezpečnosti do manažmentu sietí. Protokol SNMPv3 bol definitívne štandardizovaný v decembri 2002 v RFC 3414 a do dnešného dňa zahrnula protokol SNMPv3 do svojich sieťových zariadení väčšina výrobcov. Napriek tomu je v dnešnej dobe medzi užívateľmi najrozšírenejším použitie protokolu SNMPv2c vzhľadom k dlhodobým skúsenostiam s týmto protokolom a jeho bezpečnostnou schémou. Hlavne kvôli tomuto faktu bola v auguste 2003 v RFC 3584 definovaná koexistencia medzi protokolmi SNMPv1, SNMPv2 a SNMPv3. Protokol SNMPv3 je ale napriek tomu do budúcna najlepším kandidátom pre štandard v dohľadovaní sietí.

Pri dohľadovaní sietí prostredníctvom protokolu SNMP sú poskytované informácie prístupné vo forme množiny navzájom poprepájaných objektov. Manažovateľné objekty sú definované pomocou *Management Information Base (MIB)* súborov. Atribúty týchto objektov obsahujú hodnoty, ktoré majú význam pre dohľadovanie sietí. S novou verziou SNMPv2 pribudli nové možnosti na výmenu informácií, čo vyústilo v pridanie ďalších MIB súborov. Tieto súbory špecifické pre SNMPv2 sú nazývané MIB-II a sú definované v RFC1213.

MIB súbory sú písané vo formáte OSI Abstract Syntax Notation One (ASN.1). Pre presnejšie popísanie štruktúry týchto objektov je používaná adaptovaná podmnožina ASN.1 nazývaná *Structure of Management Information* (SMI). So štandardizovaním SNMPv2 a MIB-II vznikla potreba vylepšení tohoto spôsobu popisovania objektov. Pre tento nový spôsob popisovania objektov sa ustálilo pomenovanie SMIv2.

Ako príklad definície SNMP objektu je možné použiť objekt *sysContact*, slúžiaceho na archiváciu kontaktu na osobu zodpovednú za správu daného zariadenia. Tomuto objektu je najčastejšie priradená e-mailová adresa zodpovednej osoby. Definícia tohoto objektu pochádza z MIB súboru SNMPv2-MIB.

sysContact OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string."
::= { system 4 }

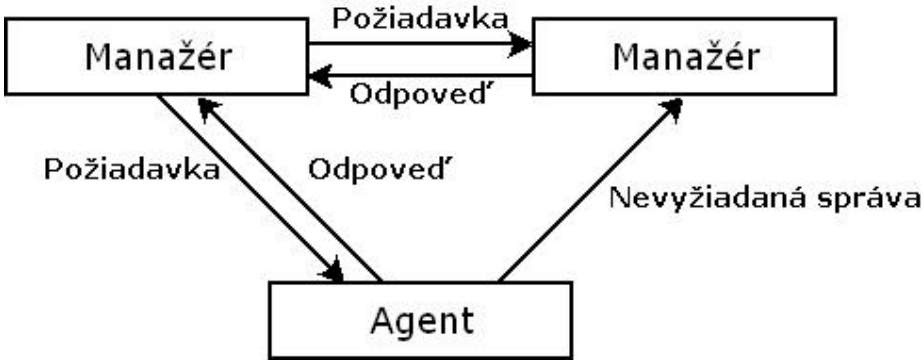
Komunikácia pomocou protokolu SNMPv2 je vytvorená v duchu objektovo orientovaného programovania, je teda založená na pojmoch entít. SNMPv2 entity majú 2 druhy: agent, alebo manažér. Agent je proces, ktorý využíva informácie priamo od zariadenia. Manažér je proces, ktorý od agenta získava nazbierané informácie. Každá entita môže fungovať buď ako manažér, alebo ako agent, alebo ako obidva naraz.

V SNMPv2 existujú 3 typy komunikácie:

- požiadavka od manažéra – odpoveď od manažéra,
- požiadavka od manažéra – odpoveď od agenta
- nevyžiadaná správa od agenta.

V prvom type pošle jeden manažér požiadavku inému manažérovi a ten mu následne odpovie. Druhá metóda je podobná, manažér pošle požiadavku agentovi a ten mu odpovie. Tretia metóda pozostáva z jedného kroku a tým je nevyžiadaná správa od agenta pre manažéra bez predchádzajúcej požiadavky. Manažér agentovi neposiela žiadnu informáciu o tom, že by k nemu správa dorazila v poriadku. Táto tretia metóda je základom pre pasívne dohľadovanie

pomocou protokolu SNMPv2. Všetky tieto druhy komunikácie sú zobrazené na obrázku 2.5.



Obrázok 2.4 – Druhy SNMP komunikácie

Remote Network Monitoring (RMON) je štandard pre dohľadovanie dát v internete. Jedná sa o štandard, ktorý je cielene využívaný dodávateľmi sieťových zariadení tak, aby ľubovoľné zariadenie zodpovedajúce špecifikácii RMON vedelo komunikovať s ľubovolným manažmentovým programom zodpovedajúcim tej istej špecifikácii. RMON bol originálne štandardizovaný v novembri 1991 v rámci RFC 1271, ale bol následne doplnený vo februári 1995 v RFC 1757. Práve RFC 1757 sa stalo štandardom, ktorý hovorí o jeho implementácii.

Hlavným cieľom štandardu RMON je umožniť vytváranie zariadení, ktoré mu zodpovedajú. O takýchto zariadeniach sa hovorí väčšinou ako o monitoroch alebo sondách *(probe)*, ktoré dohľadujú špecifické aspekty siete bez interferencie s jej normálnou prevádzkou. Tieto zariadenia zväčša fungujú samostatne vo vzdialených častiach siete, dokonca aj za jej hranicami. Štandard RMON umožňuje týmto zariadeniam komunikovať cez samotnú sieť, ktorú dohľadujú. Obvykle je štandard RMON naprogramovaný tak, aby fungoval pre ľubovolnú sieť. Sú ale vytvorené špecifiká, ktoré slúžia na dohľadovanie sietí na báze ethernetu. Programy, ktoré zodpovedajú špecifikácii RMON sú pomenúvané ako RMON manažéri. Ciele špecifikácie RMON sú teda nasledovné:

- Operácia pri prerušení spojenia – sondy môžu byť umiestnené na vzdialených miestach a preto sú stavané tak, aby mohli pokračovať v zbieraní dát, aj keď je manažment siete nedostupný.

- Proaktívne dohľadovanie – sondy zbierajú dáta neustále a to aj vtedy, keď sa v sieti nevyskytujú žiadne problémy. Z dlhodobého hľadiska to umožňuje vytvoriť model štandardného správania siete, ktorý je možné použiť ako základ pre porovnávanie v prípade výpadku.
- Zistenie a oznámenie problému – sondy majú byť schopné samostatne zistiť problém v sieti. Keď časť zariadenia nepracuje správne, sonda informuje RMON manažéra o probléme.
- Inkrementálne dáta – sondy majú udržiavať aj štatistiky, ktoré nie sú priamo využívané pri detekcii problémov. Napríklad sa môže jednať o objem dát prichádzajúci od niektorého iného zariadenia v sieti. Tieto štatistiky je potom možné použiť pri plánovaní ďalšej expanzie siete.
- Viacerí manažéri – sondy majú byť dohľadovateľné a vedieť posielať notifikácie viacerým RMON manažérom. Táto vlastnosť umožňuje redundanciu v procese dohľadovania sond a taktiež vytvorenie distribuovaného dohľadovania.

Logickým rozšírením štandardu RMON je RMON2. Cieľom RMON2 sú vyššie vrstvy ako je kontrola prístupu k médiu. Dôraz je kladený hlavne na IP a aplikačnú vrstvu. Na rozdiel od štandardu RMON, RMON2 je zameraný výlučne na používanie v dohľadových systémoch a nie na používanie ľuďmi. Každý dohľadovaný objekt musí mať zadefinované meno, syntax, úroveň prístupu a implementačný status. Meno objektu sa používa na jeho jednoznačnú identifikáciu. Syntax je štruktúra popísaná použitím notácie ASN.1, ktorá umožňuje pochopiť monitorovaný objekt. Úroveň prístupu označuje, či je možné dohľadovaný objekt len čítať, len zapisovať jeho hodnotu, alebo oboje. Implementačný status popisuje status aktuálneho objektu a môže mať jednu zo 4 hodnôt: povinný *(mandatory)*, voliteľný *(optional)*, zastaralý *(obsolete)*, alebo nedoporučovaný *(deprecated)*.

Štandardy RMON a RMON2 sú používané na dohľadovanie sietí založených na rámcoch. S nárastom využívania prepínacích sietí typu ATM je v súčasnosti vyvíjaný nový štandard SMON, ktorý je rozšírením štandardu RMON2 pre prepínané siete. Názov SMON ešte nie je definitívny a celý štandard je ešte v

štádiu vývoja. Problematické oblasti pre túto extenziu sú v odlišných vlastnostiach prepínaných sietí od rámcových:

- spojovo orientované spojenia
- veľa zdrojov potrebných na dohľadovanie
- agregácia dát
- používanie technológie 802.1q
- prioritizácia
- zameranie na pakety a nie rámce.

2.2.6. Porovnanie aktívneho a pasívneho dohľadovania

Pasívne a aktívne dohľadovanie predstavujú dva úplne odlišné prístupy k dohľadovaniu. Aj keď služby je väčšinou teoreticky možné dohľadovať aktívne aj pasívne, často je potrebné z výkonových, časových, programovacích, alebo bezpečnostných dôvodov obmedziť sa iba na jednu metódu. Je teda žiadúce pre každú službu určiť, či je pre ňu vhodnejší spôsob aktívneho alebo pasívneho dohľadovania a tento si vybrať. Nasledovné rozdelenie služieb na základe ich charakteristiky slúži ako nápoveda, ktorým smerom sa pri dohľadovaní tej ktorej služby vydať. Vo všeobecnosti je aktívny prístup vhodné použiť, ak spadá dohľadovaná služba do jednej z týchto kategórií:

- služba charakterizuje zdravosť systému (zaťaženie servera, latencia siete, …)
- služba je aplikačne orientovaná (HTTP, SMTP, streamovanie multimédií, …)

Pasívny prístup je vhodné zvoliť za nasledovných okolností:

- služba popisuje stav siete (množstvo prechádzajúcich dát, stav sieťových rozhraní v sieti)
- účtovné účely

Tieto zásady ale nemusia platiť pre všetky služby, napríklad množstvo prenesených dát nie je vždy žiadúce počítať pasívne, ale radšej aktívne odčítať stav počítadiel na začiatku a konci zvoleného obdobia. Preto v rámci tejto práce zavedieme jednoznačnejšie rozdelenie služieb a to na základe ich príslušnosti do niektorej z

vrstiev OSI modelu. Oproti štandardným siedmim vrstvám OSI modelu zavedieme ešte jednu, ktorá nemá priamy súvis s prenášaním dát po sieti. Je ňou vrstva prostredia, ktorá popisuje parametre vplývajúce na prácu celého zariadenia. Do tejto vrstvy spadá napríklad úroveň napájania zariadenia, teplota a vlhkosť okolitého prostredia, ale napríklad aj množstvo využitej a voľnej pamäte zariadenia, vyťaženie procesora, atď. Rozdelenie týchto vrstiev aj s vhodnými metódami dohľadovania pre služby každej z nich sumarizuje nasledovná tabuľka:

Názov vrstvy	Vhodné metódy dohľadovania
Vrstva prostredia	Pasívne dohľadovanie
Fyzická vrstva	Pasívne dohľadovanie
Dátová vrstva	Pasívne a aktívne dohľadovanie
Sieťová vrstva	Pasívne a aktívne dohľadovanie
Transportná vrstva	Pasívne a aktívne dohľadovanie
Vrstva spojení	Pasívne a aktívne dohľadovanie
Prezentačná vrstva	Pasívne a aktívne dohľadovanie
Aplikačná vrstva	Aktívne dohľadovanie

Tabuľka 2.2 – Vhodné dohľadovanie jednotlivých vrstiev OSI modelu

Ako vidieť z tohoto rozdelenia, služby na sieťovej a aj nižších vrstvách je vhodné dohľadovať pasívnym spôsobom s prípadným doplnením využívania aktívneho dohľadovania na elimináciu nedostatkov rýdzo pasívneho. Vzhľadom k aplikačnej povahe služieb vo vyšších sieťových vrstvách je výhodnejšie použitie aktívneho dohľadovania.

Dôležitou vlastnosťou tohoto rozdelenia je hlavne previazanie dohľadovania týchto vrstiev. Aby mohli byť na zariadení poskytované služby na dátovej vrstve, musí v prvom rade správne pracovať vrstva fyzická. Samozrejme zariadenie nemôže fungovať správne napríklad ak nie je napájané, z toho dôvodu je potrebné aby bola v poriadku aj výkonová vrstva. Tento príklad je možné zovšeobecniť nasledovným spôsobom:

Pre prácu ľubovolnej vrstvy OSI modelu je potrebné, aby všetky nižšie vrstvy pracovali bez problémov.

Táto vlastnosť sieti je v dnešnej dobe bežne používanou praxou pri odhaľovaní problémov v ľubovolnej sieti. Zároveň odôvodňuje zaradenie výkonovej vrstvy pod fyzickú sieťovú vrstvu. Toto previazanie sieťových vrstiev je možné priamo aplikovať aj na dohľadovanie sietí:

Pre dohľadovanie služby na ľubovolnej vrstve OSI modelu je potrebné, aby boli dohľadované všetky nižšie vrstvy.

Proces návrhu efektívneho dohľadovania služby je teda potrebné začať pri najnižších vrstvách a postupne sa prepracovať až k vrstve, do ktorej táto služba spadá.

2.3. Dohľadový systém

Ďalšou vrstvou v procese dohľadovania je dohľadový systém. Dohľadový systém v praxi tvorí skupina programov, ktorej účelom je poskytovať prehľadnou formou informácie o dohľadovanej sieti. Vytvorenie dohľadového systému nie je vo svojej podstate nič zložité, skúsený programátor dokáže vytvoriť jednoduchý dohľadový systém využívajúci ICMP ping v priebehu pár hodín. Cieľom moderných dohľadových systémov je ale možnosť dohľadovať čím väčšie množstvo rôznych služieb. S pribúdajúcim množstvom služieb narastá aj veľkosť programového kódu, ktorý sa v prípade chýb v návrhu programu môže stať neohrabaným a plným chýb. Na vyriešenie tohoto problému a vytvorenie dobrého návrhu je potrebné pochopiť vnútornú štruktúru dohľadových systémov. Táto kapitola je teda venovaná analýze troch najrozšírenejších a najširšie podporovaných dohľadových systémov s otvoreným zdrojovým kódom a snaží sa o nájdenie ich spoločných čŕt. Jedná sa o dohľadové systémy OpenNMS, MON a Nagios. Analýza vnútornej štruktúry týchto programov prebehla na základe ich dokumentácie,

analýzou zdrojových kódov a ich praktickým používaním. Na základe výsledkov tejto analýzy je potom vytvorený a popísaný všeobecne použiteľný model dohľadového systému.

2.3.1 OpenNMS

Je prvým dohľadovým systémom zameraným na dohľadovanie veľkých korporátnych sietí s otvoreným zdrojovým kódom. Pozostáva nielen z komunitou podporovaného projektu, ale zahŕňa aj organizáciu zabezpečujúcu potrebnú podporu a tréning pre prácu s ním. Pre zabezpečenie podpory čím väčšieho množstva operačných systémov bol programátormi zvolený pre implementáciu jazyk Java. Tieto faktory sú hlavným dôvodom, prečo sa z OpenNMS postupom času stal najpopulárnejším dohľadovým systémom s otvoreným zdrojovým kódom.

Architektúru OpenNMS je možné rozdeliť do troch častí. Prvou celistvou časťou sú moduly pre prácu so sieťou, pričom v súčasnosti sa jedná o nasledovné moduly:

- Aktívne zberače informácií zo siete *(Pollers)*, ktoré za účelom štatistík zozbierané informácie zo siete ukladajú do RRD databáz. Tieto informácie sú taktiež ďalej spracovávané v rámci dohľadového systému.
- ICMP komunikátor *(ICMPD)*, informácie z ktorého sú používané za účelom automatického objavovania zariadení v sieti. Taktiež ho je možné použiť ako jeden z aktívnych zberačov informácií.
- Zberač SNMP notifikácií zo siete *(TRAPD)*, ktorý je využívaný pre pasívne dohľadovanie pomocou protokolu SNMP. Získané informácie sú následne ďalej spracovávané.
- Zberač informácií o zariadeniach v sieti *(CAPSD)*, ktorý je používaný pre automatické zistenie aké služby poskytujú zariadenia v sieti.

Ďalšou časťou OpenNMS je jadro, ktoré obsahuje nasledovné súčasti:

- Modul pre spracovávanie udalostí *(EVENTD)*, ktorý prijíma informácie z modulov zabezpečujúcich komunikáciu so sieťou a na základe týchto informácií na základe vopred definovaných pravidiel vyvoláva akcie.

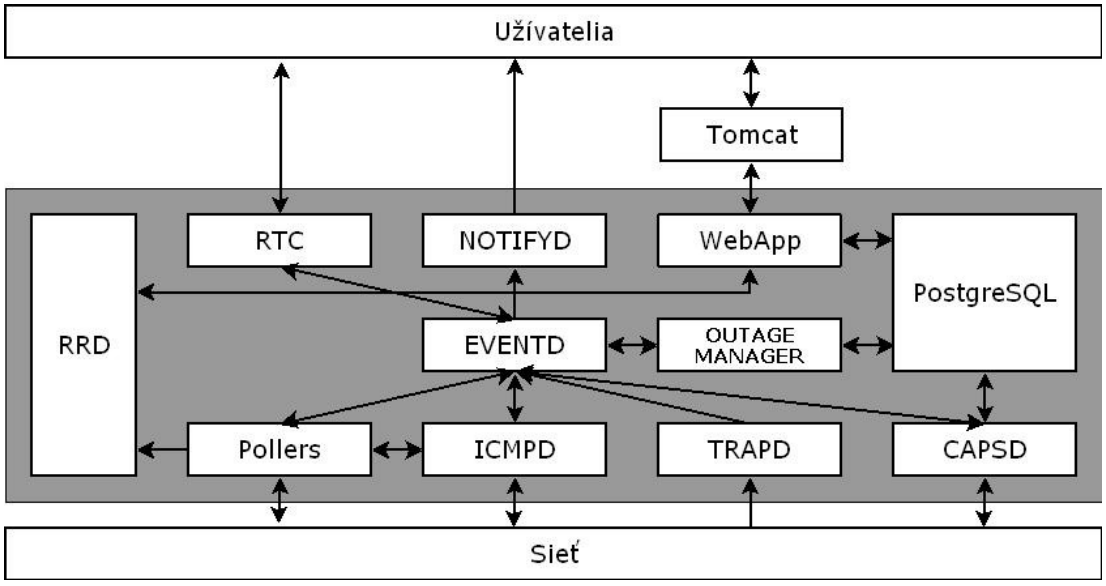
Napríklad sa môže jednať o príkaz na odoslanie notifikácie, alebo zápis do databázy výpadkov.

- Modul pre spracovávanie výpadkov *(Outage Manager)*, ktorý zapisuje do PostgreSQL databázy informácie o výpadkoch v sieti.
- Manažmentovú konzolu *(RTC)*, ktorú je možné využívať pre posielanie príkazov, ktoré má dohľadový system vykonať.

Poslednou časťou OpenNMS je prezentačné rozhranie pre prístup klientov dohľadového systému. Toto rozhranie obsahuje nasledovné dve súčasti:

- Modul pre notifikácie *(NOTIFID)*, ktorý na požiadanie posiela notifikácie klientom dohľadového systému
- Webové rozhranie *(WebApp)*, ktoré obsahuje servlety pre prístup pomocou protokolu http, pričom pre prístup k týmto servletom je umožňovaný pomocou webového servra Tomcat. Informačnou bázou pre toto rozhranie sú PostgreSQL a RRD databázy.

Celá architektúra OpenNMS v kontexte dohľadovania je zobrazená na obrázku 2.6.



Obrázok 2.5 – Architektúra OpenNMS

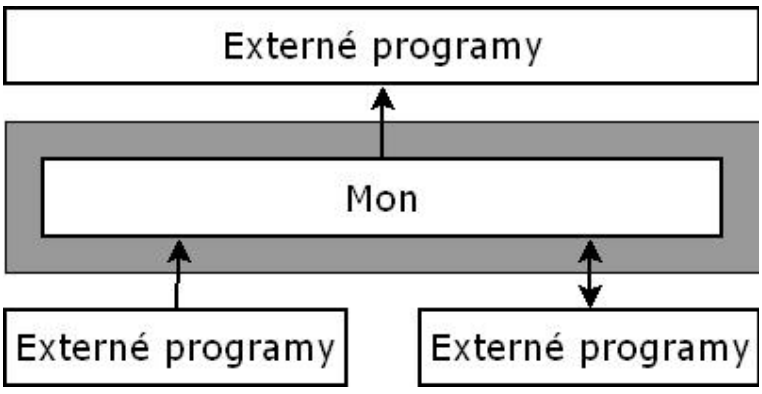
2.3.2 Mon

Dohľadový systém *Mon* bol navrhnutý tak, aby slúžil na dohľadovanie ľubovoľných služieb. V kontexte tohoto dohľadového systému môže byť službou

čokoľvek, čo je možné programovo skontrolovať. Pre zabezpečenie čím väčšej flexibility je Mon naprogramovaný výlučne ako plánovač, ktorý len volá programy zabezpečujúce kontroly služieb a spúšťajúci notifikácie v prípade že kontrolné programy zistia problém. Reálne kontroly služieb ani reporty ale nie sú súčasťou vnútornej štruktúry dohľadového systému.

Tento model bol zvolený z dôvodu jeho veľkej rozšíriteľnosti. Taktiež tento model nevyžaduje pri pridávaní dohľadovania nového druhu služby upravovať samotný zdrojový kód. Napríklad dohľadovanie teploty v miestnosti je možné zabezpečiť pomocou jednoduchého externého programu, ktorý zabezpečuje komunikáciu s teplotnými senzormi pomocou sériového portu. Taktiež notifikácie pomocou sms správ je možné jednoducho zabezpečiť pomocou externého programu zabezpečujúceho komunikáciu s GSM bránou. Jediným pevne naprogramovaným rozhraním je možnosť prijímať špeciálne notifikácie, pre ktoré sa ustálilo pomenovanie Mon trap. Táto funkcionalita umožňuje budovať pasívne a distribuované dohľadovanie.

Architektúra tohto dohľadového systému je veľmi jednoduchá. Celé dohľadovanie zabezpečuje jeden program napísaný v programovacon jazyku Perl, ktorý len vyvoláva externé programy a zachytáva pasívne notifikácie. Schéma tejto štruktúry je zobrazená na obrázku 2.7.



Obrázok 2.6 – Štruktúra dohľadového systému Mon

2.3.3 Nagios

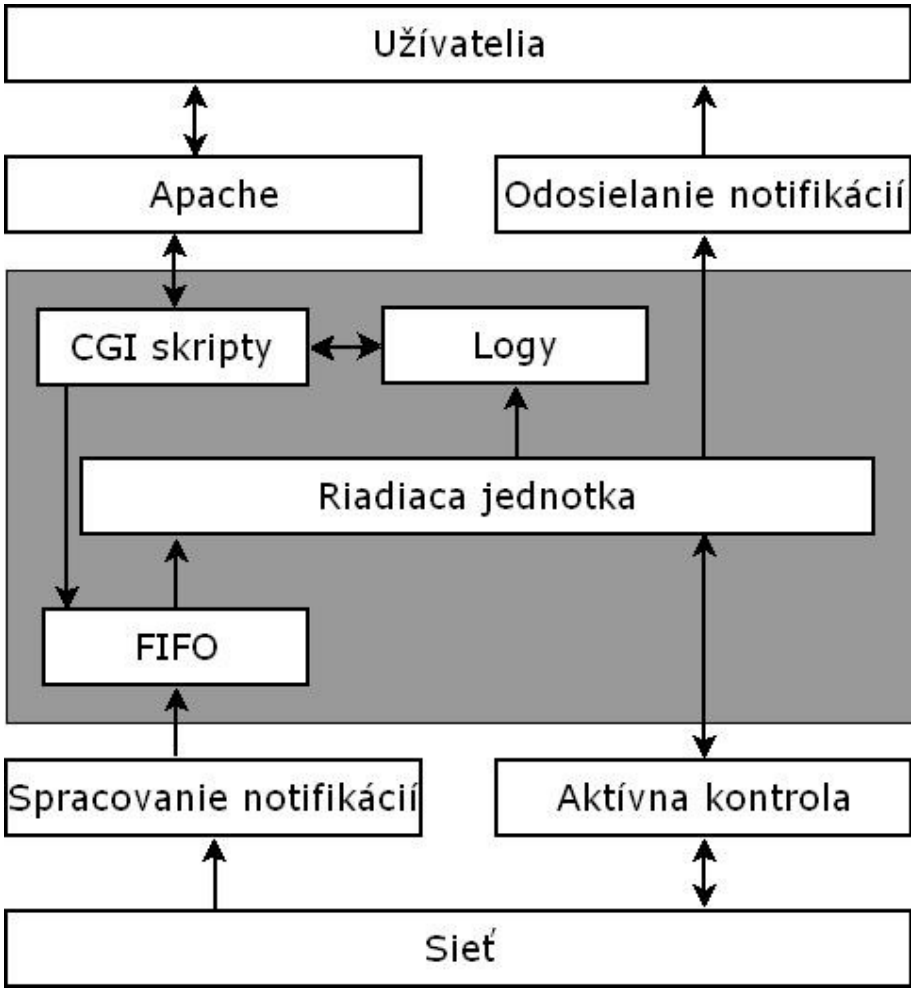
Tento projekt mal pôvodne názov Netsaint, v roku 2002 bol ale premenovaný na Nagios. Napriek tomuto faktu veľa zdrojov stále používa pomenovanie Netsaint. Svojím zameraním a štruktúrou sa Nagios nachádza niekde na pol ceste medzi dohľadovými systémami OpenNMS a Mom, no niektoré z jeho funkcionalít predčí oba tieto dohľadové systémy. Ako programovací jazyk pre implementáciu fixných častí tohoto bol pre jeho rýchlosť zvolený jazyk C.

Tak ako pri dohľadovom systéme Mon, je aj Nagios zameraný na čím väčšiu rozšíriteľnosť. Aktívna komunikácia so zariadeniami v sieti prebieha pomocou vyvolania externých programov a odchytenia jeho návratovej hodnoty a výstupu. No pasívne dohľadovanie zachádza vo svojej všeobecnosti ešte ďalej ako Mon. Pasívna komunikácia je implementovaná len vo forme práce s FIFO súborom, do ktorého externé programy zapisujú hlásenia o zmene stavu konkrétnej služby. Takýto prístup umožňuje prijímať ľubovoľné notifikácie nezávisle na použití konkrétneho sieťového protokolu.

Všetku komunikáciu vo vnútri dohľadového systému zabezpečuje riadiaca jednotka *(Core Logic)*. Táto má na starosti načítavanie konfigurácie, plánovanie a volanie aktívnych kontrol služieb v sieti, spracovávanie pasívnych notifikácií a zapisovanie logov.

Pre klientov dohľadového systému sú k dispozícii dva spôsoby, ako získať informácie uložené v dohľadovom systéme. Funkcionalita notifikácií je zabezpečovaná pomocou volania externých programov priamo z riadiacej jednotky dohľadového systému. Pre prístup k uloženým informáciám je tiež k dispozícii priamo v distribúcii dynamické rozhranie v podobe CGI skriptov, ktoré berú ako svoju informačnú bázu logy dohľadového systému a majú možnosť posielať príkazy riadiacej jednotke pomocou toho istého FIFO súboru, ktorý slúži pre prijímanie pasívnych notifikácií. Tieto CGI skripty je možné sprístupniť pomocou ľubovoľného webového servra s podporou spúšťania CGI skriptov, autori tohto dohľadového systému doporučujú použitie webového servra Apache.

Schéma vnútornej štruktúry v kontexte dohľadovania je zobrazená na obrázku 2.8.



Obrázok 2.7 – Štruktúra dohľadového systému Nagios

2.3.4., Model dohľadového systému

Je jasne vidieť, že tieto dohľadové systémy majú veľmi podobnú vnútornú štruktúru. Aj keď tieto tri programy sú len malou vzorkou zo všetkých voľne dostupných dohľadových systémov, túto vnútornú štruktúru s rôznymi drobnými obmenami je možné nájsť vo väčšine z nich. Na základe predchádzajúcej analýzy teda vieme rozdeliť dohľadový systém na tri časti, ktoré spolu navzájom komunikujú cez jasne určené rozhrania:

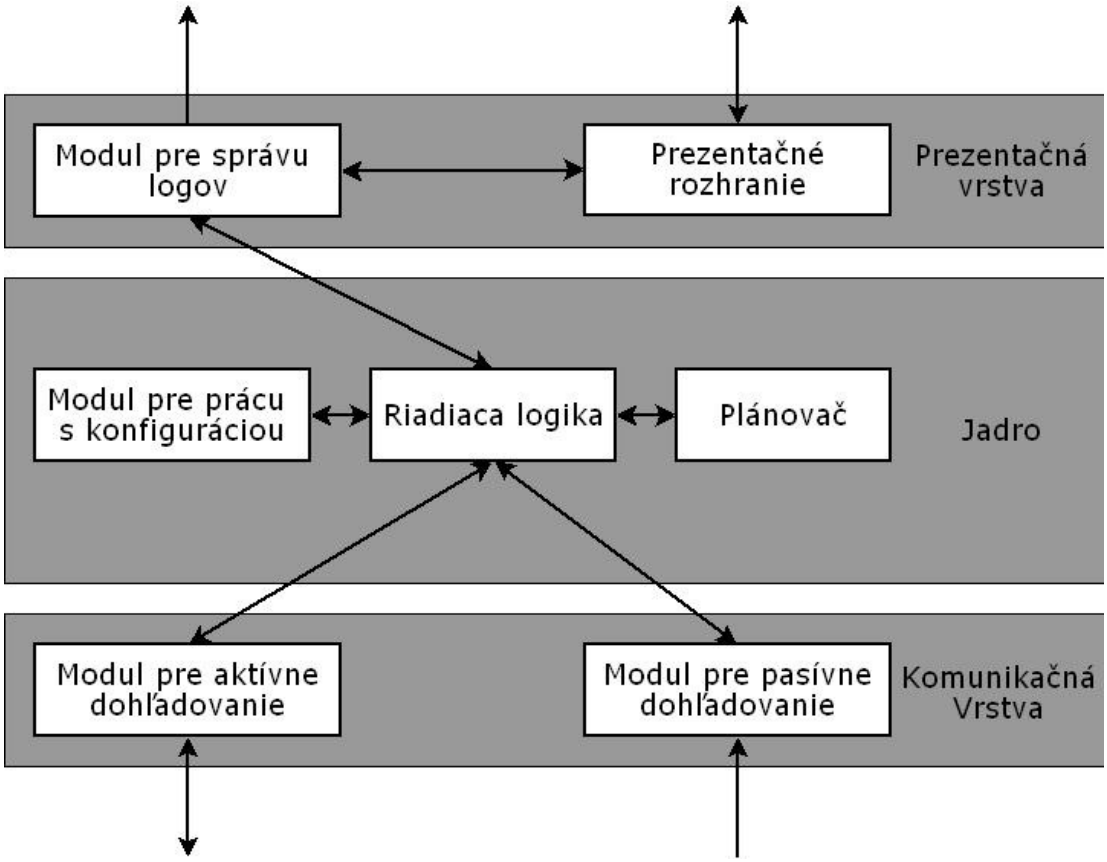
- komunikačné rozhranie – má na starosti zber informácií zo siete
- jadro – zabezpečuje plánovanie kontrol služieb a spracovanie nazbieraných informácií

- prezentačné rozhranie – zobrazuje spracované údaje v zrozumiteľnej forme

Keďže spôsoby dohľadovania služieb sa delia na aktívne a pasívne, komunikačné rozhranie musí odrážať toto rozdelenie. Preto je komunikačné rozhranie rozdelené na aktívnu a pasívnu časť.

Jadro dohľadového systému tiež nie je nedeliteľné. Obsahuje tri hlavné časti: modul na správu konfigurácie, riadiacu logiku a plánovač.

Prezentačná vrstva má v tomto modeli dve základné časti: modul pre zapisovanie logov a prezentačné rozhranie.



Obrázok 2.8 – Vnútorná štruktúra dohľadového systému

V nasledovných častiach sú podrobne popísané jednotlivé zložky tohoto modelu.

2.3.4.1. Komunikačná vrstva

Komunikačné rozhranie spracúva komunikáciu medzi dohľadovým systémom a zariadeniami v sieti. V podkapitole 2.2 boli prezentované dva spôsoby dohľadovania služieb a to aktívne a pasívne dohľadovanie. Komunikačné rozhranie musí vedieť spracovať obidve metódy dohľadovania služieb.

Práca komunikačného rozhrania pri aktívnom dohľadovaní pracuje nasledovným spôsobom:

1. Komunikačné rozhranie dostane požiadavku od jadra na kontrolu konkrétnej služby
2. Komunikačné rozhranie vyvolá potrebnú kontrolu služby
3. Získanú informáciu od externého zdroja na základe definovaných pravidiel úpravy do podoby, ktorú má dohodnutú s jadrom
4. Túto upravenú informáciu pošle jadru

Komunikačné rozhranie musí mať schopnosť spracúvať aktívnu kontrolu viacerých služieb paralelne. V prípade ak by k tomuto nedochádzalo, mohla by služba s dlhším časom aktívnej kontroly zablokovať celé komunikačné rozhranie a kontroly iných služieb by nebolo možné vykonať včas.

Pri pasívnom dohľadovaní pracuje komunikačné rozhranie nasledovne:

1. Komunikačné rozhranie prijme informáciu zo siete
2. Získanú informáciu na základe definovaných pravidiel upraví do podoby vopred dohodnutej s jadrom
3. Upravenú informáciu pošle jadru

Dnešné dohľadové systémy sa značne odlišujú v miere, do akej miery je komunikačné rozhranie pevne naprogramované. Medzi modernými dohľadovými systémami je možné nájsť aj také, ktoré majú celé komunikačné rozhranie pevne implementované. Pridať nový druh služby v prípade takýchto dohľadových systémov vyžaduje zásah priamo do zdrojových kódov dohľadového systému. Ako príklad môže slúžiť dohľadový systém FPinger vie iba posielať zariadeniam v sieti ICMP pakety a na základe toho koľko a za aký čas sa ich vráti určí stav jedinej služby dohľadovanej na danom zariadení, a to dá jeho dostupnosť. V prípade tohoto dohľadového systému úplne odpadá pasívne dohľadovanie. Úplne opačný prístup

ale zvolili napríklad vývojári dohľadového systému Nagios, v ktorom nie je priamo naprogramovaná žiadna komunikácia so sieťou.

2.3.4.2. Jadro dohľadového systému

Štruktúra jadra dohľadového systému presne odzrkadľuje jeho funkciu v dohľadovom systéme. V modeli dohľadového systému sa teda jadro skladá z modulu pre prácu s konfiguráciou, plánovača a riadiacej jednotky.

Modul pre prácu s konfiguráciou obstaráva všetku prácu s konfiguráciou v dohľadovom systéme. Konfiguračné údaje sa pritom môžu nachádzať v textových súboroch, ale napríklad môžu byť vložené v relačnej (prípadne objektovej) databáze. Okrem načítania statických dát z konfiguračnej databázy môže mať modul pre prácu s konfiguráciou rozšírenie pre objavovanie zariadení a služieb na nich bežiacich v sieti, podobne ako to je v dohľadovom systéme OpenNMS. Takto objavené služby sú potom načítané do programu tak, ako by boli zapísané priamo v konfigurácii. Automatické objavovanie zariadení a služieb v sieti je žiadúce hlavne v prípade rozsiahlych sietí, kde nie je možné jednotlivé zariadenia a služby zadať do konfigurácie manuálne. Modul pre prácu s konfiguráciou môže mať tiež funkciu opätovného načítania konfigurácie bez potreby reštartu celého dohľadového systému. V takomto prípade je ale potrebné zabezpečiť potrebné zmeny zoznamu služieb v ostatných častiach jadra.

Plánovač zabezpečuje plánovanie udalostí v rámci dohľadového systému, ako aj plánovanie aktívnych kontrol služieb. Jednoduchý plánovač je možné si predstaviť ako zoznam akcií utriedených podľa času ich vykonania. V pravidelných intervaloch posiela plánovač riadiacej jednotke informáciu o akciách, ktoré treba vykonať. Tieto akcie môžu mať súvis s aktívnou kontrolou služieb v sieti, alebo sa môže jednať o akcie potrebné pre vnútornú údržbu dát v dohľadovom systéme. Po ukončení akcie pošle riadiaca jednotka plánovaču informáciu, na aký čas treba naplánovať nové vykonanie tej istej akcie. Plánovač následne zapíše akciu do poradia na príslušné miesto. Keď znovu príde čas na vykonanie akcie, je akcia opätovne vykonaná a celý proces sa opakuje. Podľa potreby môže mať plánovač schopnosť vypísať aktuálne poradie naplánovaných akcií. Na udržiavanie poradia

akcií je možné použiť viaceré dátové štruktúry. Pre dohľadové systémy dohľadujúce len malé množstvo zariadení a služieb je vhodnou dátovou štruktúrou napríklad spájaný zoznam. Pre väčšie množstvá zariadení a služieb je vhodnejšie použitie iných dátových štruktúr, napríklad sa môže jednať o haldu.

Riadiaca jednotka jadra dohľadového systému zabezpečuje komunikáciu vo vnútri dohľadového systému. Je to práve riadiaca jednotka, ktorá v jadre prijíma informácie prichádzajúce z komunikačnej vrstvy. Ďalšou činnosťou riadiacej jednotky je priama komunikácia s ostatnými časťami jadra dohľadového systému, teda plánovačom od ktorého získava informácie o naplánovaných akciách a modulom pre správu konfigurácie. Napokon riadiaca jednotka posiela spracované informácie modulu pre správu logov v prezentačnej vrstve dohľadového systému.

2.3.4.3. Prezentačná vrstva

Najvyššou vrstvou v dohľadovom systéme je prezentácia údajov. Táto vrstva pozostáva z dvoch častí, je nimi modul pre správu logov a prezentačné rozhranie, ktoré slúži pre prístup k informáciám obsiahnutých v dohľadovom systéme.

Modul pre správu logov obhospodaruje všetky dáta, ktoré sú archivované v rámci dohľadového systému. Dáta, ktoré počas behu neprejdú týmto modulom sú po skončení behu dohľadového systému stratené. Proces zaznamenávania logov prebieha nasledovne:

1. Modul pre správu logov dostane informáciu, ktorú je potrebné zaznamenať, od jadra
2. Prijatú informáciu zapíše do úložiska správ

Týmito úložiskami môže byť súbor na disku, databáza, ale napríklad aj sieťové médium. Práve zápis na sieťové médium umožňuje jednoduché vytvorenie distribuovaného dohľadovania a notifikácií pre klientov dohľadového systému. Modul pre správu logov môže ešte vykonávať ďalšiu činnosť, je ňou zabezpečenie prístupu do logov pre iné časti dohľadového systému alebo externé programy. Táto funkcionalita umožňuje transparentný prístup k logom bez nutnosti poznať ich formát a umiestnenie. Táto transparentnosť umožňuje ľahko vytvárať nadstavby

nad dohľadový systém pracujúce s jeho logmi. Takýto prístup do logov pomocou modulu na ich správu prebieha nasledovne:

1. Modul pre správu logov obdrží cez vopred definované rozhranie požiadavku pre prístup k záznamom v logoch.
2. V prípade, že je táto požiadavka oprávnená, načíta požadované záznamy
3. Načítané záznamy pošle cez vopred definované rozhranie žiadateľovi o záznamy.

Prezentácia údajov zabezpečuje na požiadanie zobrazenie informácií z dohľadového systému jeho klientovi. Takéto poskytnutie informácií prebieha nasledovne:

1. Prezentačné rozhranie obdrží požiadavku o zobrazenie množiny informácií od klienta dohľadového systému cez vopred definované rozhranie
2. V prípade, že má klient oprávnenie pristúpiť k požadovaným informáciám, prezentačná vrstva získa potrebné informácie od ostatných častí dohľadového systému
3. Získané informácie prevedie do vopred dohodnutej formy a následne ich pošle späť klientovi

Prezentačná vrstva priamo komunikuje s modulom pre správu logov, prípadne pristupuje priamo k fyzickému úložisku logov (ak modul pre správu logov neposkytuje transparentný prístup k logom). Ďalej môže pristupovať k modulu pre správu konfigurácie (ak je potrebné zobraziť aktuálnu konfiguráciu) a plánovaču (ak je potrebné zistiť informáciu o naplánovaných akciách). Prezentačné rozhranie musí vedieť obslúžiť viacerých klientov naraz, aby nedochádzalo k zbytočným zdržaniam rýchlych klientov pomalými. Voliteľnou funkciu prezentačného rozhrania je automatická notifikácia klienta o zmene v dohľadovom systéme bez predchádzajúcej požiadavky. V tomto prípade je potrebné zabezpečiť obojsmerný komunikačný kanál medzi prezentačným rozhraním a klientom, cez ktorý sú tieto informácie poskytované. Ďalšou voliteľnou funkciou prezentačného rozhrania je možnosť priamo ovplyvňovať prácu dohľadového systému. Môže sa tak diať pomocou priameho prístupu k riadiacej jednotke dohľadového systému, ale tento spôsob je nevýhodný z bezpečnostných dôvodov. Štandardnejšie riešenie

zabezpečujúce aj zvýšenú mieru bezpečnosti je použité napríklad v dohľadovom systéme Nagios. V ňom prezentačnej vrstve sprístupnené rozhranie slúžiace pre pasívne dohľadovanie služieb v sieti, na ktoré prezentačná vrstva zapisuje príkazy pre dohľadový systém vo vopred definovanej forme. Toto riešenie je bezpečnejšie hlavne z pohľadu toho, že nie je potrebné vytvárať nové zabezpečené rozhranie medzi prezentačnou vrstvou a riadiacou jednotkou, stačí aby bolo dostatočne zabezpečené komunikačné rozhranie pre pasívne kontroly služieb.

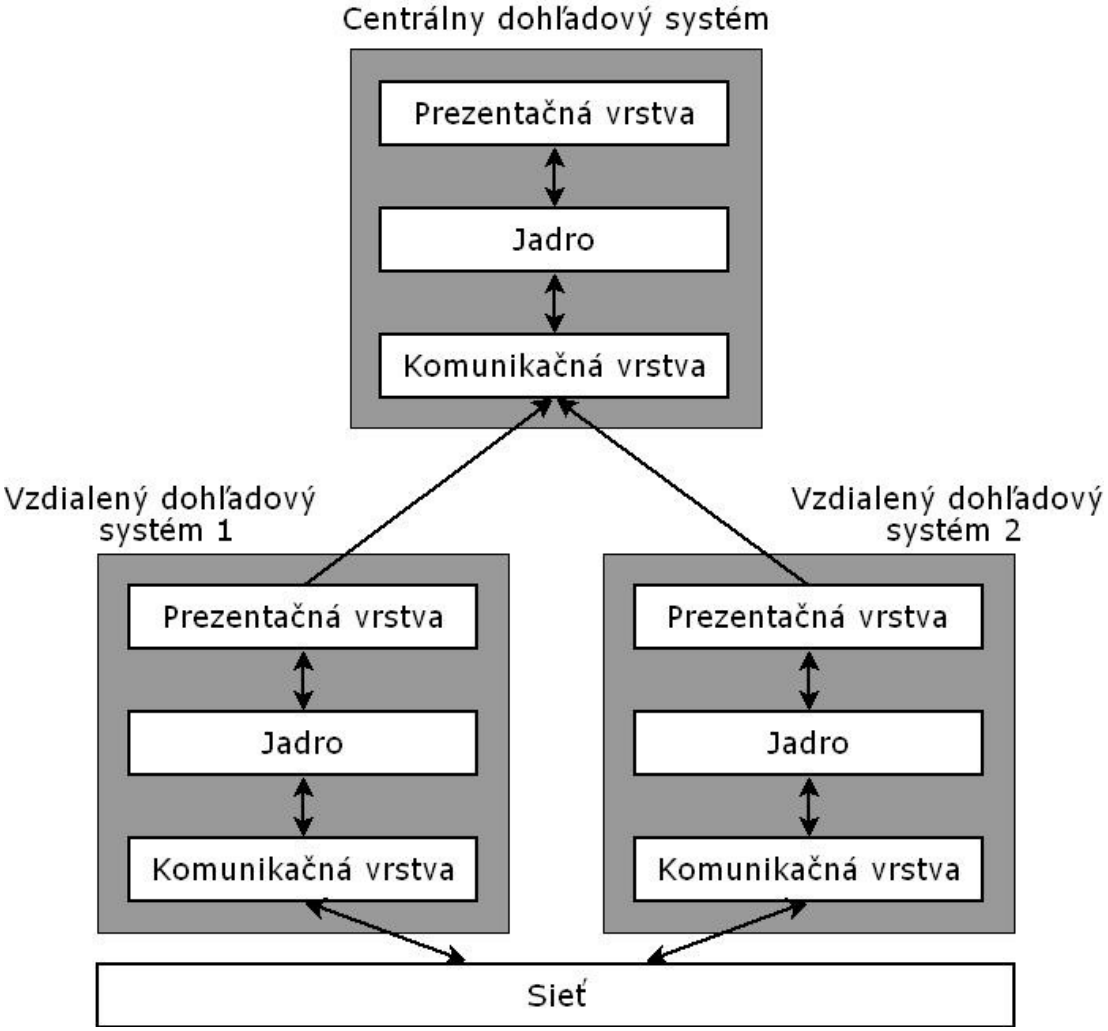
2.3.5 Distribuovaný dohľadový systém

V predchádzajúcich častiach tejto práce bola už viackrát spomenutá možnosť využitia distribuovaných dohľadových systémov. Využívanie viacerých dohľadových systémov je dnes bežnou praxou. Najčastejšie sa však jedná o nezávislé dohľadové systémy, ktoré nemajú žiadnu vzájomnú súčinnosť.

Z hľadiska využívania viacerých dohľadových systémov je ale ďaleko zaujímavejšia ich vzájomná integrácia a vytvorenie distribuovaného dohľadového systému. Význam distribuovaného dohľadovania je hlavne v presunutí záťaže spôsobenej vykonávaním kontrol služieb z jedného centrálneho na viaceré vzdialené dohľadové systémy. Väčšina malých a stredných sietí distribuované dohľadovanie nevyžaduje, keď ale vznikne potreba dohľadovať niekoľko stoviek zariadení a niekoľkonásobne viac služieb býva nasadenie distribuovaného dohľadovania často nevyhnutným krokom.

Pri vytváraní distribuovaného dohľadovania sú značné rozdiely medzi úlohami centrálneho a vzdialených dohľadových systémov. Každý zo vzdialených dohľadových systémov sleduje časť siete, ktorá je mu pridelená najčastejšie na základe geografických kritérií. Jeho úlohou je pasívne, alebo aktívne pristupovať k údajom získaným priamo od zariadení v sieti. Za vopred určených okolností posiela takýto vzdialený dohľadový systém centrálnemu notifikáciu o stavoch jednotlivých služieb. Naproti tomu, primárnou úlohou centrálneho dohľadového systému je spracovávať tieto notifikácie. Tieto informácie následne sprístupňuje svojím klientom cez svoju prezentačnú vrstvu. Môže tiež plánovať aktívne kontroly služieb, deje sa tak však len v špeciálnych prípadoch. Celý proces distribuovaného

dohľadovania s dvomi vzdialenými dohľadovými systémami je zobrazený na obrázku 3.5.



Obrázok 2.9 - Distribuované dohľadovanie

Distribuované dohľadovanie sa teda na prvý pohľad môže zdať veľmi jednoduché: vzdialený dohľadový systém vytvorí vo svojom vnútri virtuálne služby, ktoré reflektujú stav reálnych služieb v sieti, centrálny dohľadový systém potom tieto virtuálne služby pasívne dohľaduje. Distribuované dohľadovanie ale so sebou prináša viacero problémov, ktoré sú podobné problémom s rýdzo pasívnym dohľadovaním služieb. Hlavné problémy teda pozostávajú zo strát notifikácií od vzdialeného dohľadového systému centrálnemu, napríklad keď dôjde k výpadku spojenia medzi nimi, alebo dôjde ku chybe na vzdialenom dohľadovom systéme a

ten následne nepošle jednu alebo viacero notifikácií. Našťastie je možné na riešenie týchto problémov použiť podobné postupy ako pri pasívnom dohľadovaní, teda jeho kombináciu s aktívnym dohľadovaním.

Najčastejšie používaným riešením týchto problémov pri distribuovanom dohľadovaní je využitie informácií o čerstvosti stavu služby, ktorú má k dispozícii centrálny dohľadový systém. Jedná sa o prispôsobenú verziu postupu, ktorý bol podrobnejšie popísaný v podkapitole 2.2.3. Predpokladom pre úspešné využitie tohto postupu je, že vzdialený dohľadový systém kontroluje služby výlučne aktívnou metódou. Vzdialený dohľadový systém v tomto prípade pošle centrálnemu správu po každej aktívnej kontrole služby a v centrálnom dohľadovom systéme je takto zachovávaná potrebná čerstvosť informácie. V prípade, že v stanovenom čase centrálny dohľadový systém neobdrží žiadnu správu, vyhlási stav danej služby za kritický.

Ďalším populárnym riešením je aktívne kontrolovať dostupnosť vzdialených dohľadových systémov. Na prvý pohľad by sa mohlo zdať, že sa týmto eliminovala hlavná výhoda distribuovaného dohľadovania, a teda odbremenenie centrálneho dohľadového systému od aktívneho dohľadovania. Treba si však uvedomiť, že v tomto prípade nedohľaduje centrálny dohľadový systém aktívne všetky služby, ale len vzdialené dohľadové systémy. Tých je väčšinou v porovnaní s počtom dohľadovaných služieb málo, výhoda distribuovaného dohľadovania je teda zachovaná.

2.4. Komunikácia medzi dohľadovým systémom a dohľadovým centrom

Na to, aby malo dohľadovanie reálny význam nepostačuje mať iba vytvorený dobrý dohľadový systém, je potrebné zabezpečiť aj prístup k zozbieraným informáciám. Pre prístup k týmto informáciám slúži prezentačná vrstva, ktorá obsahuje modul pre správu logov a prezentačné rozhranie. Obe tieto jej časti umožňujú prístup k požadovaným informáciám, každá ale odlišným spôsobom.

Pri protokoloch medzi dohľadovým systémom a dohľadovým centrom je možné nájsť analógiu s aktívnym a pasívnym dohľadovaním služieb v sieti a je ich teda možné rozdeliť na dve kategórie vzhľadom na príbuznosť s každým z nich:

- Notifikácie, ktoré sú analógiou pasívneho dohľadovania
- Zobrazenie informácií na požiadanie, ktoré je analógiou aktívneho dohľadovania

Tieto metódy sú podrobne popísané v nasledovných podkapitolách.

2.4.1 Notifikácie

Možnosť odosielať notifikácie o zmenách stavov dohľadovaných služieb bola zabudovaná už v prvých dohľadových systémoch, pretože je najprirodzenejším spôsobom získavania informácií uložených v dohľadovom systéme. Je totiž prirodzené očakávať, že dohľadový systém pri zmene stavu niektorej dohľadovanej služby sám upozorní zodpovedné osoby o tejto udalosti.

Prístup k týmto informáciám len pomocou notifikácií ale vykazuje významné vady. Prípadnou stratou notifikácie totiž vzniká nejednotnosť medzi informáciami, ktoré má k dispozícii dohľadové centrum a reálnym stavom v sieti. Navyše na to, aby bolo reálne možné mať prehľad o stave všetkých služieb v sieti je potrebné duplicitne udržiavať informáciu o aktuálnom stave zo zozbieraných notifikácií.

2.4.2 Zobrazenie informácií na požiadanie

Druhý spôsob prístupu k informáciám v dohľadovom systéme je analógiou k aktívnemu dohľadovaniu. Je ho možné popísať ako periodické opakovanie oddelených prístupov k prezentačnému rozhraniu dohľadového systému. Každý takýto prístup prebieha nasledovne:

1. Klient dohľadového systému vyšle požiadavku prezentačnému rozhraniu dohľadového systému. Táto požiadavka obsahuje informácie o tom, aké informácie požaduje klient zobraziť.

2. Prezentačné rozhranie dohľadového systému overí, či má daný klient práva na prístup k požadovaným informáciám. Ak nie, prístup odmietne. Tento krok je voliteľný, a nemusí byť použitý v každom dohľadovom systéme.
3. Prezentačné rozhranie získa potrebné informácie z logov (prípadne od modulu pre správu logov, ak to podporuje) a získané informácie sú v zrozumiteľnej forme navrátené klientovi dohľadového systému.

Ako príklad takéhoto prístupu k informáciám je možné uviesť prezentačné rozhranie dohľadového systému Nagios.

2.4.3 Kombinácia notifikácií a zobrazenia informácií na požiadanie

Ako aj v prípade komunikácie medzi dohľadovým systémom a sieťou, aj v prípade komunikácie s dohľadovým centrom prináša najlepšie výsledky kombinácia aktívneho a pasívneho prístupu.

Pri tejto kombinácii sú z dohľadového centra v jednotlivých časových okamihoch vyžiadané aktuálne informácie o dohľadovaných službách. Medzi dvomi takýmito požiadavkami je konzistencia informácií udržiavaná pomocou spracovávania notifikácií z dohľadového systému.

2.5. Dohľadové centrum

Poslednou vrstvou v procese dohľadovania je dohľadové centrum. Forma a použitie dohľadového centra sa medzi jednotlivými organizáciami značne odlišuje a je ovplyvňovaná charakterom siete a služieb na nej poskytovaných. Väčšina dohľadových centier tvorí prvostupňovú podporu zákazníkom pre širokú škálu problémov, ako je napríklad pohotovostná podpora zákazníkom, na ktorých prebiehajú útoky za cieľom narušenia ich činnosti, riešenie problémov so stratou pripojenia a bezpečnostné problémy.

Dohľadové centrum je klientom dohľadového systému, ktorý je jedným z jeho hlavných zdrojov informácií. Ďalším zdrojom informácií je kontakt so zákazníkmi a ostatnými zložkami organizačnej štruktúry. Dohľadové centrum má

za úlohu odhaliť a riešiť problémy, ktoré sú objavené dohľadovaním siete. Hrubú kostru riešenia problémov majú všetky dohľadové centrá rovnakú. Jedná sa o nasledovný scenár:

1. Dohľadové centrum pomocou dohľadového systému, alebo na základe kontaktu so zákazníkom, zaregistruje problém v sieti
2. V spolupráci so zákazníkom a zodpovednými pracovníkmi v rámci organizácie dohľadové centrum problém vyrieši
3. Dohľadové centrum vyplní záznam o riešení problému a kópiu tohoto záznamu obdrží aj zákazník

Spomínaný záznam o riešení problému na sieti je možné následne použiť aj pre vytvorenie modelu štandardného správania siete. Takýto záznam sa nazýva *trouble-ticket* a systémy zaoberajúce sa spracovávaním takýchto dokumentov bývajú často úzko prepojené s dohľadovým systémom. Príkladom systémov na správu takýchto záznamov sú napríklad *Open-source Ticket Request System (OTRS)*, alebo *Argus*.

3. Dizajn dohľadovania siete

Táto kapitola je venovaná praktickej ukážke toho, ako je možné v praxi aplikovať poznatky, ktoré boli popísane v predchádzajúcich kapitolách. Pri našom návrhu budeme vychádzať z toho, že systematický postup pri dizajnovaní dohľadovania siete sleduje rozvrstvenie dohľadového procesu. Celý proces je teda možné rozdeliť do nasledovných šiestich krokov:

1. Definovanie požiadaviek na dohľadovanie
2. Analýza siete, nájdenie sieťových indikátorov a ich rozdelenie do príslušných sieťových vrstiev
3. Návrh komunikácie medzi sieťou a dohľadovým systémom
4. Výber dohľadového systému a jeho konfigurácia
5. Návrh komunikácie medzi dohľadovým systémom a dohľadovým centrom
6. Návrh procesov v dohľadovom centre

Návrh procesov v dohľadovom centre nie je nevyhnutnou časťou návrhu dohľadovania siete. Vo väčšine prípadov sú tieto procesy vopred dané spoločnosťou, ktorá si dohľadovanie objednávala.

3.1. Definovanie požiadaviek

V tomto kroku je potrebné popísať aké všetky požiadavky sú na začiatku kladené na dohľadovanie siete. Tieto požiadavky si kladie spoločnosť, pre ktoré je dohľadovanie stavané. Vo zvyšku tejto práce bude pre túto spoločnosť používané jednotné pomenovanie objednávateľ. Jedná sa pritom o dva druhy požiadaviek:

- Funkčné požiadavky – napríklad aktuálnosť stavu dohľadového systému, počet zariadení a služieb v sieti, atď.
- Nefunkčné požiadavky – napríklad aký konkrétny produkt musí byť v procese dohľadovania použitý dohľadový systém, pri tvorbe dohľadovania môžu byť použité len otvorené technológie, atď.

V našom príklade sú na začiatku zadané nasledovné požiadavky:

1. Dohľadový systém musí byť schopný dohľadovať všetky zariadenia v sieti.
2. Počet dohľadovaných zariadení bude maximálne 200 a služieb 1500.

3. Dohľadový systém musí vedieť zaregistrovať 100% udalostí v sieti.
4. Aktuálnosť informácií poskytovaných dohľadovým systémom musí byť maximálne 10 minút.
5. Dohľadový systém musí udržovať záznamy o všetkých udalostiach v sieti.
6. Dohľadový systém musí byť otvorený software.
7. Na dohľadovanie siete je vyhradený server s nasledovnými parametrami:

   CPU: 1x Intel P4 2.2 GHz

   Pamäť: 1x 512 MB

   Disky: 2 x 200GB SATA

   Sieťové rozhrania: 2 x Gbit

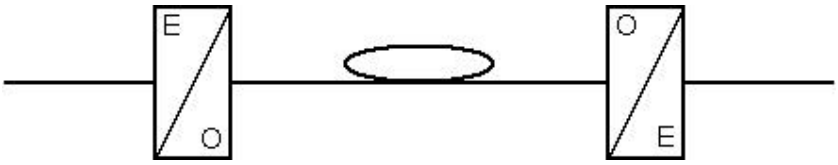
Tento zoznam môže slúžiť ako príklad toho, ako vo všeobecnosti môžu vyzerať požiadavky na dohľadovanie.

3.2. Analýza siete

V tomto kroku je potrebné sa zamerať na charakter zariadení a služieb, ktoré je cieľom dohľadovať a nájdenie sieťových indikátorov pre tieto služby. Dôležité je tiež určiť, ku ktorej vrstve OSI modelu jednotlivé služby prislúchajú. Podľa týchto informácií je potom v ďalšom kroku možné určiť vhodný spôsob, ktorým je tieto služby možné dohľadovať.

V našom príklade sa snažíme dohľadovať MAN sieť. Táto sieť je postavená na báze ethernetu a jej prenosovým médiom sú optické vlákna. Zariadenia používané v tejto sieti je možné rozdeliť do troch kategórií.

Najjednoduchším zariadením používaným v sieti je *opto-elektrický prevodník*. Tento druh zariadenia pracuje na fyzickej vrstve a pár takýchto prevodníkov zabezpečuje konverziu elektrických impulzov na svetelné a zo svetelných znovu na elektrické. Schéma takéhoto zapojenia opto-elektrických prevodníkov je na obrázku 3.1**.**



Obrázok 3.1 – Zapojenie opto-elektrických prevodníkov

Použitie opto-elektrických prevodníkov je významné hlavne z finančných dôvodov. Optické rozhrania do zariadení pracujúcich vo vyšších sieťových vrstvách sú totiž drahšie oproti metalickým. Pre využitie optickej infraštruktúry je teda potrebné použiť takéto konvertory. Parametrami, ktoré je žiadúce na týchto zariadeniach sledovať sú stavy ich optických a metalických rozhraní, ako aj podmienky v akých zariadenie pracuje (teplota, vlhkosť, …).

Ďalším typom zariadení používaných v sieti sú manažovateľné *prepínače*. Prepínače ako už názov hovorí, zabezpečujú prepoje na dátovej vrstve, pričom tieto zariadenia majú podporu 802.1q (VLAN). Pre dohľadovanie týchto zariadení je potrebné sledovať parametre dátovej a nižších vrstiev. Na dátovej vrstve sa jedná o sledovanie počtu chýb objavujúcich sa na jednotlivých zariadeniach v sieti, na fyzickej vrstve sa jedná o stav jednotlivých sieťových rozhraní. Ako aj pri opto-elektrických prevodníkoch je samozrejmosťou aj sledovanie prostredia, v ktorom takéto zariadenie pracuje.

Posledným typom zariadení používaných v sieti sú manažovateľné *smerovače*. Jedná sa o zariadenia zabezpečujúce komunikáciu na sieťovej vrstve, teda routovanie, pričom ako dynamický routovací protokol je použitý Border Gateway Protocol 4 (BGP4) popísaný v RFC1771. Pre sledovanie týchto zariadení je teda žiadúce sledovať sieťovú a nižšie manažovacie vrstvy. Pre dohľadovanie sieťovej vrstvy je potrebné sledovať stav susedných BGP zariadení a dostupnosť zariadení pomocou protokolu ICMP, pre dohľadovanie nižších sieťových vrstiev je možné použiť rovnaké postupy ako pri prepínačoch.

Na tejto sieti sú zákazníkom poskytované nasledovné služby:

- Nasvietené vlákna – služba na fyzickej vrstve
- Dátový prepoj medzi dvomi lokalitami – služba na dátovej vrstve
- Prístup do siete internet – služba na sieťovej vrstve

Pre úspešné dohľadovanie siete je teda potrebné na príslušných zariadeniach dohľadovať sieťovú a nižšie vrstvy.

Z vyššie popísaných parametrov zariadení nemusí byť možné použiť všetky ako sieťové indikátory. Ideálne by bolo, ak by všetky zariadenia v sieti podporovali dohľadovanie všetkých žiadúcich parametrov, takéto zariadenia by ale boli neúmerne drahé. Určeniu, ktoré z týchto parametrov je možné použiť ako sieťové indikátory je venovaná nasledovná podkapitola.

3.3. Návrh komunikácie medzi sieťou a dohľadovým systémom

Pri tejto časti návrhu je dôležité určiť aké protokoly budú použité pri prístupe ku každému zariadeniu a ktoré služby budú pomocou týchto protokolov dohľadované aktívne, ktoré pasívne a ktoré kombináciou pasívneho aj aktívneho dohľadovania. Rozdelenie služieb do kategórií podľa toho, akým spôsobom budú dohľadované je vhodné spracovať na základe toho, do ktorej sieťovej vrstvy spadajú. Zoznam všetkých podporovaných protokolov je možné určiť zo špecifikácie jednotlivých zariadení. V nasledovnej tabuľke sú zobrazené protokoly, ktoré jednotlivé typy zariadení podporujú:

Typ zariadenia	Použiteľné protokoly
Opto-elektrické prevodníky	SNMPv1, ICMP
Prepínače	SNMPv1, SNMPv2c, SNMPv3, RMON2, ICMP
Smerovače	SNMPv1, SNMPv2c, SNMPv3, RMON2, ICMP

Tabuľka 3.1 – Podporované protokoly

Vzhľadom na charakter protokolu SNMP a jeho širokú podporu zo strany výrobcov telekomunikačných zariadení je vhodné zvoliť pre dohľadovanie služieb v sieti

práve tento protokol. Protokol ICMP je potom možné použiť pre dodatočnú kontrolu dostupnosti zariadení.

Samotná podpora SNMP protokolov ale samozrejme pre dohľadovanie nestačí, dôležitou informáciou je aj zoznam manažovateľných objektov, ku ktorým je cez protokol SNMP prístup. Pre každé zariadenie je potrebné dohľadovať vrstvu na ktorej pracujú a aj všetky nižšie. To znamená, že pre každé zariadenie je treba nájsť manažovateľné objektov, ktoré hovoria o stave, v akom sa zariadenie nachádza. Vzhľadom k tomu, že služby poskytované na sieti sú v dostatočne nízkych sieťových vrstvách, je vhodné použitie pasívneho dohľadovania v kombinácii s aktívnym. Preto je potrebné zistiť, aké notifikácie je schopné ktoré zariadenie posielať pre účely pasívneho dohľadovania.

Pri dohľadovaní opto-elektrických prevodníkov je potrebné nájsť identifikátory tých SNMP objektov, ktoré súvisia s dohľadovaním stavu sieťových rozhraní a prostredia v ktorom prevodník pracuje. Dohľadovanie smerodajných parametrov prostredia ale na týchto prevodníkoch nie je podporované. Je teda potrebné sa uspokojiť len s dohľadovaním fyzických rozhraní na prevodníku. Výrobca týchto zariadení neumožnil podporu SNMP notifikácií, je teda k dispozícii len aktívna kontrola pomocou SNMP. Pre aktívne dohľadovanie je možné použiť manažovateľný objekt s identifikátorom .1.3.6.1.2.1.10.19.4.1.4.13 . Jeho hodnota je definovaná ako 0, ak je optický vstup v poriadku, nenulová hodnota signalizuje problém na optickej časti spoja. Pri aktívnych SNMP kontrolách nie je možné zistiť stav elektrického portu na prevodníku.

Pre dohľadovanie prepínačov je potrebné sa zamerať okrem fyzickej vrstvy a vrstvy prostredia aj na nájdenie SNMP identifikátorov pre parametre dátovej vrstvy, teda počet chýb poskytovaných na zariadeniach. Pre pasívne dohľadovanie vrstvy prostredia poskytujú prepínače hneď viacero rôznych notifikácií. Identifikátory týchto notifikácií sú popísané v tabuľke 3.2.

OID	Príčina poslania notifikácie
1.3.6.1.4.1.9.9.13.3.1	Jedna z nameraných hodnôt dosiahla hranicu, pri ktorej nie je možná ďalší práca zariadenia a je automaticky vypnuté
1.3.6.1.4.1.9.9.13.3.2	Nameraná voltáž je mimo bežných hodnôt pre prácu zariadenia
1.3.6.1.4.1.9.9.13.3.3	Nameraná teplota je mimo bežných hodnôt pre prácu zariadenia
1.3.6.1.4.1.9.9.13.3.4	Niektorý z ventilátorov na zariadení vypadol
1.3.6.1.4.1.9.9.13.2.5	Výpadok redundantného zdroju napájania

Tabuľka 3.2 – Notifikácie pre dohľadovanie vrstvy prostredia pri prepínačoch

Pre aktívne dohľadovanie teploty prostredia je možné použiť identifikátor SNMP objektu .1.3.6.1.4.1.9.9.13.1.3.1.6 . Tento objekt môže nadobúdať 6 hodnôt: normal(1), warning(2), critical(3), shutdown(4), notPresent(5), a notFunctioning(6). Pre pasívne dohľadovanie fyzickej vrstvy je možné použiť nasledovné notifikácie:

OID	Príčina poslania notifikácie
.1.3.6.1.6.3.1.1.5.3	Jedno z rozhraní zmenilo svoj stav na Down
.1.3.6.1.6.3.1.1.5.4	Jedno z rozhraní zmenilo svoj stav na Up

Tabuľka 3.3 – Pasívne dohľadovanie fyzickej vrstvy pri prepínačoch

Pre aktívne dohľadovanie fyzickej vrstvy je možné použiť identifikátor SNMP objektu .1.3.6.1.2.1.2.2.1.8.x , prislúchajúci stavu konkrétneho sieťového rozhrania na zariadení. Hodnota x predstavuje číslo pre dané rozhranie, ktoré mu bolo udelené v SNMP strome. Objekt prislúchajúci danému identifikátoru môže nadobúdať 7 hodnôt: up(1), down (2), testing (3), unknown (4), dormant(5), notPresent(6) a lowerLayerDown(7). Pasívne dohľadovanie dátovej vrstvy nie je na používaných prepínačoch podporované, je ale možné použiť aktívne dohľadovanie pomocou identifikátorov .1.3.6.1.2.1.2.2.1.14.x (IF-MIB::ifInErrors), v ktorom sa udržuje počet prijatých chybných rámcov a .1.3.6.1.2.1.2.2.1.20.x (IF-MIB::ifOutErrors), v ktorom sa udržuje počet odoslaných chybných rámcov.

Ďalšími zaujímavými objektmi sú .1.3.6.1.2.1.2.2.1.10 (IF-MIB::ifInOctets), ktorý obsahuje počet prijatých bajtov na sieťovom rozhraní a .1.3.6.1.2.1.2.2.1.16.x (IF-MIB::ifOutOctets), ktorý obsahuje počet odoslaných bajtov na sieťovom rozhraní. Hodnota .x opäť predstavuje číslo pre dané rozhranie, ktoré mu bolo udelené v SNMP strome.

Pre dohľadovanie smerovačov je potrebné sa zamerať okrem dátovej, fyzickej a vrstvy prostredia aj na nájdenie SNMP identifikátorov pre parametre sieťovej vrstvy, teda počet chýb poskytovaných na zariadeniach. Pre pasívne aj aktívne dohľadovanie dátovej, fyzickej a vrstvy prostredia je možné použiť totožné SNMP objekty, ako tomu je aj v prípade prepínačov. Pre pasívne dohľadovanie sieťovej vrstvy je možné použiť nasledovné notifikácie:

OID	Príčina poslania notifikácie
.1.3.6.1.2.1.15.7.1	Stav BGP spojenia sa dostane do stavu ESTABLISHED
.1.3.6.1.2.1.15.7.2	Stav BGP spojenia sa presunie z vyššieho stavu do nižšieho

Tabuľka 3.4 – Pasívne dohľadovanie sieťovej vrstvy pri smerovačoch

Dynamické routovanie je tiež možné dohľadovať aktívne pomocou SNMP objektu s identifikátorom .1.3.6.1.2.1.15.3.1.2 (BGP4-MIB::bgpPeerState), za ktorým je potrebné uviesť ip adresu susedného BGP smerovača, napríklad pre ip adresu 1.1.1.1 bude celý identifikátor .1.3.6.1.2.1.15.3.1.2.1.1.1.1. Tento objekt môže nadobúdať 6 hodnôt: idle (1), connect(2), active(3), opensent(4), openconfirm(5), established(6) .

3.4. Výber a konfigurácia dohľadového systému

Pri výbere dohľadového systému je potrebné zohľadniť viacero parametrov. Všetky ovplyvňujúce parametre je možné zadeliť do jednej z troch kategórii na základe toho, v ktorej fáze tvorby dohľadovania vznikli.

V prvom rade sa jedná o počiatočné požiadavky kladené na dohľadový systém, ktoré boli zadané objednávateľom dohľadovania na začiatku celého

procesu vytvárania dohľadovania. Tieto požiadavky poskytujú základné informácie o tom, aké parametre musí dohľadový systém spĺňať.

Ďalším dôležitým parametrom je štruktúra dohľadovanej siete a služieb na nej poskytovaných. V tomto prípade sa jedná o služby na sieťovej a nižších vrstvách. Podľa tabuľky 2.5 je pre dohľadovanie služieb na týchto vrstvách vhodné použitie pasívneho dohľadovania, prípadne jeho kombinácia s aktívnym.

Posledným smerodajným parametrom pre výber dohľadového systému je špecifikácia komunikačných protokolov medzi sieťou a dohľadovým systémom. V prípade našej siete je vyžadovaná hlavne podpora SNMP notifikácií a aktívnej kontroly služieb v sieti pomocou protokolov SNMP a ICMP .

Po analýze všetkých týchto parametrov sa vykryštalizovali dva vhodné dohľadové systémy – OpenNMS a Nagios. Hlavným argumentom pre tieto dva dohľadové systémy je ich natívna integrácia s protokolom SNMP a dobrá podpora zo strany komunity ich používateľov. Vzhľadom na malú veľkosť siete, požiadavky kladené na dohľadový systém, jednoduchosť inštalácie, používania, a údržby bol ako dohľadový systém zvolený Nagios. Ďalším argumentom hovoriacim pre tento dohľadový systém je jednoduchý spôsob rozšírenia v prípade, že v budúcnosti bude potrebné doplniť novú funkcionalitu.

Po výbere protokolov pre komunikáciu so sieťou a dohľadového systému je čas sa zamerať na návrh konfigurácie dohľadového systému. Hlavnou úlohou je zamerať sa na definíciu služieb, ktoré budú na každom druhu zariadenia dohľadované a ako budú tieto služby ovplyvňované hodnotami získanými zo siete. Do úvahy treba zobrať aj fakt, že dohľadový systém Nagios umožňuje definovať okrem normálnych služieb pre každé zariadenie jednu špeciálnu, ktorá slúži na kontrolu stavu zariadenia ako celku. Kontroly tejto služby nie sú potom plánované periodicky, ale pri výpadku ktorejkoľvek služby na zariadení je naplánovaná okamžitá kontrola tejto služby. Túto možnosť využijeme pre dohľadovanie dostupnosti všetkých zariadení pomocou protokolu ICMP.

Aj keď Nagios umožňuje použiť viacero rôznych stavov služby v našom príklade použijeme výlučne binárne rozdelenie: stav každej služby môže byť buď *v poriadku (OK)*, alebo *kritický*. Takéto striktné rozdelenie má viacero výhod.

V prvom rade to reflektuje fakt, že pre zákazníka využívajúceho sieť je poskytovaná služba buď úplne funkčná, alebo ju považuje za nefunkčnú. Taktiež toto rozdelenie umožňuje zjednodušiť procesy prebiehajúce v dohľadovom centre.

Opto-elektické prevodníky budú mať, vzhľadom k malému počtu vhodných manažovateľných objektov, definovanú len jednu službu a to stav optického rozhrania. Pre aktívne dohľadovanie je používaná prevodná tabuľka medzi hodnotami príslušného SNMP manažovateľného objektu a stavmi služby. Kľúč, podľa ktorého sa tak deje, je zobrazený v tabuľke 3.5 .

Názov služby	SNMP identifikátor objektu	Stav v poriadku	Kritický stav
Optické rozhranie	.1.3.6.1.2.1.10.19.4.1.4.13	0	Iná hodnota

Tabuľka 3.5 – Kľúč pre určenie stavov služby pri aktívnom dohľadovaní

Prepínače použité v sieti už umožňujú dohľadovať väčšie množstvo manažovateľných objektov. Pre každý prepínač sú definované služby dohľadujúce jeho okolitú teplotu, stav jednotlivých sieťových rozhraní a počet chýb na jednotlivých sieťových rozhraniach. Pre aktívne dohľadovanie je používaná prevodná tabuľka medzi hodnotami príslušného SNMP manažovateľného objektu a stavmi služby. Kľúč, podľa ktorého sa tak deje, je zobrazený v tabuľke 3.7 .

Názov služby	SNMP identifikátor objektu	Stav v poriadku	Kritický stav
Teplota	. 1.3.6.1.4.1.9.9.13.3.1	1	Iná hodnota
Stav rozhrania	.1.3.6.1.4.1.9.9.13.1.3.1.6.x	1	Iná hodnota
Počet chýb na rozhraní	.1.3.6.1.2.1.2.2.1.14.x a .1.3.6.1.2.1.2.2.1.20.x	Hodnoty ostali nezmenené	Jedna z hodnôt sa zvýšila

Tabuľka 3.6 – Kľúč pre určenie stavov služby pri aktívnom dohľadovaní

Pre pasívne dohľadovanie je používaná prevodná tabuľka medzi identifikátormi jednotlivých SNMP notifikácií a zmenami stavu služby, ktorý ich príchod spôsobí. Kľúč, podľa ktorého sa tak deje je zobrazený v tabuľke 3.8.

SNMP indetifikátor	Služba	Nový stav služby
. 1.3.6.1.4.1.9.9.13.3.3	Teplota	Kritický
.1.3.6.1.6.3.1.1.5.3	Stav rozhrania	Kritický
.1.3.6.1.2.1.15.7.2	Stav rozhrania	V poriadku

Tabuľka 3.7 – Kľúč pre určenie stavov služby pri pasívnom dohľadovaní

Pasívne dohľadovanie počtu chýb na rozhraní nie je podporované. Iné parametre prepínačov nie sú v dnešnej dobe dohľadované.

Vrstva prostredia, fyzická a dátová vrstva je na smerovačoch dohľadovaná spôsobom identickým s prepínačmi. Na rozdiel od prepínačov však pribúda vrstva sieťová, v ktorej je pre každé BGP spojenie definovaná jedna služba BGP. Pre aktívne dohľadovanie je používaná prevodná tabuľka medzi hodnotami príslušného SNMP manažovateľného objektu a stavmi služby. Kľúč, podľa ktorého sa tak deje, je zobrazený v tabuľke 3.9 .

Názov služby	SNMP identifikátor objektu	Stav v poriadku	Kritický stav
BGP	.1.3.6.1.2.1.15.3.1.2.a.b.c.d	6	Iná hodnota

Tabuľka 3.8 – Kľúč pre určenie stavov služby pri aktívnom dohľadovaní

Pre pasívne dohľadovanie je používaná prevodná tabuľka medzi identifikátormi jednotlivých SNMP notifikácií a zmenami stavu služby, ktorý ich príchod spôsobí. Kľúč, podľa ktorého sa tak deje je zobrazený v tabuľke 3.10.

SNMP indetifikátor	Služba	Nový stav služby
.1.3.6.1.2.1.15.7.1	BGP	V poriadku
.1.3.6.1.2.1.15.7.2	BGP	Kritický

Tabuľka 3.9 – Kľúč pre určenie stavov služby pri pasívnom dohľadovaní

Je dôležité poznamenať, že pri pasívnom dohľadovaní služieb je potrebné spárovať každú prijatú notifikáciu s konkrétnou službou na základe dát obsiahnutých v notifikácii. Napríklad pri príchode notifikácie o zmene stavu

jedného zo sieťových rozhraní na zariadení je potrebné zmeniť stav len jednej jemu prislúchajúcej službe a nie všetkým službám popisujúcim stav sieťových rozhraní.

3.5 Komunikácia medzi dohľadovým systémom a dohľadovým centrom

Reálne použiteľná komunikácia medzi dohľadovým centrom a dohľadovým systémom je v najväčšej miere ovplyvnená výberom dohľadového systému Nagios. Pre zjednodušenie prístupu k informáciám obsiahnutým v dohľadovom systéme je cieľom používať čím štandardnejšie protokoly.

Nagios vo svojej štandardnej distribúcii poskytuje prehľadné rozhranie v podobe CGI programov, ktoré je možné vyvolávať z ľubovoľného webového servra, podporujúceho spúšťanie CGI skriptov. V našom prípade bol ako webový server použitý Apache 1.3.34. Zobrazovanie informácií v dohľadovom centre je potom možné zabezpečiť pomocou ľubovoľného www prehliadača.

Pre doplnenie funkcionality notifikácií sú v našom prípade použité e-mailové správy posielané pomocou protokolu SMTP, ktoré sú doručované na adresu, ku ktorej majú prístup pracovníci dohľadového centra.

3.6. Procesy v dohľadovom centre

Pri dohľadovaní samozrejme nestačí, že dohľadové centrum má prístup k dohľadovému systému. Je potrebné zadefinovať procesy, pomocou ktorých sú v dohľadovom centre riešené vzniknuté problémy. Jedná sa o dva procesy, rozdelené na základe toho, či bol problém nahlásený dohľadovému centru zákazníkom, alebo dohľadové centrum zaregistrovalo problém pomocou dohľadového systému.

Proces prebiehajúci v prípade, že dohľadové centrum zaregistruje problém pomocou dohľadového systému je nasledovný:

1. Dohľadové centrum zaregistruje problém pomocou dohľadového systému

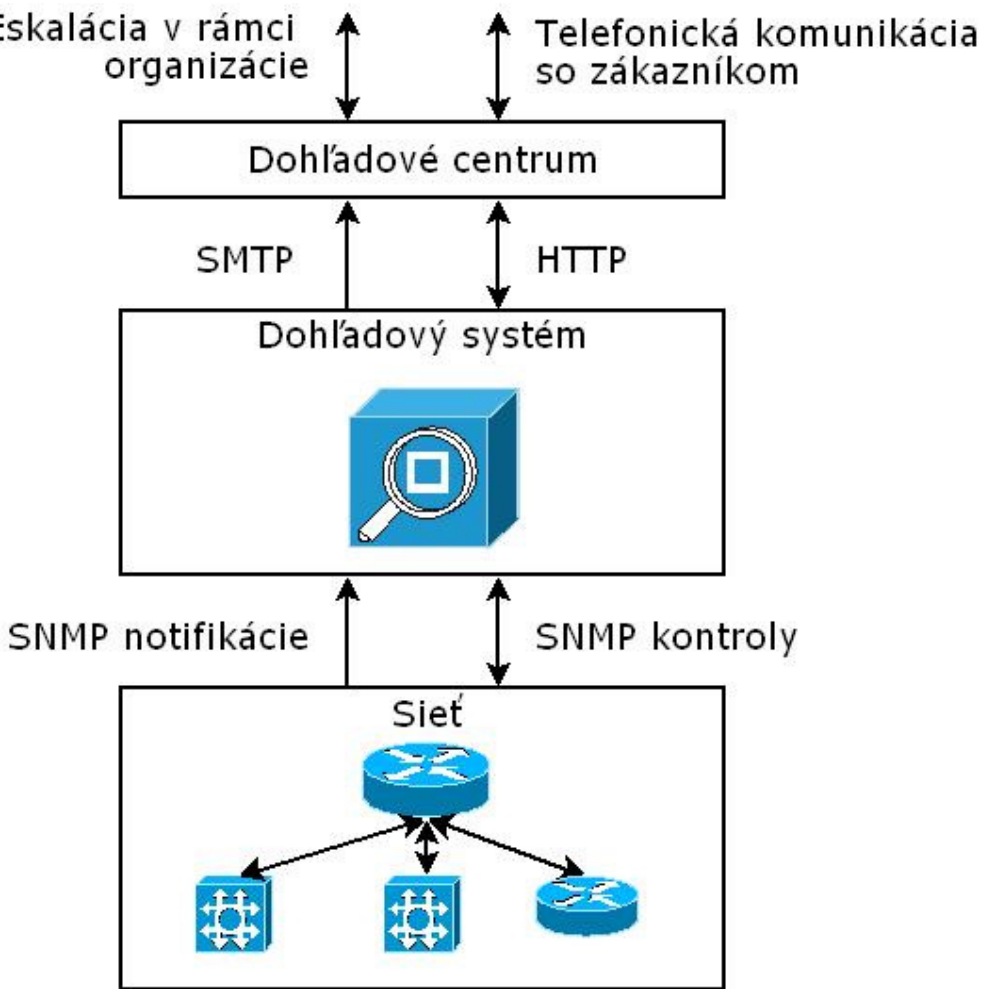
2. Dohľadové centrum sa spojí priamo so zákazníkom a zistí, či sa nejedná o plánovanú údržbu zariadení u zákazníka, prípadne či sa nejedná o výpadok elektriny u zákazníka
3. V prípade, že problém nie je spôsobený výpadkom priamo u zákazníka, založí dohľadové centrum záznam o riešení problému a problém začne riešiť
4. Pokiaľ dohľadové centrum nevie svojpomocne vyriešiť vzniknutý problém, kontaktuje zodpovedného technického pracovníka podľa definovaného eskalačného reťazca v rámci organizácie
5. Po vyriešení problému pošle dohľadové centrum vyplnený záznam o riešení problému zákazníkovi

Proces prebiehajúci v prípade, že problém nahlási dohľadovému centru zákazník je nasledovný:

1. Zákazník nahlási problém dohľadovému centru
2. Dohľadové centrum overí existenciu problému v rámci siete, ak sa jeho existencia potvrdí, založí záznam o riešení problému a informuje o tom zákazníka
3. Pokiaľ dohľadové centrum nevie svojpomocne vyriešiť vzniknutý problém, kontaktuje zodpovedného technického pracovníka podľa definovaného eskalačného reťazca v rámci organizácie
4. Po vyriešení problému pošle dohľadové centrum vyplnený záznam o riešení problému zákazníkovi

3.7 Zhrnutie dohľadovania

Pre prehľadnosť celého procesu dohľadovania je dôležité vytvoriť jeho názornú reprezentáciu. Kompletná schéma vytvoreného dohľadovania je zobrazená na obrázku 3.2.



Obrázok 3.2 – Štruktúra a technológie vytvoreného dohľadovania.

3.8 Rozširovanie dohľadovania do budúcna

Pri každom systéme je vždy možné nájsť priestor pre ďalšie vylepšenia. Výnimkou z tohoto pravidla nie je ani vytvorené dohľadovanie a do budúcna bude určite potrebné tento proces rozšíriť. Ako príklad je možné doplniť napríklad je možné uviesť funkcionalitu odosielania SMS notifikácií s využitím natívne pripojenej GSM brány. Keďže každým dňom vznikajú nové zariadenia a technológie, pri ich nasadení bude pravdepodobne potrebné rozšíriť počet parametrov sietí, ktoré bude potrebné dohľadovať. Nové technológie so sebou samozrejme prinášajú aj nové poskytovane služby, ktoré bude potrebné dohľadovať.

Záver

Napriek tomu, že dohľadovanie sietí nie je zďaleka novou technikou, systematický prístup k nemu je vzácny. Ešte aj v dnešnej dobe sa objavujú dohľadové systémy, ktoré sa snažia o dohľadovanie sietí úplne nevhodnými metódami. Často sa pritom jedná o aktívne dohľadovanie služieb, ktoré na takýto spôsob dohľadovania nie sú stavané. Dnešné problémy pri dohľadových systémoch sa ale netýkajú len zlého návrhu komunikácie medzi dohľadovým systémom a zariadeniami v sieti, nedostatky často vznikajú priamo v implementácii dohľadového systému. Problémov pri dohľadovaní sietí je teda podstatne viac ako by sa na prvý pohľad mohlo zdať. Táto diplomová práca sa snažila navrhnúť systematické riešenie na väčšinu týchto problémov.

Prehľadovo ladenú prvú kapitolu som zvolil pre uvedenie čitateľa do problematiky dohľadovania sietí. Veľa problémov s dohľadovaním sietí vzniká hlavne z neznalosti základných princípov dohľadovania.

V technicky zameranej druhej kapitole som chcel poskytnúť pohľad na dohľadovanie sietí z jeho vnútra. Postupným popisovaním existujúcich technológií na základe ich úlohy v procese dohľadovania som sa snažil poskytnúť čitateľovi prehľad o tom s akými nástrojmi je možné v dnešnej dobe počítať a aké majú svoje klady a zápory. V častiach tejto kapitoly, ktorým do dnešnej doby ešte nebola venovaná pozornosť a aktuálne používané metódy majú svoje nedostatky som sa snažil navrhnúť vlastné riešenia vzniknutých problémov.

Tretia kapitola je venovaná implementácii dohľadovania v prostredí reálne existujúcej siete. Jej úlohou v rámci tejto práce je ukázať praktické aspekty budovania dohľadovania siete. Dôraz je kladený hlavne na systematickosť tohoto postupu, ktorá je v praxi často opomínaná. Snažil som sa v nej hlavne poukázať na možnosť prispôsobenia dnešných dohľadových systémov tak, aby spĺňali potrebné kritériá bez potreby vytvárať úplne nový dohľadový systém v podstate od nuly. Takisto som sa v nej snažil poukázať na praktické využitie vlastných návrhov prezentovaných v tretej kapitole.

Zostáva teda už len zodpovedať otázku: „Ako vystihnúť celkový prínos práce?“. V minulosti boli všetky komplexnejšie systémy pre dohľadovanie sietí komerčné a väčšina úprav nutných pre splnenie špecifických zákazníckych požiadaviek smerovala cestou nákladného vývoja veľkej časti aplikácie. Alternatívy vyvíjané podľa modelu s otvoreným zdrojovým kódom si takýto spôsob vývoja nemôžu dovoliť a riešenia väčšiny problémov musia zovšeobecniť do takej miery, aby boli univerzálne použiteľné pre väčšinu používateľov. Jednoduchosť nasadenia preniesla na plecia správcu dohľadového systému nové problémy súvisiace s nasadením efektívnych algoritmov kontroly a vyhodnocovania stavov siete, ktoré som v práci popísal. Verím, že poskytla dostatočný teoretický základ a praktický prínos pri nasadení otvorených dohľadových technológií v heterogénnej sieti, kde sú dohľadovane viaceré druhy zariadení rôznych výrobcov.

Slovník pojmov

Argus Nástroj pre sledovanie riešenia problémov. Je naprogramovaný v jazyku Java.

Abstract Syntax Notation One (ASN.1) Formálny jazyk pre abstraktný popis správ, ktoré sú vymieňané medzi veľkým množstvom aplikácií. Jeho použitie je možné nájsť napríklad v Internete, mobilných telefónoch, bezpečných elektronických službách a interaktívnej televízii.

Asynchronous Transfer Mode (ATM) Sieťová technológia založená na prenose dát v bunkách fixnej dĺžky. Veľkosť týchto buniek je relatívne malá v porovnaní so staršími technológiami, čo umožňuje prenášať obrazové, hlasové a počítačové dáta pomocou tej istej siete bez toho, aby ani jeden z týchto prenosov nezahltil linku.

Apache Populárny server slúžiaci pre poskytovanie prístupu k WWW stránkam.

Border Gateway Protocol (BGP) Routovací protokol medzi autonómnymi systémami, ktoré sú sieťami pod jednotnou správou. V dnešnej dobe sa používa na routovanie v Internete.

Common Gateway Interface (*CGI)* Štandardný protokol pre komunikáciu s externých aplikácií so serverom WWW. Umožňuje WWW serveru poslať informácie odosielané z WWW prehliadača externej aplikácii a jej výstup poslať späť prehliadaču.

Ethernet Počítačová sieť založená na rámcoch zameraná na lokálne siete. Postupom času nahrádza všetky ostatné štandardy v lokálnych sieťach.

First In First Out (FIFO) Termín popisujúci poradie. Položky sú spracovávané v takom poradí, v akom prichádzajú.

Friendly Pinger (FPINGER) Dohľadový systém zameraný na dohľadovanie dostupnosti zariadení v sieti pomocou protokolu SNMP.

File Transfer Protocol (FTP) Bežne používaný protokol slúžiaci na presun súborov.

Global System for Mobile Communications (GSM) Najpopulárnejší štandard pre mobilnú telefónu sieť na svete.

HP OpenView Komerčná rada produktov spoločnosti *Hewlett Packard* zameraná na správu sietí. Obsahuje stovky rozšírení priamo od výrobcu a tisícky ďalších poskytovaných tretími stranami.

Hypertext Transfer Protocol (HTTP) Metóda používaná pre prenos informácií obsiahnutých vo WWW.

Internet Control Message Protocol (ICMP) Jeden z hlavných protokolov v Internete. Slúží väčšinou na dohliadanie dostupnosti zariadení v sieti.

Internet Protocol (IP) Dátovo orientovaný protokol používaný pre komunikáciu cez paketovo prepínanú sieť.

Metropolitan Area Network (MAN) Stredne veľká počítačová sieť, ktorá svojimi rozmermi pokrýva rozlohu jedného mesta.

Management Information Base(MIB) Je databáza používaná pre správu telekomunikačných zariadení v sieťach.

Object Identifier (OID) Identifikátor používaný na pomenovanie objektu. Štrukturálne sa skladá z uzla v hierarchickej štruktúre pomenovávania definovanej pomocou ASN.1.

Open Systems Interconnection (OSI) Snaha pre štandardizáciu sietí, ktorá začala v roku 1982. Až do jej vzniku bola implementácia sietí úplne závislá od výrobcov a dodávateľov.

Plesiochronous Digital Hierarchy (PDH) Technológia používaná v synchrónnych telekomunikačných sieťach. Slovo plesiosynchronous je odvodené od gréckeho *plesio*, znamenajúceho skoro, a *chronos*, čas, a hovorí o tom, že PDH siete pracujú v stave, kde sú jednotlivé časti siete skoro, ale nie úplne synchronizované

Ping Program využívajúci protokol ICMP na sledovanie dostupnosti zariadení.

Request for Comments (RFC) Skupina memoránd, ktoré sprevádzajú nový výskum, inovácie a metodológie aplikovateľné na technológie Internetu.

Remote Monitoring (RMON) Štandard používaný v telekomunikáciách, ktorý implementuje MIB súbor umožňujúci vzdialenú správu a dohľad nad sieťovými zariadeniami. Pre komunikáciu so zariadeniami využíva protokol SNMP.

Simple Mail Transfer Protocol (SMTP) Protokol, ktorý sa v podstate stal štandardom pre výmenu elektronickej pošty v dnešných sieťach.

SimpleNetwork Management Protocol (SNMP) Protokol slúžiaci na dohľadovanie a správu sieťových zariadení.

World Wide Web (WWW) Globálny informačný priestor, z ktorého môžu ľudia čítať, a na ktorý môžu zapisovať informácie pomocou veľkého množstva rozličných zariadení pripojených do siete Internet.

Zoznam bibliografických odkazov

[1] Edmund Wong , Network Monitoring Fundamentals and Standards, Washington University in St. Louis, August 1997, Formát HTML, Dostupné na internete: < http://www.cse.wustl.edu/~jain/cis788-97/ftp/net_monitoring/index.htm >

[2] Les Cottrell, Network Monitoring Tools, Standford Linear Accelerator Center, Marec 2006, Formát HTML, Dostupné na internete: < http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html>

[3] Issues about the Integration of Passive and Active Monitoring for Grid Networks, Foundation for Research and Technology-Hellas, 2005, Formát PDF, Dostupné na internete: < http://www.ics.forth.gr/dcs/Activities/papers/2005.coregrid.pasvactive.pdf >

[4] Arati Baliga, Nitin Gupta, Lev Kaufman, Prashant Mekaraj, Andrew Tjang, Wenyuan Xu, Network Monitoring and Forensics, Rutgers University, Máj 2004, Formát PDF, Dostupné na internete: < http://www.research.rutgers.edu/~aratib/presentations/forensics_paper.pdf >

[5] Les Cottrell, Passive vs. Active Monitoring, Standford Linear Accelerator Center, Marec 2001, Formát HTML, Dostupné na internete: < http://www.slac.stanford.edu/comp/net/wan-mon/passive-vs-active.html>

[6] Warren Matthews, Les Cottrell, Davide Salomoni, Passive and Active Monitoring on a High Performance Research Network, Standford Linear Accelerator Center, Február 2001, Formát PDF, Dostupné na internete: < http://www.slac.stanford.edu/cgi-wrap/getdoc/slac-pub-8776.pdf>

[7] Ethan Galstad , Nagios Documentation, Február 2006, Formát HTML a PDF, Dostupné na internete: < http://www.nagios.org/docs/ >

[8] Tarus Balog, OpenNMS Documentation,Marec 2003, Formát HTML, Dostupné na internete: < http://www.opennms.org/index.php/Official_Documentation>

[9] Jim Trocki, Mon Documentation, Február 2002, Formát HTML, Dostupné na internete: < http://www.kernel.org/software/mon/>

[10] RFC1157 – A Simple Network Management Protocol (SNMP), MIT Laboratory for Computer Science, Máj 1990, Formát HTML, Dostupné na internete: < http://rfc.net/rfc1157.html>

[11] RFC1901 – Introduction to Community-based SNMPv2, International Network Services, Január 1996, Formát HTML, Dostupné na internete: < http://rfc.net/rfc1901.html>